Технологическая концепция

McAfee
An Intel Company

АНАЛИЗ СЕТЕВОГО ТРАФИКА

Устранение пробелов в администрировании и обеспечении безопасности

ЭТАЛОННАЯ АРХИТЕКТУРА SECURITY CONNECTED

УРОВЕНЬ 1 2 **3** 4 5

Security Connected

Разработанный компанией McAfee подход Security Connected позволяет интегрировать друг с другом большое количество разных продуктов, услуг и партнерских отношений, создавая возможность централизованно, эффективно и надежно снижать уровень риска. Основанный на мерах безопасности, проверенных на практике на протяжении более двадцати лет, подход Security Connected позволяет организациям любого размера, в любом регионе мира и в любой отрасли повысить свой уровень безопасности, оптимизировать систему защиты, снижая расходы на нее, и выполнить стратегическую интеграцию системы безопасности и бизнес-процессов организации. В эталонной архитектуре McAfee Security Connected предлагаются конкретные шаги от идей до их воплощения. С их помощью концепцию Security Connected можно адаптировать к конкретным рискам, инфраструктуре и коммерческим целям вашей организации. Компания McAfee непрерывно ведет поиск новых путей защиты своих клиентов.

Устранение пробелов в администрировании и обеспечении безопасности

Ситуация

Среднестатистический пользователь компьютера пользуется Интернетом около четырех часов в неделю. В месяц среднестатистический пользователь Интернета посещает 94 доменов и просматривает 2 905 страниц. Из них 830 — страницы Facebook.[1] Пик использования Интернета на рабочем месте приходится на обеденный перерыв.[2]

В результате генерируется сетевой трафик, имеющий неоднородный характер: часть его является вредоносной, часть безопасной, часть его генерируется в результате продуктивного труда, часть является пустой тратой пропускной способности, а часть его зашифрована. Часть трафика является откровенно опасной и может подвергнуть вашу организацию риску утечки данных. Как решить задачу классификации трафика, чтобы иметь возможность отделять вредоносное от безопасного среди гигабайтов данных, поступающих с тысяч разных веб-сайтов?

Описание проблемы

Сетевая безопасность в современном виде — это уже не только порты и протоколы. Сегодня это и проверка приложений, и анализ структуры трафика, и выявление замаскированных данных, и полный анализ данных. На сегодняшний день у вас есть возможность создавать правила, открывающие стандартные порты для тех или иных протоколов, а также выбирать, каким приложениям разрешать работать на этих портах. Неплохо, не правда ли?

Чем более эффективной становится ваша система безопасности, тем быстрее вы начинаете понимать взаимосвязь между приложениями, риском нарушения безопасности, использованием пропускной способности и уязвимостью. Во всех этих категориях важную роль играют пользователи, потому что наибольшая активность в сети инициируется именно ими. Вам нужна возможность видеть, какие приложения на самом деле запущены в вашей среде, возможность определять, каким приложениям следует разрешить запускаться, и возможность создавать для них точные правила. Имея все эти возможности, вы сможете использовать средства защиты для блокирования нежелательного трафика и повышения уровня быстродействия и эффективности ваших систем. Задача заключается в том, чтобы установить контроль над обменом информацией внутри сети и при этом обеспечить сбор информации о происходящем в сети. В конечном итоге вы сможете блокировать лишний трафик, повысить уровень своей защищенности, начать более эффективное использование пропускной способности и стать менее уязвимыми для угроз.

Подумайте об имеющейся у вас реализации системы безопасности: понижает ли она уровень быстродействия вашей сети? Не мешает ли она вам собирать информацию о происходящем? Возможные проблемы:

- **Нежелательный трафик.** Большая часть трафика идет через порты 80 (HTTP) и 443 (HTTPS). Если эти стандартные порты открыть для всего трафика, то нежелательные приложения и вредоносные программы смогут свободно попадать в вашу сеть и свободно ее покидать. Одним из основных упускаемых из виду аспектов является шифрование. Вредоносные программы и атаки обычно используют непроверяемый канал зашифрованного трафика HTTPS.
- **Не соответствующее политике или нежелательное поведение пользователей.** Первая задача, которая встает перед администраторами, это определить, какой тип сетевого трафика генерируется пользователями. Трафик может быть вредоносным (например, кража данных или разведка сети), неприемлемым и нарушающим политику (например, использование служб обмена файлами) или выходящим за рамки обычных бизнес-процессов (например, генерирование трафика в нерабочее время).
- **Потенциально опасные приложения.** У разных сетевых приложений (для использования социальных сетей, служб обмена мгновенными сообщениями, служб обмена файлами, одноранговых служб и др.) разные риски безопасности. Они могут ставить под угрозу данные и системные активы, влиять на производительность труда сотрудников и использовать пропускную способность сети.
- **Наличие нескольких администраторов с собственными приоритетами.** Администраторы средств защиты сети и администраторы средств защиты приложений нередко имеют разные подходы к обеспечению безопасности. Но преодолеть разрыв между этим двумя группами помогают новые технологии. Чтобы повысить уровень эффективности и безопасности сетей, этим двум группам теперь приходится взаимодействовать друг с другом и сопоставлять информацию. Так, например, чтобы узнать, какой пользователей был зарегистрирован в системе, которая установила соединение с сервером в другой стране и использовала потоки замаскированных данных, администраторы должны обменяться соответствующими данными.

Рис. 1. Для сбора информации о происходящем в сети необходимо использовать несколько видов анализа.

Факторы, влияющие на принятие решений

Ответы на следующие вопросы могут быть важны при построении архитектуры.

- Где вы собираетесь проводить проверку трафика с помощью IPS: на периметре или в ядре сети? Или и там, и там?
- Есть ли у вас входящий трафик SSL, который необходимо проверять?
- Сколько в вашей сети сегментов, для которых вы хотели бы обеспечить защиту и управление (внутренняя зона, VPN, демилитаризованная зона, PCI)?
- Какова рабочая пропускная способность вашей сети на данный момент?
- Позволяет ли имеющийся у вас на данный момент пакет средств защиты собирать информацию о репутации IP-адресов, файлов и URL-адресов?

Описание решения

Специалисты по обеспечению сетевой безопасности постепенно отходят от старой практики закрепления тех или иных протоколов за стандартными портами и защиты конечных точек с помощью антивирусов. Теперь у вас есть возможность анализировать сетевой трафик и выявлять все угрозы. Вы можете видеть, что происходит в сети, и измерять, насколько успешно вы защищаете свою среду.

Раньше вас, наверно, раздражала невозможность полностью проследить, как изменения в трафике и методах обеспечения безопасности влияют на уровень быстродействия. У вас, вероятно, не было возможности блокировать нежелательные приложения или проводить углубленный анализ взаимодействия всех объектов в вашей сети. Вы, возможно, сталкивались с проблемой поиска события или приложения, ставшего причиной уязвимости.

Сегодня у вас есть возможность повысить уровень операционной эффективности и сетевой безопасности благодаря оптимизированным методам внедрения защитных продуктов и обеспечения безопасности, к которым, среди прочего, относится продуманное использование средств защиты и аналитических инструментов.

Использование средств защиты, помогающих автоматизировать проверку вредоносных программ благодаря более подробному сбору информации о происходящем в сети, поможет вам стабилизировать свою операционную среду и повысить уровень эффективности своего бизнеса. С их помощью вы сможете получить полное представление обо всех взаимосвязях между пользователями, приложениями и адресами назначения, благодаря чему внедрение и обслуживание любой технологии «следующего поколения» не истощит имеющиеся у вас ресурсы.

McAfee рекомендует использовать разные уровни защиты в разных точках сети. По периметру сети защиту обеспечивает брандмауэр следующего поколения. Брандмауэр проводит углубленную проверку трафика и применяет политики, позволяющие снизить риски, связанные с исходящим трафиком. Этот брандмауэр поможет вам блокировать современные атаки благодаря наличию таких функций, как:

- сбор информации о приложениях, позволяющий определять, какие в среде запущены приложения и какие из них используют пропускную способность сети;
- сбор информации об идентификационных данных пользователей, дающий администраторам возможность контролировать, какой трафик приложений может быть сгенерирован тем или иным идентификатором пользователя. Такой метод зарекомендовал себя в случаях, когда разрешение на запуск приложений нужно дать только некоторым пользователям, не используя названия конкретных систем и их IP-адреса;
- анализ репутации файла (содержимое) и источника (соединение), позволяющий заблокировать нежелательный трафик и уменьшить количество времени, которое администраторам приходится тратить на изучение входящих и исходящих соединений в своей среде;
- контроль за тем, какие пользователи могут генерировать трафик на уровне приложений, независимо от того, с какого устройства пользователь входит в систему.

Внутри сети за защиту отвечает система предотвращения вторжений в сеть (IPS). Она поможет вам выявлять и снижать входящие и исходящие риски до того, как угрозы достигнут намеченных целей. Система IPS отфильтровывает опасный и вредоносный входящий трафик и снижает объем трафика, подлежащего углубленной проверке. Она должна:

- защищать от известных и неизвестных угроз с помощью сигнатур, данных о репутации и поведенческого анализа;
- обеспечивать защиту от атак DoS и DDoS для поддержки высокого уровня доступности сети;
- расшифровывать трафик SSL для проверки на наличие замаскированных угроз.

Что касается ядра сети, то здесь IPS тоже может помочь защитить самые важные активы предприятия. IPS поможет вам выявить внутренние атаки, берущие начало во внутренней сети и нацеленные на активы предприятия (например, на базы данных). Она может:

- защитить от известных и неизвестных угроз с помощью сигнатур, данных о репутации и поведенческого анализа;
- защитить ядро сети от неизвестных вредоносных программ, проникающих во внутреннюю сеть на мобильных носителях (например, на ноутбуках).

Технологии, используемые в решении McAfee

За выполнение этих требований в решении McAfee отвечают два основных компонента: McAfee® Firewall Enterprise и McAfee Network Security Platform, наша сетевая система IPS. У McAfee Firewall Enterprise и у аппаратного устройства McAfee IPS есть дополнительные функции для оптимизации сбора информации о том, что происходит в сети. С помощью McAfee SIEM и других дополнительных продуктов можно расширить объем собираемой и анализируемой информации, включив в него больше аспектов сетевого трафика.

- **McAfee Firewall Enterprise** позволяет обнаруживать и контролировать приложения, а также обеспечивает защиту от атак эпохи Веб 2.0 с помощью широкого набора функций:
  - **McAfee AppPrism®** дает возможность собирать информацию о приложениях, используемых в сети. Эта функция может распознать приложение на основе сигнатур приложений и результатов наблюдения за его протоколом и данными. AppPrism распознает такие характерные для приложения признаки, как комбинация данных и протокол, а в большинстве случаев также стандартные или ожидаемые порты. Данная функция обеспечивает защиту от приложений, контролируя или блокируя приложения, способные находить открытые порты (например, Skype и TeamViewer). Она может также расшифровывать и проверять зашифрованный трафик. Когда приложение определено (с помощью сигнатур), к нему применяется политика. В зависимости от заданных правил используются дополнительные средства защиты или другие функции обеспечения безопасности, например, проверка на наличие вредоносных программ. Работающая в режиме реального времени служба McAfee Global Threat Intelligence™ помогает брандмауэру анализировать меняющиеся уровни риска содержимого, соединений и приложений.
  - **McAfee Control Center** представляет собой факультативную консоль управления для Firewall Enterprise. Она облегчает процесс управления одним или несколькими брандмауэрами, предоставляя администраторам возможность создавать правила брандмауэра и сразу же рассылать их на все брандмауэры. Control Center становится центральной консолью управления всеми имеющимися в сети брандмауэрами McAfee, сокращая необходимость повторно создавать и развертывать политики.
- **McAfee Network Security Platform (NSP)** выполняет углубленную проверку пакетов, позволяющую получить всю информацию по каждому соединению. Она выявляет угрозы с помощью сигнатур и путем анализа поведения. Как и McAfee Firewall Enterprise, NSP распознает и проверяет приложения с помощью AppPrism. У системы IPS есть единая консоль управления, McAfee Network Security Manager (NSM), с помощью которой можно управлять одним или несколькими устройствами IPS, а также дополнительные компоненты, расширяющие ваши возможности сбора информации о происходящем в сети и повышающие скорость вашего реагирования на происходящее.
  - **McAfee Network Threat Behavior Analysis (NTBA)** позволяет собирать больше информации о потоках сетевого трафика в режиме реального времени и дает вам возможность обнаруживать в сети объекты, ведущие себя ненормально. Собрав информацию о том, какое поведение является нормальным, а какое аномальным, NTBA устанавливает пороговые значения, а при превышении этих порогов рассылает оповещения. Вместе с оповещением администратор получает подробный отчет и может с помощью панели управления немедленно начать расследование инцидента.
  - **McAfee Network Threat Response (NTR)** декодирует замаскированный трафик и обеспечивает анализ трафика потока в режиме реального времени. Кроме того, NTR позволяет обнаруживать атаки, скрытые в файлах распространенных форматов (PDF, форматы Microsoft Office и т. п.).

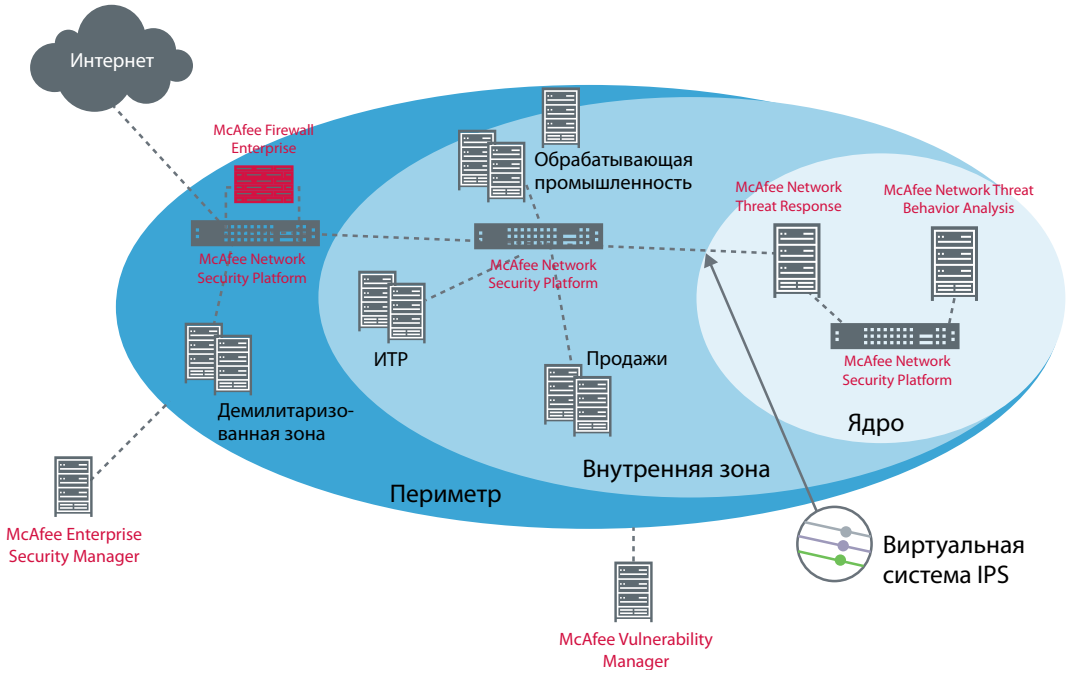

Рис. 2. В типичной модели развертывания продукты McAfee создают несколько уровней защиты в каждой зоне сети, а SIEM обеспечивает сопоставление событий для получения единой картины происходящего.

Интеграция с дополнительными решениями

Предлагаемое компанией McAfee решение в категории SIEM называется McAfee Enterprise Security Manager (ESM). Его можно использовать для анализа данных, сопоставления событий и отслеживания тенденций. McAfee ESM дает администраторам возможность сопоставлять события, получаемые от брандмауэра и из других источников данных в среде. С помощью этой системы SIEM вы можете выявить основную причину проблемы, не тратя огромное количество времени на проведение исследований и экспертиз. Сопоставив трафик приложений по всем сетевым событиям и отобрав взаимосвязанные инциденты, она может дать вам информацию о таких подробностях, как объем трафика, генерируемого каждым приложением, и тенденции трафика. Данные, собираемые и сопоставляемые системой McAfee ESM, помогают специалистам по расследованию инцидентов быстро получать полную картину событий.

McAfee Vulnerability Manager позволяет получить оперативную, точную и полную картину уязвимостей на всех ваших активах, соединенных в сеть. Интеграция McAfee Vulnerability Manager и McAfee Network Security Manager дает администраторам возможность запускать поиск уязвимостей на внутренних узлах путем простого щелчка мышью по угрозе. Администратор будет видеть, является ли внутренний узел уязвимым для угрозы, обнаруженной платформой McAfee Network Security Platform. Если провести также интеграцию с McAfee ePolicy Orchestrator, то можно будет видеть, какие защитные продукты McAfee установлены на этом внутреннем узле. Это даст вам возможность определять, обновлены ли эти защитные продукты и требуются ли дополнительные меры безопасности для защиты узла от угроз. Если вы хотите еще больше повысить эффективность защиты, то мы предлагаем вам провести дополнительную интеграцию с рядом других решений McAfee для защиты конечных точек.

McAfee в действии

Взаимодействие этих систем дает вам возможность отслеживать и контролировать трафик в вашей сети. Для начала вы можете запустить McAfee AppPrism на брандмауэре, чтобы выяснить, какие приложения используются в вашей сети. В AppPrism есть каталог приложений, содержащий более 1 100 наименований (в том числе Facebook). Их он может определить сразу, как только они начинают генерировать трафик в сети. McAfee ежедневно обнаруживает новые приложения, и мы добавляем их в этот каталог.

Изучив свой каталог, вы, возможно, захотите использовать сразу несколько разных средств защиты. Контролировать сетевые подключения можно с помощью McAfee Firewall Enterprise. Для этого в нем используются правила брандмауэра, содержащие в том числе и блокировку приложений. AppPrism дает вам возможность контролировать приложения в Facebook на уровне функций. Вы можете, например, разрешить пользователям заходить в Facebook, но запретить им писать посты или пользоваться чатом. Благодаря интеграции идентификационных данных брандмауэр дает администраторам возможность создавать политики использования приложений для отдельных пользователей и вносить в них коррективы, привязывая отдельные меры безопасности к тем или иным группам пользователей.

Допустим, вы хотите, чтобы право размещать информацию в Facebook было только у небольшой группы пользователей из отдела маркетинга в рамках проведения кампаний в социальных сетях. В таком случае вы можете создать правило, которое будет распознавать этих пользователей из отдела маркетинга и разрешать им публиковать информацию. У всех же других пользователей функция публикации информации в Facebook будет заблокирована. Такие действия позволяют уменьшить площадь атаки путем сокращения количества потенциально опасных случаев использования приложений.

Для решения проблем, связанных с использованием приложений и их влиянием на пропускную способность сети, вам нужна более подробная информация, позволяющая не только идентифицировать приложения и создавать правила использования приложений пользователями. Вам необходимо знать, какой объем трафика генерирует каждое приложение, и отслеживать тенденции трафика. Отслеживать и анализировать этот трафик, сопоставляя события по всей сети, можно с помощью McAfee Enterprise Security Manager (ESM).

Основная проблема с точки зрения анализа событий и создания правил заключается в том, как определить, представляет ли приложение угрозу для сети, особенно для других систем. Например, представим себе ситуацию: пользователь зашел в Facebook и открыл полученное от друга сообщение со ссылкой. Пользователь без колебаний щелкает эту ссылку. В фоновом режиме, без ведома пользователя, происходит установка программного обеспечения.

Используя разработанные компанией McAfee систему SIEM, брандмауэр и систему IPS, вы можете видеть, какое количество трафика генерирует это вредоносное ПО, а также получать информацию, которая может пригодиться для анализа приложения и событий. Вы можете видеть IP-адрес источника, IP-адрес назначения, название приложения, категорию приложения, рейтинг риска, порт, зону, количество соединений и объем используемой пропускной способности.

McAfee NSP дает вам возможность видеть вредоносные действия, регистрируемые устройством IPS. Имея эту информацию, вы можете начинать подстраивать правила уровня приложений в брандмауэре и в системе IPS. Например, AppPrism на NSP даст вам возможность создавать политики IPS для угроз, связанных с такими приложениями, как Facebook.

McAfee NSP выявляет и блокирует угрозы двумя способами. Во-первых, правила на основе сигнатур блокируют известные угрозы по мере их обнаружения. Затем NSP проводит углубленную проверку пакетов на предмет наличия в них аномалий. Если данные или трафик содержат какие-либо аномальные признаки, то NSP начинает относиться к ним как к угрозе.

Использование этих двух механизмов блокирования (сигнатуры и анализ поведения) может помочь в процессе обнаружения и устранения угроз. Запустив IPS Threat Analyzer, вы увидите список известных угроз, имеющихся в вашей среде. Threat Analyzer дает вам возможность делать моментальные снимки трафика либо в режиме реального времени, либо на основе архивных данных.

А теперь посмотрите на консоль McAfee ESM (SIEM). Панели консоли McAfee ESM дают очень полезную информацию, отображая и сопоставляя сетевые события, что позволяет быстро отслеживать случаи использования приложений, отсортированные по событиям. McAfee помогает администраторам проводить анализ действий приложения, прослеживая весь путь от источника к точке назначения. Отслеживание действий приложения с помощью консоли NSP и консоли McAfee ESM дает администратору возможность проследить весь процесс от начала до конца.

Дополнительная функция McAfee NSP под названием Network Threat Behavior Analysis (NTBA) поможет вам собирать полную информацию о приложениях, их использовании, угрозах и аномальном поведении в масштабах всей сети. В приведенном выше примере NTBA дает возможность получить больше информации о том вредоносном приложении, которое было загружено из Facebook. К вашим услугам отчеты об угрозах на отдельных узлах, о сетевых моделях трафика, а также об обмене данными между узлами в вашей сети. Большинство вредоносных приложений генерирует всплески трафика, превышающие установленные в NTBA пороговые значения и вызывающие рассылку оповещений. Большинство расследований будет начинаться с информации, почерпнутой из панелей NTBA, потому что они дают администраторам возможность получить огромное количество данных обо всей сети.

Опишем, как использовать все эти продукты для выявления и нейтрализации вышеупомянутой угрозы, распространяющейся через Facebook:

- пользователь, сам того не желая, загружает приложение;
- вредоносное приложение начинает обмениваться данными с другими узлами внутри сети и генерирует стандартный исходящий трафик HTTP на IP-адрес в Китае;
- администраторы сети замечают всплеск трафика на панели NTBA;
- панель NTBA вносит узел в список угроз, имеющихся в среде;
- администраторы наблюдают большой объем трафика, исходящего от того узла, который первым загрузил данный файл;
- затем администраторы выявляют приложение, генерирующее весь этот трафик на данном узле;
- один из администраторов хочет получить дополнительную информацию об этом узле и «щелкает правой кнопкой» на этом узле в панели NTBA, чтобы посмотреть информацию об узле, полученную из консоли McAfee ePO. На узле не установлены новейшие DAT-файлы для VirusScan. Теперь администратор знает, что для устранения данной угрозы необходимо установить на узле обновления и удалить вредоносную программу;
- на консоли IPS администраторы могут также видеть другие модели трафика для данного узла и данного приложения, а также сведения о подключениях каждого узла, отсортированные по географическому местоположению;
- с помощью консоли McAfee Firewal администраторы настраивают правила брандмауэра, чтобы заблокировать данное вредоносное приложение для данного пользователя. Они также блокируют все соединения с Китаем, потому что их компания не ведет бизнес с находящимися там компаниями. Эти меры позволяют предотвратить появление аналогичных проблем в будущем и повысить уровень безопасности.

Результаты внедрения решения

Совместное развертывание McAfee Firewall Enterprise и McAfee Network Security Platform позволяет решить насущные проблемы, изложенные нами в самом начале: обнаружение приложений, сбор информации о моделях трафика, а также устранение белых пятен в сети. Использование дополнительных средств защиты, таких как McAfee ESM и McAfee Vulnerability Manager, помогает McAfee NSP и McAfee Firewall собирать еще больше информации о происходящем.

Это решение McAfee дает вам возможность быть в курсе того, кто использует сеть, какие действия совершают эти пользователи, и обеспечивать соответствие их действий корпоративной политике. Вы можете обеспечить надежный уровень безопасности и сократить время, необходимое для устранения угроз в своей среде. Такой подход позволяет повысить операционную эффективность и собирать больше информации о происходящем в сети.

Выявив все белые пятна в своей сети и внедрив более жесткие средства контроля сетевого трафика, вы можете свести к минимуму угрозы, атакующие вашу организацию изнутри и снаружи. Зная это, ваша компания может перейти к реализации других проектов в сфере ИТ, не ставя под сомнение безопасность работы и защиту от риска.

Вопросы и ответы

Есть ли в McAfee Firewall Enterprise функции IPS?
Да, в McAfee Firewall Enterprise есть функции предотвращения вторжений, но в них используются не те сигнатуры, которые используются в аппаратном устройстве NSP. Имеющийся в брандмауэре компонент IPS не так надежен, как решение IPS, специально разработанное для NSP. Функция IPS в брандмауэре предназначена для небольших сред, и развертывание ее зачастую проводят для внутренней проверки трафика между зонами.

Это решение требует установки программного обеспечения на конечных токах?
Нет. И McAfee Firewall, и Network Security Platform представляют собой сетевые аппаратные устройства, не имеющие непосредственного контакта с узлами. Если вам нужна возможность собирать и анализировать информацию об узлах в McAfee Network Security Manager, то для интеграции с конечными точками можно использовать McAfee ePolicy Orchestrator.

Могу ли я собрать данные о сетевых потоках в своей системе SIEM?
Да, McAfee ESM интегрируется и с продуктами McAfee, и с продуктами других производителей, что дает возможность сопоставлять данные, собираемые в масштабах всего предприятия, в одной консоли. Кроме того, McAfee тесно сотрудничает с другими поставщиками SIEM и иных решений, что дает вам возможность собирать данные, необходимые для анализа и экспертиз.

Дополнительные ресурсы

www.mcafee.com/ru/products/epolicy-orchestrator.aspx
www.mcafee.com/ru/products/network-security/index.aspx
www.mcafee.com/ru/products/network-security-platform.aspx
www.mcafee.com/ru/products/firewall-enterprise.aspx
www.mcafee.com/ru/products/network-threat-response.aspx
www.mcafee.com/ru/products/siem/index.aspx

Дополнительную информацию об эталонной архитектуре McAfee Security Connected см. по адресу www.mcafee.com/ru/enterprise/security-connected/index.aspx

Об авторе

Джош Тёрстон (Josh Thurston) работает в McAfee инженером по продажам. Он помогает подбирать для клиентов подходящие защитные решения, системы безопасности и лучшие практики работы, позволяющие повысить их уровень безопасности и защитить их самые важные цифровые активы. В качестве специалиста по безопасности имеет опыт работы с крупными клиентами из списка Fortune 100: Oracle, Wal-Mart, CVS, Walgreen и др.

До того как стать инженером по продажам, работал в подразделении профессиональных услуг McAfee, помогая создавать и поставлять защитные решения для Министерства обороны и разведывательных структур США. Участвовал в разработке рекомендаций по лучшим практикам работы, а также в разработке программы обучения и сертификации для McAfee University.

1 http://blog.nielsen.com/nielsenwire/mediauniverse/
2 http://timesofindia.indiatimes.com/business/india-business/Internet-usage-peaks-during-office-lunch-hrs/articleshow/8741252.cms

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной», Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.McAfee.ru

43506bp_net-traffic-L3_0412_fnl_ETMG