McAfee Next Generation Firewall

Ключевые преимущества

- Лучшая защита для вашего бизнеса и цифровых активов
- Блокирование попыток кражи данных с конечных точек
- Простота адаптации к конкретным потребностям в защите
- Легкость масштабирования по мере развития бизнеса
- Оптимизация производительности труда сотрудников и клиентов
- Снижает общую стоимость владения системой безопасности и сетевой инфраструктурой

Ключевые функции

- Средства защиты с функциями сбора и анализа информации об угрозах
- Защита данных от кражи на уровне приложений
- Усовершенствованные средства предотвращения обхода защиты
- Единое программное ядро
- Высокий уровень доступности инфраструктуры безопасности и сетевой инфраструктуры
- Мощные средства централизованного управления
- Встроенные функции IPsec VPN и SSL VPN

McAfee® Next Generation Firewall защищает сети предприятий при помощи высокопроизводительных средств безопасности, способных использовать информацию об угрозах и в реальном времени получать обновления от экосистемы Security Connected. Это позволяет компании Intel Security предоставлять лучшие в отрасли средства противодействия динамическим техникам обхода, а также комплексные решения на основе брандмауэра следующего поколения своевременно и именно там, где они необходимы — на удаленных объектах, в филиалах, в центрах обработки данных и на периферии сети.

McAfee Next Generation Firewall (McAfee NGFW) — это эффективное, расширяемое и легко масштабируемое централизованное решение. Его основу составляют надежные базовые средства защиты, обеспечивающие детальный контроль за приложениями, предотвращение вторжений (IPS), криптографическую защиту трафика (VPN) и углубленную проверку пакетов. Кроме того, мощные технологии противодействия обходу защиты осуществляют расшифровку и нормализацию трафика — до проверки и на всех уровнях протоколов — для обнаружения и блокирования наиболее сложных методов атаки.

Блокирование изощренных попыток кражи данных

Компании и организации в самых разных отраслях давно и регулярно сталкиваются с крупными случаями кражи данных. Теперь у них есть возможность успешно бороться с кражей данных путем защиты данных на уровне приложений. Это новое решение дает McAfee NGFW возможность выборочно и автоматически блокировать сетевой трафик, исходящий от компьютеров, ноутбуков, серверов, файловых ресурсов и других конечных устройств, на основе очень подробной контекстной информации о конечных точках. В деле предотвращения попыток кражи конфиденциальных

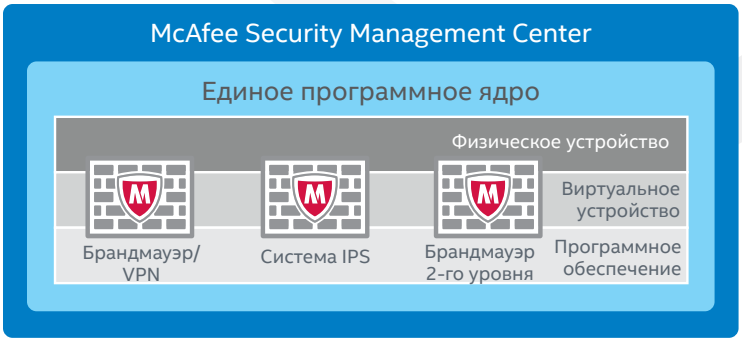

Рис. 1. McAfee NGFW поддерживает три разных функциональных роли и три варианта развертывания.

данных с конечных точек с помощью несанкционированных программ, веб-приложений, пользователей и каналов связи защита на уровне приложений является единственным решением, позволяющим выйти за рамки возможностей обычных брандмауэров следующего поколения.

Высокий уровень гибкости позволяет своевременно реагировать на меняющиеся требования к системе безопасности

Единое программное ядро позволяет решению (McAfee NGFW) легко менять свою роль в обеспечении безопасности динамично развивающихся бизнес-сред. Например, решение может выполнять функции брандмауэра/VPN, системы предотвращения вторжений или брандмауэра 2-го уровня. Также единое программное ядро способствует оптимизации плоскости данных, обеспечивая значительное повышение производительности независимо от своей роли или числа активных защитных функций. Еще большую гибкость дает возможность развертывания McAfee NGFW в различных форматах — в виде физического устройства, программного решения, виртуального устройства, а также виртуальных контекстов на физическом устройстве.

Высокий уровень масштабируемости и доступности для защиты важных для бизнеса приложений

Современный бизнес нуждается в полной отказоустойчивости решений, обеспечивающих безопасность сетей. McAfee NGFW обладает тремя мощными функциями, повышающими уровень масштабируемости и доступности.

- **Встроенная кластеризация в режиме «активный–активный».** Кластеризация обеспечивает более высокую производительность и отказоустойчивость при выполнении требовательных защитных приложений, таких как средства углубленной проверки пакетов и VPN. В кластер можно объединить до 16 узлов.
- **Незаметное переключение сеансов на другой ресурс при сбое.** Непревзойденный уровень доступности и удобства обслуживания систем безопасности. McAfee NGFW поддерживает незаметное переключение сеансов даже в том случае, если в пределах одного кластера используется много разных версий программного и аппаратного обеспечения.
- **McAfee Multi-Link.** Обеспечивает высокий уровень доступности сетевых соединений и соединений по IPsec VPN. Благодаря этой функции вы сможете быть уверены в постоянной защите и высокой производительности при любом развертывании решения.

Непревзойденная защита для бизнеса

Злоумышленники с каждым днем находят новые возможности проникновения в сети предприятий, приложения, центры обработки данных и конечные точки. Преодолев защиту, они могут похитить интеллектуальную собственность, информацию о клиентах и другие конфиденциальные данные, нанося непоправимый вред коммерческой деятельности и репутации компании. Некоторые злоумышленники используют динамические техники обхода (advanced evasion techniques — AET), позволяющие уклоняться от большинства современных устройств безопасности. Техники AET позволяют доставлять вредоносные программы по частям. Для доставки отдельных частей используются разные уровни сети или разные сетевые протоколы, при этом сами части кода маскируются и запутываются. Попав внутрь сети, вредоносный код собирается в единое целое и находит место, где можно спрятаться. После этого он на протяжении дней, месяцев или даже лет пересылает за пределы сети обнаруженные внутри сети конфиденциальные данные.

McAfee NGFW применяет к сетевому трафику методы обнаружения многоуровневых угроз, что позволяет с большой степенью точности выявлять приложения и пользователей и успешно применять политики безопасности в соответствии с принятыми в компании правилами. Решение выполняет специализированную углубленную проверку пакетов с использованием таких передовых методов, как нормализация всего стека и проверка на основе горизонтального потока данных. Полно нормализуя потоки трафика, эти методы дают McAfee NGFW возможность выявлять динамические техники обхода и аномалии трафика, пропускаемые другими брандмауэрами следующего поколения. Надлежащая проверка трафика на наличие угроз и вредоносных программ по всем протоколам и уровням возможна только после его полной нормализации. Только McAfee NGFW успешно прошел тестирование на обнаружение более чем 800 млн динамических техник обхода.

Знание — сила!

Изолированные решения для обеспечения безопасности ограничивают обмен информацией, что снижает их способность распознавать и блокировать угрозы. Экосистема обнаружения угроз Security Connected позволяет быстро обмениваться обширной информацией об угрозах, обновляемой в режиме реального времени, благодаря чему организации могут успешно применять в борьбе с киберпреступностью новейшие знания об угрозах, собираемые в глобальном и локальном масштабе. Security Connected дает McAfee NGFW возможность эффективно использовать информацию об угрозах, полученную из широкого спектра сторонних источников, а также от других защитных решений McAfee, в частности перечисленных ниже.

- **McAfee Endpoint Intelligence Agent (McAfee EIA).** Для защиты данных на уровне приложений в McAfee NGFW используется очень подробная информация о пользователях и клиентских приложениях на конечных точках, поступающая от McAfee EIA. Сочетая эту информацию о конечных точках с информацией о сетевых угрозах, McAfee NGFW имеет возможность блокировать соединения, исходящие от несанкционированных и подозрительных комбинаций процессов, протоколов и пользователей.
- **Программное обеспечение ePolicy Orchestrator®.** Это решение позволяет McAfee Next Generation Firewall получать контекстную информацию от пользователей и узлов, что дает ценное представление об уровне защищенности конечных точек. Эту информацию можно также использовать для упрощения рабочих процессов при устранении неполадок или исследовании угроз и проблем.
- **McAfee Enterprise Security Manager.** Эта система осуществляет непрерывный мониторинг и оповещение о состоянии нормативно-правового соответствия, что дает возможность контролировать ситуацию в режиме реального времени, повышает уровень защищенности и сокращает время реагирования на события.
- **McAfee Advanced Threat Defense.** Этот продукт обеспечивает превосходную защиту от угроз «нулевого дня» при помощи динамического анализа вредоносных программ в «песочнице» и статической проверки подозрительного кода. Интеграция с McAfee Advanced Threat Defense также позволяет McAfee NGFW передавать проверку подозрительных файлов другой системе для быстрой оценки угроз без снижения производительности сети.

- **McAfee Global Threat Intelligence.** Дает брандмауэру McAfee NGFW возможность получать высококачественную информацию о репутации файлов, необходимую для защиты от сложных угроз и вредоносных программ, действующих в глобальных масштабах.

Экосистема Security Connected в сочетании с гибкостью McAfee Next Generation Firewall позволяет динамично развивающимся предприятиям легко и быстро развертывать многоуровневые защитные решения именно там, где они необходимы.

Полнофункциональный механизм централизованного управления позволяет повысить эффективность работы и снизить совокупную стоимость владения

Стремление сдерживать расходы и оптимизировать использование ресурсов требует от современных компаний повышения уровня эффективности операций по обслуживанию сети и обеспечению безопасности. McAfee Security Management Center обеспечивает централизованное управление и сбор информации обо всех ролях и функциях решения McAfee NGFW. McAfee Security Management Center глубоко анализирует приложения, трафик пользователей и содержимое в общем доступе. Наличие интуитивно понятного графического пользовательского интерфейса упрощает работу по настройке, администрированию и мониторингу всей системы, ведет к снижению эксплуатационных расходов и дает компании возможность уделять основное внимание развитию собственного бизнеса.

Варианты лицензирования

Мы предлагаем две отдельные лицензии, позволяющие учесть и спрос на гибкость, и необходимость соблюдения бюджетных ограничений.

- **Лицензия McAfee NGFW — NGF.** Для организаций, которым нужны разные эксплуатационные режимы с полной пропускной способностью, виртуальными контекстами, антивирусной защитой и полной углубленной проверкой пакетов. Данная лицензия позволяет использовать следующие три функциональных роли:
  - брандмауэр/VPN (3-й уровень);
  - режим IPS (2-й уровень);
  - брандмауэр 2-го уровня.
- **Лицензия McAfee NGFW — FWL.** Для организаций, которым необходим только один эксплуатационный режим с некоторыми ограничениями, касающимися пропускной способности и возможностей проверки трафика. Данная лицензия позволяет использовать только функциональную роль «Брандмауэр/VPN (3-й уровень)».

Важные примечания.

- Подробная информация о лицензировании приведена в информационном листке **«Варианты лицензирования и функциональные роли McAfee Next Generation Firewall»** (**mcafee.com/ngfw-specs**).
- Некоторые аппаратные устройства McAfee Next Generation Firewall для СМБ можно приобрести только с лицензией McAfee NGFW — FWL.

Технические характеристики McAfee Next Generation Firewall

Поддерживаемые платформы	
Устройства	Многочисленные варианты аппаратных устройств для разных сред (от филиала компании до центра обработки данных). Дополнительную информацию см. на страницах **«Сравнение аппаратных устройств NGFW-(FWL)»** и **«Сравнение аппаратных устройств NGFW-(NGF)»**.
Программное устройство	Системы на основе x86
Виртуальное устройство	Поддержка VMware ESX, Oracle VM и KVM
Поддерживаемые роли	С лицензией NGF: Брандмауэр/VPN (3-й уровень), режим IPS (2-й уровень), брандмауэр 2-го уровня С лицензией FWL: Брандмауэр/VPN (3-й уровень)
Виртуальные контексты (только лицензия NGF)	Виртуализация для разделения логического контекста (брандмауэр, IPS или брандмауэр 2-го уровня) с отдельными интерфейсами, системами адресов, маршрутизацией и политиками
Функциональная роль «Брандмауэр/VPN»	
Общие	Фильтрация пакетов с отслеживанием и без отслеживания состояния, брандмауэр сеансового уровня сеанса с агентом протокола TCP-прокси
Проверка подлинности пользователей	Внутренняя база данных пользователей, LDAP, Microsoft Active Directory, RADIUS, TACACS+
Высокий уровень доступности	• Кластеризация брандмауэров в кластеры размером до 16 узлов в режиме «активный–активный»/«активный–резервный» • Сохранение состояния соединений (включая VPN-соединения) • VRRP • Выравнивание серверной нагрузки • Агрегирование каналов (802.3ad) • Обнаружение отказа соединения
Множественная адресация с использованием нескольких интернет-провайдеров	McAfee Multi-Link: высокая отказоустойчивость и выравнивание нагрузки между разными интернет-провайдерами, включая VPN-соединения, агрегирование VPN-каналов при использовании McAfee Multi-Link, выбор каналов в зависимости от качества обслуживания
Назначение IP-адресов	• Кластер брандмауэров: статические, IPv4, IPv6 • Брандмауэры на отдельных узлах: статический, DHCP, PPPoA, PPPoE, IPv4, статический IPv6 • Службы: DHCP-сервер и DHCP-ретрансляция для IPv4
Преобразование адресов	• IPv4, IPv6 • Статическое NAT, NAT для адреса источника с помощью трансляции порт-адрес (PAT), NAT для адреса назначения с помощью PAT
Маршрутизация	Статические маршруты для IPv4 и IPv6, маршрутизация на основе политик, статическая многоадресная маршрутизация
Динамическая маршрутизация	Прокси для IGMP, RIPv2, RIPng, OSPFv2, OSPFv3, BGP, PIM-SM
IPv6	IPv4/IPv6, ICMPv6, DNSv6 с двойным стеком
SIP	Динамический пропуск медиа-потоков, передаваемых по RTP, обход NAT, внимательное отслеживание, взаимодействие с SIP-устройствами, отвечающими требованиям RFC 3261
Перенаправление на сервер проверки содержимого	Перенаправление протоколов HTTP, FTP, SMTP на сервер проверки содержимого (Content Inspection Server — CIS)
IPSec VPN	
Протоколы	IKEv1, IKEv2, IPsec с IPv4 и IPv6
Шифрование	AES-128, AES-256, AES-GCM-128, AES-GCM-256, Blowfish, DES, 3DES[1]
Алгоритмы представления сообщений в краткой форме	AES-XCBC-MAC, MD5, SHA-1, SHA-2-256, SHA-2-512
Метод Диффи-Хеллмана	Группы Диффи-Хеллмана: 1, 2, 5, 14, 19, 20, 21
Аутентификация	Цифровые подписи на основе RSA, DSS, ECDSA с использованием сертификатов X.509, общие ключи, смешанный вариант, XAUTH, EAP
Другие	• Сжатие с помощью IPCOMP Deflate • NAT-T • Обнаружение неактивных участников • MOBIKE

Технические характеристики McAfee Next Generation Firewall (продолжение)

VPN типа «сеть–сеть»	• VPN на основе политик, VPN на основе маршрутизации (GRE, IP-IP, SIT) • Топологии: «звезда», полная сетка, частичная сетка • McAfee Multi-Link с динамическим выбором канала на основе нечеткой логики • Режимы многоканального подключения (McAfee Multi-Link): распределение нагрузки, активный/резервный, агрегирование каналов
VPN от клиента к шлюзу	• Клиент VPN для Microsoft Windows • Автоматические обновления конфигурации со шлюза • Автоматическая отработка отказа с помощью McAfee Multi-Link • Проверка безопасности клиентов • Защищенный вход в домен
SSL VPN (только лицензия NGF)	
Доступ через клиент	• Поддерживаемые платформы: Android 4.0, Mac OS X 10.7 и Windows Vista SP2 (и более новые версии)
Доступ через портал	• Доступ к OWA и интрасети через портал SSL VPN с использованием браузера
Защита от нежелательных сообщений	
Сканируемые протоколы	SMTP
Ядро	Обнаружение нежелательных сообщений с использованием рейтинга
Методы фильтрации	• Настраиваемые функции сопоставления информации в конвертах, заголовках и содержимом электронной почты • Локальная защита от спуфинга и ретрансляция • Фильтр-ловушка для нежелательных сообщений • Сопоставление SPF-записей и MX-записей • Черные списки на основе DNS
Функциональные роли «Режим IPS» и «Брандмауэр 2-го уровня» (только лицензия NGF)	
Общие	• Фильтрация пакетов без отслеживания состояния для протоколов Ethernet (DIX/IEEE) • Фильтрация пакетов с отслеживанием состояния для протоколов IP • Сопоставление логических интерфейсов для виртуальных локальных сетей и физических интерфейсов • Повторная маркировка VLAN • Фильтрация по MAC-адресам
Управление доступом	• IPv4 и IPv6 • Туннелированный IP • IP in IP • Инкапсуляция IPv6 • GRE
Высокий уровень доступности	• Кластеризация брандмауэров 2-го уровня («активный–активный») • Кластеризация систем обнаружения вторжений («активный–активный»/«активный–пассивный») • Серийная кластеризация систем предотвращения вторжений («активный–активный») • Поддержка интерфейса открытия при отказе (режим IPS) • Динамическое устранение перегрузки при проверке (режим IPS)
Общие функции (все функциональные роли)	
Инкапсуляция	Ethernet, 802.1q VLAN, PPPoA[2], PPPoE[2]
Расширенное управление доступом	• Зоны интерфейсов • Время • Информация по TLS • Доменные имена • Информация о пользователе • Сетевые приложения • Клиентские приложения: информация о приложениях на узле поступает от McAfee Endpoint Intelligence Agent (только лицензия NGF)
Управление трафиком и контроль качества обслуживания (QoS)	• Управление скоростью трафика на основе политик • Назначение приоритета пропускной способности: гарантированная/максимальная • Сопоставление/маркирование точек DSCP • Ограничение количества одновременных сеансов на основе политик • Переопределение значения MSS в пакетах TCP на основе политик

Технические характеристики McAfee Next Generation Firewall (продолжение)

Проверка	
Защита от бот-сетей	• Обнаружение угроз путем дешифровки трафика • Обнаружение угроз путем анализа последовательности длин сообщений
Динамическое обнаружение контекста	Протокол, приложение, тип файла
Передовая защита от вредоносных программ	Фильтрация файлов на основе политик
McAfee Advanced Threat Defense	Анализ в изолированной среде («песочнице») и статический анализ кода: файлы PE, файлы Adobe, файлы Microsoft Office, архивы, файлы Java, файлы Android Application Package
McAfee Global Threat Intelligence	Классификация с помощью облачной службы оценки репутации файлов
McAfee Anti-Malware Engine	Сканируемые протоколы: FTP, HTTP, HTTPS, POP3, IMAP, SMTP
Нормализация/проверка/обработка трафика отдельно по каждому протоколу[3]	Ethernet, H.323, GRE, IPv4, IPv6, ICMP, IP in IP, инкапсуляция IPv6, UDP, TCP, DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, MGCP, Modbus/TCP, MSRPC, NetBIOS Datagram, OPC Classic, OPC UA, Oracle SQL Net, POP3, POP3S, RSH, RSTP, SIP, SMTP, SSH, SunRPC, NBT, SCCP, SMB, SMB2, SIP, TCP Proxy, TFTP
Идентификация угроз независимо от протокола	Любой протокол TCP/UDP
Обнаружение попыток обхода защиты и аномалий	• Многоуровневая нормализация трафика • Цифровые отпечатки на основе анализа уязвимостей • Расширяемый программный модуль для проведения проверок • Регистрация попыток обхода защиты и аномалий
Самостоятельное получение цифровых отпечатков	• Сопоставление цифровых отпечатков независимо от протокола • Язык для получения цифровых отпечатков с использованием регулярных выражений • Преобразователь сигнатур Snort • Самостоятельное получение цифровых отпечатков приложений
Проверка TLS	• Расшифровка и проверка потока от HTTPS-клиента и HTTPS-сервера • Проверка сертификатов TLS • Список исключений на основе доменных имен сертификатов
Сопоставление (корреляция) данных	Локальное сопоставление данных, сопоставление данных на сервере регистрации событий
Защита от DoS/DDoS-атак	Обнаружение SYN-флуда и UDP-флуда Ограничение количества одновременных подключений, сжатие журналов (на основе интерфейса) Защита от методов, основанных на медленных HTTP-запросах
Разведка	Обнаружение случаев сканирования по протоколам TCP/UDP/ICMP, обнаружение случаев скрытого («стелс-сканирование») и медленного сканирования (IPv4 и IPv6)
Методы блокировки	Прямая блокировка, сброс подключения, включение в черный список (локальный или распределенный), HTML-ответ, перенаправление протокола HTTP
Запись трафика	Автоматическая запись трафика, запись случаев злоумышленного использования трафика
Обновления	• Автоматические динамические обновления с помощью McAfee Security Management Center • В настоящее время охвачено около 4 700 защищенных уязвимостей
Фильтрация URL-адресов	
Протоколы	HTTP, HTTPS
Ядро	Фильтрация URL-адресов по категориям Webroot, черные и белые списки
База данных	• Более 280 млн доменов верхнего уровня и подстраниц (миллиарды URL-адресов) • Техническая поддержка осуществляется на более чем 43 языках, по 82 категориям

Технические характеристики McAfee Next Generation Firewall (продолжение)

Управление и мониторинг	
Интерфейсы управления	Система корпоративного уровня для централизованного управления, ведения журналов и формирования отчетов; для получения дополнительной информации см. **лист данных по McAfee Security Management Center**. (**mcafee.com/smc**) Local Manager for enterprise.
Мониторинг по SNMP	SNMPv1, SNMPv2c и SNMPv3
Захват трафика	tcpdump в консоли, удаленный захват посредством McAfee Security Management Center
Надежно защищенная передача управляющих сообщений	256-разрядная защита сообщений между ядром и системой управления
Сертификаты в сфере безопасности	Common Criteria EAL4+, криптографический сертификат FIPS 140-2, сертификат CSPN от ANSSI (сертификация безопасности 1-го уровня)

[1] Набор поддерживаемых алгоритмов шифрования зависит от используемой лицензии.
[2] Относится только к роли «Брандмауэр/VPN».
[3] См. лицензионные ограничения брандмауэра.

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