McAfee Web Gateway

Безопасность. Обмен информацией об угрозах. Быстродействие.

Современный Интернет дает организациям намного больше возможностей, чем прежде. Современные веб-технологии позволяют динамически взаимодействовать с пользователями в реальном времени. Но пользоваться Интернетом сегодня стало опаснее, чем прежде. Степень изощренности интернет-атак растет изо дня в день. McAfee® Web Gateway представляет собой критически важное средство защиты, позволяющее обезопасить любую организацию от новейших угроз, исходящих от вредоносного ПО. Реализованный в нем передовой подход к обеспечению безопасности, сочетающий в себе тщательный локальный анализ намерений и облачную защиту на основе технологий McAfee Labs, дает организациям возможность значительно сократить уровень риска и обеспечить себе безопасный доступ в Интернет.

McAfee Web Gateway

- Предлагается в виде разных моделей аппаратных устройств и в виде виртуальной машины с поддержкой VMware и Microsoft Hyper-V.
- Интегрируется со смежными решениями McAfee, такими как McAfee Endpoint Security, McAfee Advanced Threat Defense, McAfee Threat Intelligence Exchange, McAfee Cloud Data Protection и McAfee Cloud Visibility — Community Edition.
- Сертифицирован в соответствии со стандартами Common Criteria уровня EAL2+ и FIPS 140-2 уровня 2.
- Поддержка разных вариантов хранения ключей шифрования, в том числе аппаратных модулей безопасности Gemalto SafeNet и Thales nShield, а также плат Thales PCIe.
- Продукт признан лучшим решением для защиты от вредоносных программ среди безопасных веб-шлюзов (AV-TEST).

Чем больше используется Интернет, чем сложнее он становится, тем острее ощущается потребность в современных средствах веб-защиты. Если сайт производит впечатление «безопасного», это не значит, что он не может стать объектом атаки и быть превращен в инструмент распространения вредоносного ПО. В сложившейся на сегодняшний день ситуации уже недостаточно просто блокировать известные вирусы или ограничивать доступ к «заведомо плохим» веб-сайтам. Такие методы реагирования на угрозы безопасности, как антивирусная защита с использованием сигнатур и фильтрование URL-адресов только по категориям, хоть и являются необходимыми, однако недостаточными для защиты доступа к облачным приложениям и для борьбы с современными средствами использования уязвимостей.

В их основе лежит информация об уже известном содержимом, уже известных вредоносных объектах и исполняемых файлах, поэтому эти методы не в состоянии ни предотвращать современные атаки, скрывающие вредоносный код внутри, казалось бы, надежного трафика HTTP или HTTPS, ни защищать от неизвестных и новейших угроз. Сегодня крайне важно иметь возможность обеспечивать безопасный и детально настраиваемый доступ к облачным приложениям и при этом быть в состоянии блокировать неизвестные и известные угрозы в упреждающем режиме.

Комплексная защита входящего и исходящего трафика

Аппаратно-программная архитектура McAfee Web Gateway, отличающаяся высоким уровнем быстродействия, обеспечивает комплексную и всестороннюю защиту веб-трафика. При обработке веб-запросов пользователей McAfee Web Gateway сначала проверяет их на соответствие принятым в организации правилам использования Интернета. Затем с помощью локальных и глобальных технологий выполняется

McAfee
Together is power.

анализ разрешенных к просмотру веб-страниц с целью проверки как их содержимого, так и находящегося в них активного кода, благодаря чему обеспечивается немедленная защита от вредоносных программ и других скрытых угроз. Однако в отличие от базовых методов проверки пакетов устройство McAfee Web Gateway способно осуществлять проверку трафика SSL (Secure Sockets Layer), обеспечивая тем самым глубинную защиту от вредоносного кода и недопустимых приложений, замаскированных с помощью шифрования.

Благодаря защите входящего трафика снижаются также уровни риска в тех организациях, на серверах которых размещены веб-сайты, принимающие данные или документы из внешних источников. В таком случае McAfee Web Gateway в режиме обратного проксирования сканирует все получаемое содержимое еще до его загрузки на сервер, что позволяет обеспечить безопасность как сервера, так и содержимого.

Для обеспечения безопасности исходящего трафика в McAfee Web Gateway используется передовая технология McAfee для предотвращения утечки данных, позволяющая сканировать генерируемый пользователем контент по всем основным веб-протоколам: HTTP, HTTPS, FTP и др. Кроме того, она защищает организацию от утечки конфиденциальной, важной и регламентированной информации, покидающей пределы организации через сайты социальных сетей, блоги, вики-ресурсы или офисные веб-приложения: веб-почту, органайзеры, календари и т. п. Помимо этого, McAfee Web Gateway предотвращает случаи несанкционированного вывода данных за пределы организации через «зараженные ботом» компьютеры, пытающиеся связаться с узлами бот-сети или передать конфиденциальные данные.

McAfee Web Gateway — лучшее из имеющихся в отрасли средств защиты

В этом средстве веб-защиты, занимающем первое место[1] по показателям защиты от вредоносных программ, реализован запатентованный бессигнатурный метод анализа намерений с помощью антивирусного ядра McAfee Gateway Anti-Malware Engine. Функция упреждающего анализа намерений в режиме реального времени проверяет веб-трафик на наличие ранее не встречавшегося вредоносного контента и отфильтровывает эти угрозы «нулевого дня». Сканируя активное содержимое веб-страницы, проводя эмуляцию и анализ его поведения и прогнозируя его дальнейшие действия, McAfee Web Gateway препятствует доставке на конечные точки вредоносных программ «нулевого дня» и тем самым способствует резкому сокращению расходов на очистку и восстановление систем.

Такой анализ в сочетании с антивирусом McAfee и разработанными в McAfee Labs технологиями глобального сбора информации о репутации дает нам возможность быстро блокировать известное вредоносное ПО и известные вредоносные сайты. Использование большого числа разных технологий дает McAfee Web Gateway возможность обеспечивать более высокий уровень защиты, оптимизируя систему безопасности на единой платформе с помощью различных и вместе с тем дополняющих друг друга технологий. Именно этого требуют многие организации для реализации своих стратегий многослойной защиты.

- **Антивирус McAfee в режиме реального времени анализирующий репутацию файлов с помощью McAfee Global Threat Intelligence (McAfee GTI).** Возможность проверки репутации файлов с помощью облачной технологии McAfee GTI позволяет ликвидировать временной разрыв между моментом обнаружения вируса и моментом обновления/защиты системы.
- **Анализ репутации веб-сайтов и их категоризация с помощью McAfee GTI.** McAfee Web Gateway имеет функции веб-фильтрации и веб-защиты, в которых используется эффективное сочетание методов фильтрации как на основе репутации, так и на основе категорий. Сначала на основе сотен

различных атрибутов, получаемых лабораторией McAfee Labs с помощью средств массового сбора данных по всему миру, служба McAfee GTI создает перечень всех интернет-объектов (веб-сайтов, адресов электронной почты и IP-адресов). Затем она присваивает каждому объекту показатель репутации, отражающий тот уровень риска, который представляет данный объект. Это дает администраторам возможность создавать детально настраиваемые правила для определения того, что допускать, а что отклонять.

- **Географическое местонахождение.** McAfee Web Gateway включает в себя функцию определения географического положения, позволяющую отслеживать географические данные (например, о стране происхождения веб-трафика и местонахождения пользователя) и использовать эти данные в управлении политиками.

При использовании как категорий, так и показателей репутации веб-сайтов у организаций с недавнего времени появилась возможность выбирать, по какой базе данных осуществлять поиск: по локальной или по облачной. Можно также совмещать оба варианта. Поиск по облачной базе данных дает возможность избавиться от периодов незащищенности между моментом обнаружения угрозы или изменения и моментом обновления системы. Кроме того, он отличается особой широтой охвата, поскольку предоставляет доступ к данным о сотнях миллионов уникальных образцов вредоносных программ.

Интеграция с анализом сложных угроз
McAfee Web Gateway интегрируется с McAfee Advanced Threat Defense — нашей передовой технологией обнаружения вредоносных программ, представляющей собой сочетание настраиваемой изолированной среды («песочницы») с механизмом глубокого статического анализа кода. McAfee Advanced Threat Defense в сочетании с функциями линейного сканирования, за которые в McAfee Web Gateway отвечает антивирусный модуль Gateway Anti-Malware Engine, позволяет получить самое надежное из имеющихся на рынке средств защиты от угроз безопасности, распространяемых посредством Интернета. Организации, которым требуется менее затратный, упрощенный вариант решения для анализа сложных угроз, могут провести интеграцию со службой McAfee Cloud Threat Detection — облачной «песочницей» с целым рядом дополнительных уровней анализа угроз безопасности.

Обмен информацией об угрозах
На сегодняшний день многие средства защиты работают изолированно друг от друга и не предназначены для обмена информацией об угрозах, хотя такая информация может быть предоставлена средствами защиты конечных точек и сетей, системой управления информацией о безопасности и событиями безопасности (SIEM), шлюзом и т. д. Обмен информацией об угрозах позволяет повысить уровень защиты от угроз, лучше выявлять случаи нарушения безопасности и оптимизировать процесс реагирования на инциденты путем эффективного восстановления взломанных систем. Решения McAfee, в том числе McAfee Web Gateway, обмениваются друг с другом информацией об угрозах с помощью системы McAfee Threat Intelligence Exchange. Роль McAfee Web Gateway в этом процессе очень велика: создавая и рассылая информацию о репутации файлов вредоносного ПО «нулевого дня», обнаруживаемых с помощью антивирусного модуля Gateway Anti-Malware Engine, решение дает, например, возможность обеспечивать защиту устройств в конечных точках, не дожидаясь выпуска нового DAT-файла. А информация об угрозах, предоставляемая системой McAfee Threat Intelligence Exchange, дает McAfee Web Gateway возможность блокировать еще больше угроз безопасности.

Сбор информации и обеспечение защиты внутри зашифрованного трафика
С недавнего времени в качестве лазейки, позволяющей проникать сквозь защитные барьеры компаний, изощренные киберпреступники начали использовать

трафик SSL (HTTPS и HTTP/2). Ирония заключается в том, что созданный для обеспечения безопасности протокол тоже приходится проверять на надежность. McAfee Web Gateway включает в себя функции обнаружения вредоносных программ, проверки SSL и проверки сертификатов, которые позволяют комплексно подойти к задаче проверки зашифрованного трафика.

Однако дополнительного оборудования для сканирования SSL приобретать не требуется: архитектура McAfee Web Gateway обеспечивает выполнение всех задач с помощью одного-единственного аппаратного или виртуального устройства. McAfee Web Gateway непосредственно сканирует весь SSL-трафик, что позволяет обеспечить безопасность, целостность и конфиденциальность зашифрованных транзакций.

Организации, желающие обеспечить более глубокую проверку трафика SSL, могут направить весь поток (или отдельные потоки) расшифровываемого трафика на имеющийся в McAfee Web Gateway интерфейс ответвления SSL (SSL TAP). Эта программная функция позволяет отправлять полное или частичное зеркало расшифрованного трафика SSL на обработку дополнительными защитными решениями, такими как системы предотвращения вторжений (IPS) и сетевые системы предотвращения утечек данных.

Предотвращение утечки данных
McAfee Web Gateway защищает организации от угроз, связанных с исходящим трафиком, например, от утечки конфиденциальной информации. Это достигается путем сканирования содержимого исходящего трафика по всем основным сетевым протоколам, включая SSL. Тем самым McAfee Web Gateway превращается в мощный инструмент, позволяющий предотвращать утечки интеллектуальной собственности, обеспечивать и документировать нормативно-правовое соответствие и собирать данные, необходимые для проведения компьютерно-технических экспертиз в случае нарушений безопасности. Используя возможности решения McAfee Data Loss Prevention (McAfee DLP), McAfee Web Gateway поддерживает встроенные готовые DLP-словари и дает возможность создавать пользовательские словари путем нахождения ключевых слов и (или) использования регулярных выражений.

Встроенные функции шифрования файлов позволяют защитить от несанкционированного доступа данные, загружаемые в облачные хранилища (файлообменные сайты и сайты для совместной работы), если организация пользуется такими сервисами. Пользователи не могут получать и просматривать данные в обход McAfee Web Gateway.

Защита пользователей, находящихся за пределами сети
Учитывая тот факт, что уровень распределенности и мобильности персонала возрастает день ото дня, все большую важность приобретают решения для фильтрации веб-содержимого и защиты от интернет-угроз, позволяющие автоматически переключаться между офисным и мобильным режимами работы. McAfee Client Proxy (агент клиента, защищенный от несанкционированного вмешательства) дает мобильным пользователям возможность автоматически проходить проверку подлинности и перенаправляет их к либо на локальный McAfee Web Gateway, расположенный в демилитаризованной зоне, либо в службу McAfee Web Gateway Cloud Service. Это позволяет принудительно применять к мобильным и удаленным пользователям политики доступа в Интернет и проводить полную проверку на наличие угроз, даже если пользователи входят в Интернет через публичный портал, например, в кафе, в гостинице или в иной точке доступа к WiFi.

Кроме того, McAfee Web Gateway дает компаниям возможность включить мобильные устройства в сферу действия корпоративных политик безопасности путем направления веб-трафика в McAfee Web Gateway. Благодаря нашим партнерам AirWatch и MobileIron, разрабатывающим средства управления мобильными устройствами, McAfee Web Gateway обеспечивает защиту мобильных устройств на базе Apple iOS и Google Android с помощью передовых технологий защиты от вредоносных программ и с помощью корпоративных политик фильтрации веб-трафика.

McAfee Web Gateway предоставляет максимальную свободу действий

В McAfee Web Gateway используется многофункциональный модуль создания и применения политик на основе правил, предоставляющий большую свободу действий. Для оптимизации процесса создания политик McAfee Web Gateway предлагает обширную библиотеку готовых правил, содержащих все типичные меры по реализации политик. Организации могут выбирать из набора различных правил, легко их изменять и делиться собственными правилами с другими пользователями в рамках нашего интернет-сообщества. Кроме того, уникальное сочетание критериев правил на основе контекста и списков общего доступа предоставляет опытным администраторам неограниченные возможности для решения проблем и оптимизации интернет-защиты. Возможность интерактивной трассировки правил упрощает процесс отладки правил.

McAfee Web Gateway позволяет контролировать не только локально развернутые, но и облачные приложения: его прокси-сервер обеспечивает детальный контроль за использованием веб-приложений. Организации могут использовать тысячи средств контроля за облачными веб-приложениями, при необходимости активируя или блокируя отдельные функции и осуществляя контроль над тем, кто и как использует веб-приложения. Вы хотите разрешить доступ к Dropbox, но запретить выгружать файлы? Запросто!

Принцип гибкости и контроля распространяется также на аутентификацию пользователей и их права доступа. McAfee Web Gateway поддерживает большое количество способов аутентификации, включая NTLM (NT LAN Manager), RADIUS (Remote Authentication Dial In User Service), AD (Active Directory)/LDAP (Lightweight Directory Access Protocol), eDirectory, аутентификацию с использованием файлов cookie, Kerberos и аутентификацию с использованием локальной базы пользователей. Используемый в McAfee Web Gateway механизм аутентификации дает администраторам большую свободу выбора при создании правил, позволяя, например, использовать несколько разных способов аутентификации. Так, например, McAfee Web Gateway может попытаться выполнить автоматическую аутентификацию и в зависимости от полученного результата запросить у пользователя регистрационные данные, использовать другой способ аутентификации, применить политику ограничения или просто отказать в доступе.

Дополнительный компонент McAfee Web Gateway Identity включает в себя соединительные модули (коннекторы) для осуществления единого входа (single sign-on — SSO) в сотни популярных облачных приложений. McAfee Web Gateway Identity дает возможность повысить уровень своей безопасности и сократить число звонков в службу поддержки с просьбой сменить пароль: пользователи получают в свое распоряжение особую панель SSO, позволяющую получать доступ к санкционированным облачным приложениям одним щелчком мыши. Поддержка соединительных модулей для запросов HTTP POST (самодиагностика после включения) и языка SAML (язык разметки декларации безопасности) позволяет охватить широкий диапазон приложений. Наличие соединительных модулей для инициализации учетных записей дает системным администраторам возможность создавать и удалять учетные записи пользователей в отдельных SaaS-приложениях (Software-as-a-Service).

Благодаря встроенной поддержке прокси-серверов потоковой передачи McAfee Web Gateway позволяет также контролировать доступ к потоковому контенту, что ведет к уменьшению нагрузки на пропускной канал и сокращению времени задержки. Может быть применен дополнительный контроль пропускной способности с целью принудительной установки минимальных и максимальных значений, а также приоритизации определенных классов трафика, что позволяет организациям оптимизировать использование доступных ресурсов полосы пропускания.

Гибкая инфраструктура и высокий уровень быстродействия благодаря McAfee Web Gateway

McAfee Web Gateway представляет собой прокси-сервер корпоративного класса с высоким уровнем быстродействия, предлагаемый в виде масштабируемого семейства моделей аппаратных устройств с интегрированной функцией обеспечения высокого уровня доступности, поддержкой вариантов виртуализации и гибридного развертывания посредством McAfee Web Gateway Cloud Service. McAfee Web Gateway дает организациям свободу выбора вариантов развертывания и высокий уровень быстродействия, а также обеспечивает масштабируемость, позволяющую работать с сотнями тысяч пользователей в одной-единственной среде.

Более того, эти варианты развертывания можно сочетать между собой. Например, весь веб-трафик пользователей, находящихся внутри сети организации, можно направлять на локально развернутый шлюз, а веб-трафик всех пользователей, находящихся за пределами сети, — в облачную службу: это позволит кардинально сократить расходы на обратную передачу трафика по каналам многопротокольной коммутации пакетов (MPLS) или по виртуальной частной сети (VPN). Наличие автоматизированных процессов синхронизации политик и генерирования отчетов, касающихся гибридных (локальных и облачных) развертываний, помогает оптимизировать управление, обеспечить единообразное применение политик и упростить порядок формирования отчетов, отслеживания событий и расследования инцидентов.

McAfee Web Gateway предлагает большое количество параметров установки — от явного указания прокси-сервера до выбора режимов прозрачного моста и маршрутизатора, — поэтому поддержка вашей сетевой архитектуры гарантирована.

Благодаря поддержке большого числа стандартов интеграции McAfee Web Gateway идеально подойдет для работы в любом сетевом окружении. McAfee Web Gateway эффективно взаимодействует с другими сетевыми и защитными устройствами, используя целый ряд разных протоколов: Web Cache Communication Protocol (WCCP), WebSocket, Socket Secure (SOCKS), Internet Content Adaptation Protocol (ICAP) и др.

Кроме того, McAfee Web Gateway поддерживает протокол IPv6, что помогает крупным организациям и федеральным ведомствам обеспечивать соответствие нормативно-правовым требованиям. McAfee Web Gateway обеспечивает взаимодействие между внутренними сетями с IPv4 и внешними сетями с IPv6 и применяет к трафику все доступные функции защиты и сетевой инфраструктуры.

Единая платформа для будущего

McAfee Web Gateway объединяет в себе большое количество разных средств защиты, что избавляет вас от необходимости приобретать целый ряд отдельных продуктов. Единая аппаратно-программная архитектура включает в себя функции фильтрации URL-адресов, защиты от вирусов и вредоносных программ «нулевого дня», сканирования SSL-трафика (Secure Sockets Layer), предотвращения утечки данных и централизованного управления. Управление шлюзом унифицировано для всех вариантов его развертывания, т. е. одну и ту же политику можно применить и к локально развернутым аппаратным шлюзам, и к кластерам аппаратных шлюзов, и к виртуальным шлюзам, и к облачной службе. А осуществляется это с помощью одной-единственной консоли управления.

Управление рисками безопасности и отчетность

McAfee Web Gateway поддерживает программное обеспечение McAfee ePolicy Orchestrator® (McAfee ePO™) — популярную и признанную технологию управления средствами защиты, способную служить единым источником отчетов по всем аспектам безопасности.

Программное обеспечение McAfee ePO с помощью модуля McAfee Content Security Reporter поддерживает генерирование подробных отчетов о состоянии веб-трафика. McAfee Content Security Reporter предоставляет в ваше распоряжение информацию и инструменты технико-криминалистической экспертизы, позволяющие определять то, как ваша организация использует Интернет, а также выполнять нормативно-правовые требования, выявлять тенденции, изолировать проблемы и настраивать параметры фильтрации в соответствии с вашими политиками использования Интернета. Для снижения нагрузки на имеющейся сервер McAfee ePO модуль McAfee Content Security Reporter использует внешний автономный сервер, на котором выполняются ресурсоемкие функции обработки и хранения данных. Это дает такой уровень масштабируемости, который позволяет удовлетворить потребности самых крупных международных корпораций.

Кроме того, McAfee Web Gateway интегрируется со службой McAfee Cloud Visibility — Community Edition, доступ к которой предоставляется клиентам, использующим использующим продукты McAfee для предотвращения утечки данных, шифрования и веб-защиты. Эта бесплатная служба позволяет собирать информацию об объеме и риске использования облачных приложений. Дело в том, что ИТ-подразделениям известна лишь часть облачных приложений, используемых сотрудниками их организаций, и такая нехватка информации является источником риска. Проблема решается с помощью простой панели мониторинга, позволяющей отслеживать доступ ко всем облачным приложениям, связанные с этими приложениями уровни риска и уровни конфиденциальности данных. Сэкономленное время специалисты по информационной безопасности могут посвятить выполнению своей основной задачи — защите передаваемых в облако данных и контролю доступа к облачным приложениям, что позволит снизить уровень риска в организации.

Бесплатная служба McAfee Cloud Visibility — Community Edition входит также в состав службы McAfee Cloud Data Protection, являющейся следующим этапом защиты данных в облаке.

Лицензирование

Для достижения максимальной гибкости развертывания и долговременной эффективности ваших инвестиций компания McAfee предлагает все функции McAfee Web Gateway и McAfee Web Gateway Cloud Service в одном комплекте под названием **McAfee Web Protection**. Это решение можно развернуть локально, в облаке или в виде гибрида первых двух вариантов. Гибридный вариант даст вам дополнительную гибкость и обеспечит высокий уровень доступности. Выбор за вами! При любом варианте вы получите удостоенную наград защиту от вредоносных программ и комплексную веб-фильтрацию McAfee.

Аппаратное обеспечение McAfee Web Gateway приобретается отдельно.

1. В ходе испытаний, проведенных компанией AV-TEST, аппаратное устройство McAfee Web Gateway обнаружило 94,5 % вредоносных программ «нулевого дня», 99,8 % вредоносных файлов в формате переносимого исполняемого (PE) кода для Windows 32 и 98,63 % файлов в других форматах (не PE). «**McAfee Web Gateway Security Appliance Test**» (Тестирование защитного аппаратного устройства McAfee Web Gateway), AV-TEST GmbH.

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

Июнь 2017 г.