Документ

Внедрение системы McAfee Host Intrusion Prevention

Оптимальные методы для быстрого успеха

Содержание

Краткое содержание

На сегодняшний день комбинированные атаки и атаки «нулевого дня» представляют большую опасность, чем вирусы. Чтобы обеспечить бесперебойную работу компании, защитить конфиденциальные данные и сократить зависимость от критических обновлений, необходимо помимо сетевой защиты использовать точные инструменты системной защиты. Верный подход к пробному развертыванию и простая процедура настройки позволяют эффективно внедрить систему McAfee® Host Intrusion Prevention (Host IPS) и обеспечить системную защиту, не нарушая повседневного хода работы компании. В настоящем документе описана пошаговая процедура, которой должен следовать каждый администратор для обеспечения быстрого перехода от пробного развертывания к полноценному, успешному внедрению McAfee Host IPS. Настоящий документ не является заменой для *McAfee Installation and Product Guides* (руководства по установке и использованию продуктов McAfee).

Введение

Система Host IPS может принести огромную пользу вашей организации, так как ее использование ведет к сокращению частоты установки критических обновлений, обеспечивает бесперебойность работы и сохранение производительности труда работников, помогает защищать конфиденциальные данные и выполнять регулятивные требования и предписания. Она сочетает в себе систему предотвращения вторжений (IPS) на основе анализа поведения и сигнатур, брандмауэр, имеющий функцию отслеживания состояния соединений, и механизм блокирования приложений с целью защиты всех конечных точек — настольных ПК, ноутбуков и серверов — от известных и неизвестных угроз.

Во избежание нарушений в работе компании необходимо, однако, проявлять осторожность при внедрении всего, что затрагивает конечных пользователей и критически важные приложения. Специалисты по безопасности, уделяющие должное внимание предотвращению возможных рисков, разбивают процесс развертывания системы Host IPS на несколько небольших, простых шагов, позволяющих повышать уровень защиты постепенно, шаг за шагом подстраивая систему под особенности компании и минимизируя число нововведений для конечного пользователя. Такой «медленный, но верный» подход позволяет за период от одного до трех месяцев добиться максимального уровня защиты, потребовав минимальных усилий администраторов для проведения необходимых мероприятий..

IPS в составе Host IPS

Host IPS включает в себя три функциональные группы: IPS, брандмауэр и блокирование приложений. Конечно, все они приносят пользу, но лучше не запускать их всех сразу.

Мы рекомендуем начинать с внедрения IPS, за исключением случаев, когда регулятивные требования или имеющиеся риски заставляют уделять первостепенное внимание брандмауэру. Система IPS обеспечивает критически важную и универсально необходимую защиту от известных угроз и угроз «нулевого дня». Предустановленные настройки политик позволяют за короткое время начать использовать Host IPS для защиты ваших систем от уязвимостей и атак.

Успешное развертывание и конфигурация IPS с помощью указанных в настоящем руководстве методов даст вам возможность спокойно перейти к активации брандмауэра и любых функций блокирования приложений, требуемых для вашей системы и вашей компании. Программное обеспечение для этих дополнительных функций уже будет установлено, так как все три группы функций входят в один и тот же программный пакет. Описанную здесь стратегию пробного развертывания можно будет использовать также при активации брандмауэра и механизма блокирования приложений, хотя отдельные политики, правила и реакции на события будут отличаться.

Совет: если вы предпочитаете начать с активации брандмауэра для защиты ноутбуков или обеспечения соответствия стандарту PCI DSS (стандарт защиты информации при работе с платежными системами), то используйте описанный в настоящем руководстве подход, а за информацией о конфигурации и активации политик брандмауэра обратитесь к пользовательской документации.

Большинство администраторов способно самостоятельно осуществить описанную пошаговую процедуру. Если потребуется, партнеры McAfee и специалисты McAfee из службы поддержки всегда готовы помочь вам. Эти эксперты внесли большой вклад в составление настоящего руководства. В своей работе они придерживаются похожей процедуры, поскольку она способствует надежному снижению рисков в большинстве предприятий.

Перейдем к делу.

Несколько простых этапов

Рекомендуемая процедура пробного внедрения состоит из семи шагов:

1. Стратегия и планирование
2. Подготовка окружения
3. Установка и конфигурация
4. Начальная настройка
5. Адаптивный режим (необязательно)
6. Усиление защиты и более сложная настройка
7. Обслуживание и выход за пределы IPS

Процедуры развертывания системы на настольных ПК и серверах схожи между собой. Однако для защиты сложных и особо важных серверов и настольных ПК квалифицированных пользователей мы рекомендуем задавать более консервативные первоначальные настройки и временные рамки фаз. Соответствующие отличия указаны ниже в тексте.

Замечание по поводу сроков и ожидаемого результата

Процесс адаптации, требуемый для успешного развертывания системы (т. е. с минимальными усилиями при максимальном предотвращении рисков), составляет от одного до трех месяцев. В течение этого срока непосредственно на работу администраторов уходит всего несколько дней. Остальное время это промежутки между отдельными этапами, необходимые для того, чтобы продукт мог собрать данные об использовании системы, на основании которых осуществляется настройка.

Сроки внедрения в большей степени зависят от количества и характера систем и пользовательских профилей в вашем проекте. Чем больше у вас разных пользователей, тем больше времени займет процесс внедрения Host IPS на всех требуемых системах. Процесс активации механизмов защиты не должен ограничивать производительность пользователей и функциональность приложений. Каждый значительный системный или пользовательский профиль заслуживает настройки и тестирования.

Во многих окружениях осуществлять развертывание ПО, переводить систему в режим блокирования и использовать брандмауэр можно только после согласования с руководством отдела ИТ. Запланируйте дополнительное время для получение необходимых согласований.

Примечание: все ссылки в настоящем документе относятся к *McAfee Host Intrusion Prevention Product Guide* («Руководство по продукту McAfee Host Intrusion Prevention»), если не указано иное.

Потенциальные проблемы при внедрении IPS Что ни в коем случае *нельзя* делать	Практические рекомендации
1. Блокировать сигнатуры среднего и высокого уровня опасности без предварительного анализа собранных данных.	Сначала заблокируйте только сигнатуры высокого уровня опасности. Это обеспечит защиту от самых серьезных уязвимостей, генерируя лишь небольшое количество ложных событий. Сигнатуры среднего уровня опасности работают по поведенческому алгоритму и обычно требуют хотя бы небольшой предварительной настройки, чтобы сократить до минимума число вызовов службы поддержки.
2. Исходить из того, что во всех системах будут использоваться одни и те же политики.	Разделите настольные ПК на группы по приложениям и привилегиям. Начните с самых простых систем и создайте стандартные профили пользования для основных групп. По мере поступления новой информации постепенно добавляйте новых пользователей и новые профили пользования.
3. Проводить слишком мало тестов для выявления мнения пользователей.	Выберите несколько важных групп пользователей и проведите пробные испытания с репрезентативными пользователями, готовыми поделиться своим мнением. Протестируйте все приложения на правильность работы. Широкое развертывание начинайте только тогда, когда убедитесь, что использование политик не снижает продуктивность. Таким образом у пользователей с самого начала сложится хорошее впечатление о работе новой системы.
4. Относиться к Host IPS по принципу «поставил и забыл».	В отличие от антивируса, для обеспечения точности и эффективности защиты требуется регулярный мониторинг и регулярное обслуживание системы. Запланируйте время для просмотра журналов и обновления правил как минимум раз в неделю после завершения периода развертывания.
5. Одновременно включать IPS, брандмауэр и режим блокирования приложений.	Начните с IPS, затем добавьте брандмауэр, а потом при необходимости активируйте режим блокирования приложений. К этому времени вы уже будете знать, как создавать политики, будете лучше разбираться в целесообразности разных видов защиты, а также сможете легче соотносить вносимые изменения с получаемыми результатами.
6. Оставлять IPS, брандмауэр или механизм блокирования приложений работать в адаптивном режиме на неопределенный срок.	Включайте адаптивный режим на короткие промежутки времени, когда у вас есть возможность отслеживать создаваемые правила.
7. Немедленно блокировать все, что система распознает как вторжение.	Не торопитесь и сначала убедитесь, что наблюдаемый трафик действительно является вредоносным. В этом вам помогут такие средства, как захват пакетов, сетевой IPS и др.

Необходимые основы

Для успешного внедрения IPS необходимо четкое понимание принципа функционирования IPS, настройки основных политик и конфигурации системы.

Каков принцип работы IPS на узле?

IPS отслеживает системные вызовы и вызовы API (Application Programming Interface). Система IPS также проверяет входящий и исходящий трафик и анализирует поведение приложений и операционной системы. Сочетая сигнатуры с бихевиористической защитой, она обнаруживает и блокирует враждебные атаки и программы, нацеленные на использование уязвимостей системы.

Механизм бихевиористической защиты изолирует приложения, разрешая каждому приложению доступ только к собственным ресурсам, таким образом защищая эти ресурсы от других приложений. Подобную изоляцию иногда называют «бихевиористическим пузырем». Если приложение пытается выйти за пределы своего «пузыря», чтобы получить доступ к файлам, ключам реестра или области памяти другого приложения, то клиент IPS может заблокировать это действие и/или сделать запись в журнал событий. Кроме того, благодаря запатентованной технологии McAfee для универсальной защиты от переполнения буфера система не допускает выполнение кода из запрещенных ячеек памяти, что является одним из самых распространенных видов серверных атак.

Все вместе эти функции IPS защищают системы от атак «нулевого дня», использующих новые уязвимости, и не требуют при этом установки обновлений, благодаря чему у администраторов появляется время на тестирование исправлений перед их развертыванием.

Что такое сигнатуры и уровни опасности?

IPS использует сигнатуры — файлы с описанием синтаксических или поведенческих признаков вирусов или атак — для обнаружения и предотвращения вредоносных действий. Категоризация сигнатур в базе данных проводится на основе уровня опасности, отражающего степень риска, связанного с атакой.

- *High* (высокий) — в основном это небихевиористические сигнатуры легко обнаруживаемых угроз безопасности или вредоносных действий, включая широко известные средства использования уязвимостей. Установите для этих правил параметр «prevent» («не допускать») на всех системах.
- *Medium* (средний) — бихевиористические сигнатуры для случаев, когда приложения работают за пределами своей изолированной зоны Установите для этих правил параметр «prevent» («не допускать») на критически важных системах, в особенности на веб-серверах и SQL-серверах.
- *Low* (низкий) — бихевиористические сигнатуры для случаев, когда приложения и системные ресурсы заблокированы и не могут быть изменены. Установка для этих правил параметра «prevent» («не допускать») повышает безопасность соответствующей системы, но требует дополнительной настройки.
- *Information* (информационный) — бихевиористические сигнатуры для случаев, когда приложения и системные ресурсы подвергаются изменениям. Изменения могут свидетельствовать о легкой угрозе безопасности или о попытке получить доступ к конфиденциальной системной информации. События этого уровня происходят в ходе нормальной работы системы и, как правило, не свидетельствуют об атаке.

Правила IPS для отдельных приложений и операционных систем разрабатываются сотрудниками McAfee Labs™. На клиенты IPS эти сигнатуры поступают через инфраструктуру McAfee ePolicy Orchestrator® (McAfee ePO™). Автоматические обновления сигнатур позволяют поддерживать оптимальный уровень защиты.

Многие сигнатуры служат для защиты всей операционной системы, а некоторые только для защиты часто атакуемых приложений. Клиенты IPS для настольных ПК содержат, к примеру, средства защиты для Internet Explorer и Microsoft Outlook. Если Internet Explorer сделает попытку установить программу-лазейку, то IPS перехватит команду «записать файл», данную приложением, и отменит ее. В случае серверов (веб-серверов и серверов баз данных) специальные бихевиористические сигнатуры защищают от таких известных атак, как поиск по директориям и внедрение SQL-кода.

Что такое политики и уровни защиты?

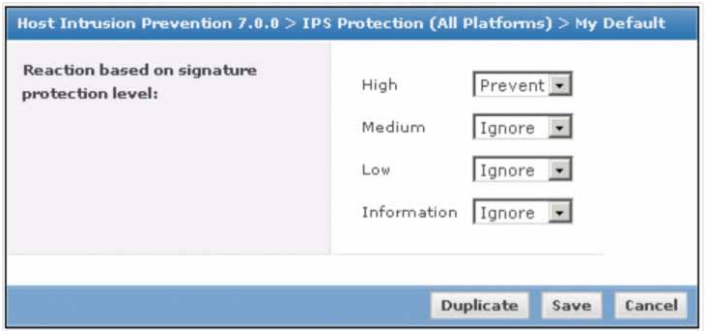
Политики IPS определяют необходимые методы реагирования для каждого уровня опасности: *Prevent* (Предотвращение), *Log* (Записание в журнал) и *Ignore* (Игнорирование). Каждая политика содержит правила для определения поведения, а также функции активации и деактивации этих правил реагирования.

Политики сгруппированы в уровни защиты. McAfee поставляет систему с предустановленными уровнями защиты, начиная с базового. Вы можете также создать свой собственный уровень защиты.

Перечень предустановленных политик:

- *Basic Protection (McAfee Default)* (Базовая защита (McAfee Default)) — не допускать сигнатуры высокого уровня опасности, а все остальные игнорировать.
- *Enhanced Protection* (Усиленная защита) — не допускать сигнатуры высокого и среднего уровня опасности, а все остальные игнорировать.
- *Maximum Protection* (Максимальная защита) — не допускать сигнатуры высокого, среднего и низкого уровня опасности, а все остальные записывать в журнал.
- *Prepare for Enhanced Protection* (Подготовка к усиленной защите) — не допускать сигнатуры высокого уровня опасности, записывать в журнал сигнатуры среднего уровня опасности, а все остальные игнорировать.
- *Prepare for Maximum Protection* (Подготовка к максимальной защите) — не допускать сигнатуры высокого и среднего уровня опасности, записывать в журнал сигнатуры низкого уровня опасности, а все остальные игнорировать.
- *Warning* (Предупреждение) — записывать в журнал сигнатуры высокого уровня опасности, а все остальные игнорировать.

Возможность самостоятельной настройки защиты позволяет создавать и редактировать политики. С помощью консоли ePO вы можете установить в IPS собственную политику защиты. Настройка правил на требуемый уровень опасности осуществляется с помощью параметров *Prevent* (Предотвращение), *Log* (Записание в журнал) и *Ignore* (Игнорирование), которые можно задать отдельно для каждого уровня опасности.



Конфигурация реакций на атаки и подозрительное поведение

Политика безопасности может предусматривать, например, следующее: если распознанная клиентом сигнатура относится к среднему уровню опасности, то он записывает факт появления этой сигнатуры в журнал и допускает обработку этого процесса операционной системой; если же сигнатура относится к высокому уровню опасности, то он не допускает этот процесс.

Многоэкземплярные политики позволяют группировать несколько разных настроек в одной политике, охватывающей разные виды систем и пользователей. Сначала вы задаете отдельные политики для каждого приложения, а затем собираете их в пакет в зависимости от конфигурации конкретной системы. Например, создав две пользовательские политики — одну для почтовых серверов, а другую для серверов баз данных — вы можете с помощью многоэкземплярной политики задать обе эти политики для системы, на которой установлены Microsoft Exchange и SQL Server.

Шаг 1: выработка стратегии

Первый шаг первого этапа заключается в определении направления. Продумайте стратегию защиты своей системы, поставьте реалистичные цели и создайте соответствующий план пробного развертывания системы и ее итогового внедрения.

Определение приоритетов пробного развертывания

Определитесь с тем, что вы ждете от системы безопасности, и разработайте соответствующий план пробного развертывания. Возможно, вам придется сознательно пойти на компромисс между срочностью задачи и вашей скоростью обучения. Вы можете сразу заняться блокированием обнаруженных вами конкретных атак, или начать с фазы общего наблюдения, чтобы просто побольше узнать о том, что происходит на ваших клиентах. Каждая организация находит свой собственный баланс между защитой и производительностью. Четкое определение приоритетов с самого начала помогает упростить весь последующий процесс.

Задайте себе следующие вопросы:

- Согласно результатам проверок, в каких областях имеется особая угроза безопасности и где были отмечены нарушения?
- Какие системы являются наиболее уязвимыми?
- Считать ли переносные ноутбуки приоритетной задачей?
- Требуется ли сокращение числа уязвимостей в какой-либо ключевой группе пользователей или систем согласно нормативам?

По мнению многих клиентов, самые большие уязвимости находятся на ноутбуках, которые покидают сферу контроля организации. Эти системы идеально подходят в качестве начального объекта развертывания IPS. Некоторые наши клиенты хотели бы усилить защиту своих ключевых серверов. В случае таких критически важных для компании систем мы рекомендуем выбрать особо осторожный подход. Составьте список главных целей, и последующие шаги помогут вам расставить приоритеты.

Общий контекст

В настоящем руководстве мы делаем акцент на систему IPS. Однако не стоит выпускать из виду и общий контекст развертывания системы Host IPS. В следующем примере показано поэтапное развертывание системы IPS, при котором подключению брандмауэра и механизма блокирования приложений на определенных типах систем предшествует тщательное планирование.

- Система IPS на ноутбуках и стандартных настольных ПК
- Система IPS на критически важных серверах
- Система IPS на настольных ПК квалифицированных пользователей
- Брандмауэр на ноутбуках
- Расширение масштабов развертывания серверной системы IPS (подключение брандмауэра, увеличение числа серверов)
- Подключение брандмауэра на настольных ПК квалифицированных пользователей
- Тестирование базового механизма блокирования приложений (обучение и черные списки)
- Усиление защиты (контроль за соблюдением политик и белые списки)

Это всего лишь один пример. Если вам, например, срочно требуется брандмауэр, то можно изменить последовательность этих шагов или пропустить ненужные. Поступайте в соответствии с целями и структурой рисков вашей организации.

Выбор окружения для пробного развертывания

Для пробного развертывания мы рекомендуем использовать небольшой набор тестовых систем. Последовательное тестирование уровней защиты следует проводить не более чем на 100 узлах в трех подсетях. Наращивая объем пошагово, вы сможете легко решать любые проблемы, возникающие в ходе тестирования. Осталось ответить на вопрос, какие компьютеры выбрать для пробного развертывания.

Определение класса систем

Распределите системы по основным классам и используйте в пробном развертывании выборку из этих классов. IPS поддерживает следующие системы, начиная с самого простого уровня внедрения и заканчивая самым сложным:

- Стандартные настольные ПК и ноутбуки конечных пользователей, не имеющих, как правило, прав администратора для установки и удаления приложений на своих системах. Вы можете создать несколько разных пользовательских профилей, каждый со своим набором стандартных приложений.
- Индивидуально настроенные настольные ПК и ноутбуки квалифицированных пользователей, имеющих права администратора для установки собственных приложений. К квалифицированным пользователям относятся, как правило, администраторы и разработчики программного обеспечения. Иногда некоторые пользователи по ошибке автоматически получают права администратора. В идеале права администратора должны быть деактивированы на всех системах, не требующих непосредственного контроля со стороны администратора. Это помогает сократить число систем, для которых требуется создавать отдельные профили и конфигурации.
- Серверы, выделенные под базу данных, электронную почту, веб-приложения и иные приложения, а также файловые серверы и серверы печати.

Тестовое окружение или рабочее?

Во многих компаниях перед установкой нового продукта обязательно проводят тесты в тестовом окружении. Для этого изготавливаются образы рабочих компьютеров либо на основе корпоративных образов, либо из свежих сборок с корпоративным программным обеспечением, и перед началом масштабного развертывания эти образы тестируются в контролируемом окружении.

В случае с IPS такой подход позволяет очень быстро создать первоначальный набор базовых правил. Однако эффективность такого подхода очень низкая, так как он не принимает в расчет пользователя. Тестеры искусственно симулируют поведение пользователя, поэтому им не всегда удается учесть все нюансы разрешенных действий. Пользователи и вредоносные программы постоянно находят новые способы использования приложений, в результате чего генерируются события, которые либо требуют незамедлительного реагирования, либо остаются незамеченными, если их вдруг по незнанию пропустят как «нормальное поведение». В обоих случаях теряется время и возникает цепочка проблем.

Наш опыт показывает, что больше всего полезной информации можно получить с помощью реальных систем в рабочем окружении. Для тестирования в рабочем окружении лучше всего использовать специально отобранные компьютеры и целевых пользователей, выполняющих повседневные задачи. Этот подход, при котором настоящие пользователи совершают настоящие действия со своими системами, дает самую надежную базу правил. Пользователи могут предоставить непосредственную информацию о последствиях изменений, внесенных в уровни и политики защиты. Однако такой подход, как правило, замедляет процесс развертывания.

Для тех, у кого есть время и ресурсы, хорошим компромиссом будет сочетание этих двух моделей. Пробный период в тестовом окружении помогает обрести уверенность в действиях и позволяет лучше изучить процессы и политики системы Host IPS. Потестировав несколько профилей пользования, вы можете перенести их в пробный проект на рабочих системах. Пробное развертывание в рабочем окружении позволяет выявить действия и приложения, пропущенные в тестовом окружении. Такой двухшаговый процесс идеален для организаций, действующих с особой осторожностью.

Совет: у администраторов должна быть возможность простого физического доступа к пробным системам. По этой причине в первую пробную группу, как правило, не могут быть включены безлюдные офисы и домашние пользователи.

Гарантия достаточной репрезентативности тестовой группы пользователей

Разобравшись в типах систем, переходите к определению профилей пользования и компьютеров в вашем пробном проекте. Определяя круг пользователей, включите в выборку представителей разных сегментов целевой организации. Чем шире выборка, тем легче вам будет создавать правила и политики, отражающие принятый в этой организации порядок работы. Так, например, в штат стандартного контакт-центра или службы поддержки входят менеджеры, операторы и технические специалисты. Обязательно включите в проект как минимум один профиль пользования из каждой группы, чтобы система IPS могла собрать информацию и создать политики для всего пользовательского спектра.

Подтверждение стратегии развертывания

Вариант № 1: «Начинай с простого»

С целью ускорения внедрения первоначальных методов защиты и упрощения процесса изучения продвинутых методов защиты мы рекомедуем активировать базовый уровень защиты только на стандартных настольных ПК и ноутбуках, а на настольных ПК квалифицированных пользователей и на серверах использовать режим записи событий в журнал.

Базовый уровень защиты является политикой IPS по умолчанию. На этом уровне блокируются действия, соответствующие сигнатурам высокого уровня опасности. Базовый уровень не требет предварительной настройки и генерирует мало событий. Вот некоторые из настроек этого уровня:

- Защита IPS активирована; блокируются действия, соответствующие сигнатурам высокого уровня опасности; все остальные сигнатуры игнорируются.
- Приложения McAfee имеют статус надежных приложений во всех правилах, за исключением правил самозащиты IPS; являясь надежными приложениями, они не генерируют исключительных событий.
- Брандмауэр, карантин и механизм блокирования приложений не активированы.

Хотя производители и модели настольных ПК и ноутбуков различны, число их вариантов относительно невелико. Большой объем собранной информации позволяет IPS с очень большой точностью реагировать на проблемы высокого уровня опасности. Так, за последние несколько лет McAfee показала, что предустановленный в IPS базовый уровень защиты обеспечил защиту от 90 и более процентов уязвимостей, исправления для которых раз в месяц выпускаются компанией Microsoft. Поэтому активация даже предустановленного по умолчанию уровня защиты уже приносит немедленный ощутимый результат.

Мы настоятельно рекомендуем следовать принципу «начинай с простого». Защита серверов может оказаться самой приоритетной задачей — но при этом и самой непростой. Серверы требуют особого внимания, потому что для развертывания на них системы IPS обязательно придется редактировать правила IPS, чтобы они не блокировали допустимые действия приложений и соответствовали тщательно настроенным на большинстве серверов режимам оптимизации работы приложений и системы. А отладка правил методом проб и ошибок на рабочих, критически важных системах связана с большим риском.

Еще один пример: системы квалифицированных пользователей нередко имеют разные наборы приложений и специальных прав, таких как, например, право на запуск скриптов. Активация IPS может вызвать большое количество событий, которые необходимо тщательно проверить на предмет необходимости их допуска или блокирования. Для сбора информации о допустимых действиях квалифицированных пользователей и серверов требуется дополнительное время.

Наблюдение и запись в журнал

Параллельно с активацией базовой защиты на стандартных настольных ПК можно также включить функцию записи в журнал событий среднего уровня опасности. Такой метод наблюдения позволяет обнаруживать события, которые IPS будет регистрировать, когда вы начнете повышать уровень защиты. Записи в журнале дают информацию об объемах и видах пользования, что позволяет по-настоящему изучить поведение системы. Мы рекомендуем использовать запись в журнал в первой фазе внедрения, чтобы избежать сюрпризов и сбоев. События следует записывать в журнал в течение полного делового цикла, т. е. на протяжении как минимум месяца или даже целого квартала, чтобы собрать информацию обо всех имеющихся приложениях и действиях. Для автоматизации этой задачи используйте политику *Prepare for Enhanced Protection* (Подготовка к усиленной защите), которая будет не допускать сигнатуры высокого и среднего уровня опасности и игнорировать все остальные.

Для остальных систем, серверов и настольных ПК квалифицированных пользователей установите режим наблюдения и записи в журнал для среднего и высокого уровней опасности. Стандартной конфигурации для этого не существует, поэтому вам придется создать копию существующей политики и отредактировать ее. Отслеживание событий только среднего и высокого уровней опасности дает достаточное количество необходимой информации, не перегружая вас деталями. Различия межу системами вы обнаружите, например, там, где серверные платформы настроены под определенные приложения, или где разработчики пользуются собственными любимыми программами и экзотическими компиляторами.

Совет: активация режима наблюдения и записи в журнал не должна влиять на работу системы и приложений. Однако мы рекомендуем тщательно наблюдать за системой после перевода IPS в рабочий режим, пусть даже только в режиме записи в журнал. Поскольку работа IPS основана на низкоуровневом взаимодействии с приложениями и операционными системами, не исключена возможность того, что это может повлиять на производительность некоторых приложений.

Планирование расширения

Набрав достаточно опыта в ходе пробной фазы и научившись отличать допустимые действия от недопустимых, можете начинать переводить сигнатуры из режима записи в журнал в рабочий режим по классам систем, правилам настройки и политикам конфигурации. Этот процесс описан ниже в данном руководстве.

Вариант № 2: Базовая защита для всех систем

В некоторых окружениях имеет смысл воспользоваться накопленным McAfee опытом, нашедшим свое отражение в стандартных настройках, и развернуть базовый уровень защиты сразу на всех системах. Этот подход рекомендуется пользователям, которым нужны основные функции IPS без необходимости их долго конфигурировать. Если IPS не является основной причиной, по которой вы купили данный продукт, то такой подход даст вам возможность быстро установить защиту от масштабных атак с минимальной затратой усилий.

Решение за вами

Вариант № 1 поможет вам извлечь максимальную пользу из инвестиции в IPS. Вариант № 2 предлагает надежный упрощенный подход. Выберите тот вариант, который соответствует вашей структуре рисков.

Шаг 2: подготовка тестового окружения

Определив приоритеты, цели и стратегию защиты, проверьте свое окружение на соответствие техническим требованиям и устраните все системные ошибки до начала установки. Это позволит вам сосредоточиться на развертывании IPS и избежать возникновения проблем, не связанных с программным обеспечением IPS.

Установка/обновление программного обеспечения McAfee ePO

Перед установкой IPS необходимо сначала установить сервер ePO, а затем установить агент McAfee Agent на целевых узлах.

Программное обеспечение ePO понадобится вам не только для установки Host IPS, но и для назначения политик. Если вы еще не знаете, как создавать политики с помощью ePO, обратитесь к *McAfee ePolicy Orchestrator Product Guide* («Руководство по продукту McAfee ePolicy Orchestrator»).

Почему ePO?

Host IPS требует наличия ePO. В отличие от антивирусных систем McAfee, в которых используется инфраструктура автоматического обновления сигнатур DAT, и поэтому использование ePO необязательно (принцип «поставил и забыл»), для развертывания Host IPS каждой организации требуются свои собственные политики и правила, в которые необходимо постоянно вносить поправки по мере изменения рабочих процессов и состава пользователей. Чтобы в таких условиях иметь возможность простого и эффективного обновления политик, Host IPS использует надежную инфраструктуру, предоставляемую программным обеспечением ePO. Использование программного обеспечения ePO сокращает число отклонений и ошибок и предоставляет администратору улучшенные возможности наблюдения и контроля.

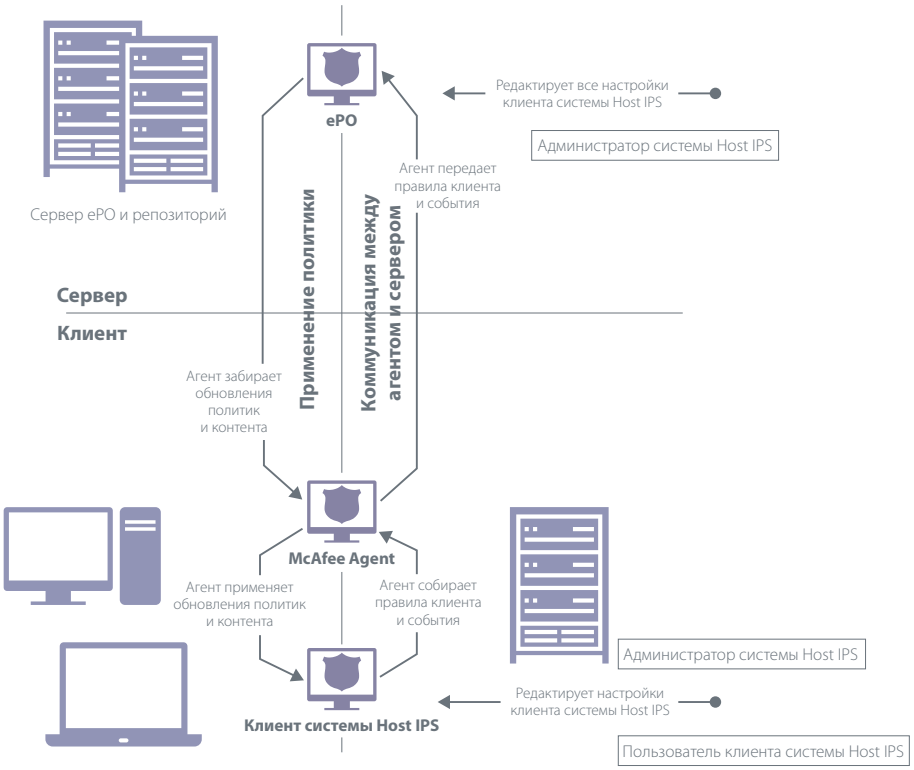


Схема процесса: установка и обслуживание IPS с помощью программного обеспечения ePO

- Сервер ePO и агент McAfee Agent, находящийся на каждом узле, совместно устанавливают клиент IPS на каждой целевой системе.
- Политики IPS создаются и обновляются в консоли управления ePO.
- Сервер ePO передает политики агенту на узловой системе.
- Клиент IPS применяет политики и генерирует информацию о событиях, которую отправляет агенту.
- Агент передает информацию о событиях в ePO.
- Через установленные промежутки времени или по требованию пользователя сервер ePO загружает контент и программные обновления из репозитория McAfee, а агент забирает их с сервера для обновления клиента IPS.
- При изменении политик агент забирает с сервера измененные версии и обновляет клиент IPS.

Использование ePO для настройки клиентов и профилей пользования

Для каждого отдельного вида пользования — веб-серверы, ноутбуки, терминалы — рекомендуется создать в ePO отдельный профиль пользования. Впоследствии вам надо будет привязывать эти профили к отдельными политиками IPS, поэтому к тому моменту, когда вам понадобится обрабатывать исключения, хорошо иметь уже готовые профили.

Совет: программное обеспечение ePO позволяет присваивать системам логические теги. Теги — это метки, которыми можно пометить одну или несколько систем вручную или автоматически. На основе тегов можно распределять системы по группам для пробного развертывания. Также их можно использовать в качестве критериев при составлении отчетности.

При распределении клиентов по группам руководствуйтесь логикой. Клиенты можно группировать в соответствии с любыми критериями, не противоречащими структурной иерархии системы ePO. Например, первый уровень можно сгруппировать по географическому местоположению, а второй уровень по операционным системам или IP-адресам. Мы рекомендуем группировать системы по критериям конфигурации Host IPS, таким как тип системы (сервер или настольный ПК), ключевые приложения (веб-приложение, база данных или почтовый сервер) и стратегическое местоположение (DMZ или интранет).

Большое значение имеют правила выбора наименований. В идеале наименования следует выбирать так, чтобы они были без труда понятны каждому. Наименования служат для однозначного определения клиентов в структуре системы, в некоторых отчетах и в генерируемых клиентом данных о событиях, происходящих на клиенте.

Контроль за состоянием пробных систем

После того, как вы определитесь с клиентами, удостоверьтесь, что на имеющихся системах устранены все проблемы, способные помешать развертыванию. Просмотрите соответствующие файлы журналов сервера ePO и журналы системных событий на предмет наличия ошибок или сбоев, свидетельствующих о неправильной конфигурации и системных аномалиях, которые могут повлиять на ход установки Host IPS. Ошибки следует устранить до начала установки Host IPS. Обратите внимание прежде всего на следующие моменты:

- *Состояние обновлений* — Установлены ли последние обновления всех драйверов и приложений? Как показывает практика, старые версии медиа-проигрывателей, браузера Internet Explorer и драйверов сетевых карт могут создавать несовместимости, ведущие к срыву процесса установки. Установите все последние обновления и исправления.
- *Несовместимое программное обеспечение* — Не запущены ли на узле другие приложения для обнаружения вторжений или брандмауэры? Возможно их придется деактивировать или удалить.
- *Права администратора* — У вас должны быть права администратора для доступа к системе. Обратите внимание на то, есть ли права администратора у пользователя. Почему? Пользователь может помешать процессу тестирования, установив новое приложение во время проведения теста. Если у вас нет возможности лишить конечного пользователя прав администратора, имеет смысл поместить эту систему в другой профиль пользования, соответствующий квалифицированному пользователю.
- *Организационные соображения* — Некоторые компьютеры требуют особого внимания по причине наличия приложений повышенной опасности, использования другого языка, специфичных для этого региона приложений или приложений собственного производства. В таком случае имеет смысл подключить эти системы лишь во второй фазе развертывания или вывести эти специализированные приложения из-под защиты IPS до тех пор, пока у вас не появится время собрать данные и проанализировать их поведение (См. *Конфигурация базовой политики (необязательно)* в следующем разделе).

Шаг 3: установка и начальная конфигурация

Вы планировали. Готовились. Наконец настало время развертывания.

Установка программы управления Host IPS на сервере ePO и импортирование клиентского программного обеспечения Host IPS в репозиторий ePO

На серверной системе ePO установите компонент управления Host IPS, обеспечивающий интерфейс с управлением политики Host IPS в консоли ePO. Импортируйте клиентскую программу Host IPS в репозиторий ePO на сервере.

Проверьте наличие обновлений или статей о базах знаний на сервисном портале McAfee https://mysupport.mcafee.com/Eservice/Default.aspx. Скачайте обновленное содержимое с сайта http://www.mcafee.com/us/downloads/. Более подробно см. в *McAfee Host Intrusion Prevention Installation Guide* («Руководство по установке McAfee Host Intrusion Prevention»).

Установка начальных уровней защиты и ответов

Настало время отдачи от инвестиций, сделанных вами в разработку стратегии и профилей пользования. Внедряйте свою стратегию путем определения или присвоения уровней защиты каждому профилю пользования. Если вы следуете стратегии «начинай с простого», то сначала вы активизируете базовую защиту для стандартных профилей пользования настольных ПК.

См. инструкции в *Working with IPS Protection Policies* («Работа с политиками защиты IPS»).

Конфигурация базовых политик (необязательно)

Некоторые администраторы настраивают установки защиты по умолчанию сразу же, до начала развертывания. Вы можете выбрать автоматическую защиту приложений высокого риска (тех, которые запускаются как службы или открытые порты на стороне опорной сети) и приложений, разработанных своими силами. Приложения, разработанные самими компаниями, зачастую исключаются из IPS в начале развертывания, особенно, если они ожидают сетевых соединений. Разработчики внутрифирменного программного обеспечения могут не столь скрупулезно подходить к программированию ожидаемого и безопасного поведения, как разработчики коммерческих программ. Например, программа, связанная с Internet Explorer, может непреднамеренно запустить сигнатуру защиты Internet Explorer, если программа ведет себя небезопасно. Так как разработанные самой фирмой приложения не являются типичными мишенями атак, не видны и неизвестны злоумышленникам, они подвергаются меньшему риску компьютерного вторжения.

Рассмотрите целесообразность добавления IP-адресов своих сканеров уязвимостей к списку надежных сетей. Ваша существующая платформа ePO и политики безопасности могут предоставить дополнительные указания относительно очевидных мер блокирования или разрешения индивидуальных профилей пользования. Наконец, вы можете использовать адаптивный режим выборочного определения правил для исключенных приложений и внедрить защиту. Эта мера может быть принята после того, как вы установите базовые уровни защиты и ознакомитесь с сигнатурами и политиками IPS.

Более подробно см. в *Management of Policies* («Управление политиками»).

Уведомление конечных пользователей и планирование обходных путей

До начала активизации IPS уведомьте пользователей о новой защите и о том, что в некоторых случаях имеются обходные пути. Такая мера снизит имеющийся риск для производительности конечного пользователя, что особенно важно для пользователей, работающих на портативных компьютерах во время поездок. В течение пилотного периода пользователи могут обходить блокировку IPS тремя способами. Администратор может:

- Создать пароль с ограниченным сроком действия
- Передача конечному пользователю полномочий блокирования модулей
- Разрешить конечным пользователям при необходимости полностью удалять Host IPS

Не следует раздавать такие временные решения слишком щедро, чтобы пользователи не затруднили процесс развертывания программы. Два обходных приема из перечисленных выше будут закрыты в процессе испытаний позднее. См. *Working with Client UI Policies* («Работа с политиками в отношении клиентского пользовательского интерфейса»).

Привлечение службы технической поддержки

Сообщите в службу технической поддержки о том, что вы собираетесь активизировать Host IPS. Хотя проблем и не должно возникать, работникам этой службы следует быть готовыми к распознаванию симптомов. Возможно, в каких-то ситуациях вам придется доказывать непричастность Host IPS к возникшей проблеме, однако это является частью работы администратора программ системы безопасности.

Установка Host IPS на пилотные узлы

Начните с малого. Установите программу сначала у нескольких клиентов, затем постепенно расширяйте ее на другие системы по мере возрастания уверенности в своих действиях. Начните с одной системы, затем увеличьте количество систем до 10, затем до 20, затем до 50 и до 100 систем. Рекомендуется следующая последовательность развертывания:

1. Убедитесь, что целевые узлы подключены к питанию, соединены в сеть и имеют связь с программой ePO.
2. С помощью задачи развертывания ePO разместите агенты Host IPS на небольшом количестве узлов внутри пилотной группы.
3. Подтвердите правильность установки, выявите неисправности, при необходимости выполните корректировку.
4. Выполните расширение на другие системы.

По мере развертывания установки проверьте пилотные системы на предмет корректной работы новой программы и проследите за журналами ePO на предмет событий сервера и любых значительных воздействий на работу сети. Не исключено, что возникнет несколько проблем, поэтому так важны пилотные испытания и медленное развертывание.

1. Убедитесь, что службы Host IPS и структуры начали работу.
2. *Важно*: запустите простые приложения, например, бухгалтерские программы, программы редактирования документов, электронную почту, доступ в Интернет, мультимедиа или средства разработки и убедитесь в их корректной работе. Могут ли ваши пользователи выполнять свои обычные обязанности? Необходимо продемонстрировать и подтвердить корректную работу функций обнаружения приложений/операций.
3. При возникновении проблем в системе клиента вы можете изучить журналы IPS клиента и журналы операционной системы клиента на предмет ошибок. См. *Working with Host Intrusion Prevention Clients* («Работа с клиентами защиты предотвращения вторжения на узел»).

Для добавления систем повторите эти действия до заполнения пилотной группы.

Совет: выполняйте тестирование при каждой установке или изменении политики с целью обеспечения успешной работы конечных пользователей. Такое тестирование может быть единственным необходимым действием в обеспечении успешного развертывания.

Шаг 4: начальная настройка

Когда пилотная группа будет в состоянии рабочей готовности, можно некоторое время подождать и понаблюдать. Подождите накопления событий в течение 2-7 дней, но не забывайте о пилотной группе. Реагируйте на все вызовы службы поддержки.

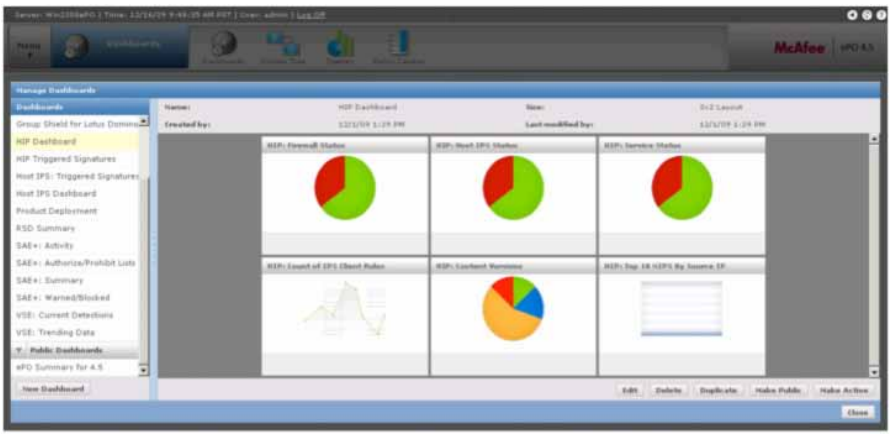
Ежедневный мониторинг

Администратору важно понять, что IPS отличается от антивирусных программ или устройств, предназначенных для установки и автономного управления угрозами без осуществления наблюдения за ними. С самого начала ежедневно уделяйте несколько минут просмотру журналов событий IPS и наблюдения за объемами и типами активности. Благодаря этой привычке вы получите базовое представление о нормальном уровне работы и характере активности. Например, при ежедневном наблюдении вы заметите регулярные процессы и уровни активности в обслуживании сервера и обновлении приложений. Обладая знанием базовой активности, вы немедленно распознаете любое произошедшее необычное событие.

И, наконец, ваш ежедневный обзор будет включать в себя детализацию правил, политик и исключений по мере возникновения новых событий. Программа Host IPS обеспечивает детальное управление, так как она способна осуществлять наблюдение за всеми вызовами системы и API, а также блокировать вызовы, которые могут привести к злоумышленным действиям. Так же, как и для системы IPS сети, необходимо периодически выполнять дополнительную настройку правил в связи с изменением требований к приложениям, предприятию и политике.

Совет: зачастую при сканировании журналов специалисты устают от большого количества повторов и пропускают детали, которые могли бы повлечь за собой принятие иного решения о правиле. Во время длительных обзоров рекомендуется периодически делать перерыв, чтобы возобновить работу с новыми силами.

Текущее обслуживание развертывания Host IPS включает наблюдение, анализ и реагирование на активность; изменение и обновление политик, а также выполнение задач системы, таких как установка полномочий пользователей, задач сервера, уведомлений и обновление содержимого. Эте меры должны быть предусмотрены на оперативном уровне с целью поддержания исправности и эффективности функций IPS.



Панели мониторинга ePO для наблюдения за событиями и тендециями

Обзор записей в журнале через несколько дней

Журналы с накопленными событиями помогут конфигурировать политики с целью обеспечения баланса между защитой и свободой доступа к информации и приложениям. Как правило, этот баланс отличается в зависимости от типа пользователя. На этом этапе вы будете настраивать политики вручную, с помощью программы ePO. Позднее мы обсудим автоматическое создание политик с помощью адаптивного режима.

Начните с анализа журналов. В программе ePO выберите вкладку *Events* («События») для Host IPS во вкладке *Reporting* («Отправка отчетов»). Вы можете просмотреть такие детали события как процесс, вызвавший событие, дата события и клиент, вызвавший событие. Необходимо обращать внимание на красные флаговые указатели, такие как мнимые ложные положительные результаты или сигнатуры, вызванные угрозами высокой степени серьезности.

Проверьте корректность процессов и служб. Те приложения, от которых вы ожидаете функционирования, должны работать, а те, которых вы не ожидаете увидеть, не должны появляться. Если вы видите зарегистрированные события, основанные на законной активности, что нередко бывает при наличии внутрифирменных приложений, такие ложные положительные результаты могут быть скорректированы описанным ниже способом.

Совет: довольно часто события создаются и блокируются без видимого влияния на конечного пользователя или работу приложения. Например, таким поведением часто отличаются конверты VMware и приложения Adobe. Можно смело игнорировать такие события, если вы можете подтвердить, что взаимодействие с пользователем не меняется. Вы также можете закрыть лазейки, такие как, например, уязвимость межсайтового скриптинга, которыми можно воспользоваться.

Начало настройки для улучшения защиты и запуска законных операций предприятия

Теперь в отношении вышеизложенных инициируемых событий вам следует сделать следующее:

- Усилить защиту зарегистрированных событий, которые должны быть блокированы
- Устранить ложные положительные результаты на основании законной активности предприятия

Клиенту можно сообщить о трех возможных вариантах реагирования:

- *Ignore* (Игнорирование) — отсутствие реакции; событие не зарегистрировано и процесс не предотвращен
- *Log* (Записание в журнал) — событие зарегистрировано, но процесс не предотвращен
- *Prevent* (Предотвращение) — событие зарегистрировано и процесс предотвращен

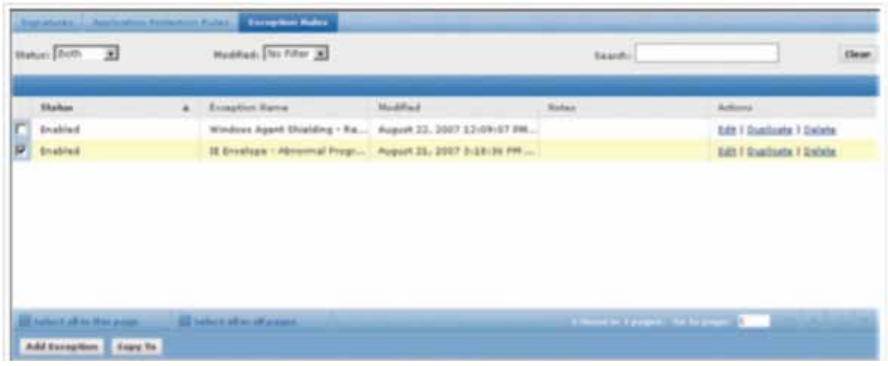
Совет: держите окно или вкладку обозревателя открытым на разделе IPS Events(«События») консоли ePO и используйте отдельное окно для управления продуктом IPS. Таким образом, вы не потеряете нужное место в дереве системы или политике при переходах туда и обратно.

Настройка правил реагирования

Прежде всего следует активизировать режим предотвращения для всех сигнатур первой степени опасности в отношении тех систем, наблюдение за которыми велось в режиме регистрации.

Создание исключений

Затем следуе выявить события, устанавливающие флаг на законном поведении, которое должно быть разрешено или, возможно, разрешено и зарегистрировано. Вы можете сократить число таких ложных положительных результатов, создав правила исключения и надежные приложения или просто настроив ответы реагирования.



Редактирование правил исключения с целью управления поведением

Создайте правила исключения для обхода политики безопасности в конкретных случаях. Возможно установить ответ реагирования на «Ignore» (Игнорирование), чтобы отменить регистрацию событий. Например, хотя политика и может рассматривать обработку некоторых сценариев как незаконное поведение, для некоторых систем в ваших инженерных группах требуется работа сценариев. Создайте исключения для инженерных систем для их нормального функционирования, в то время как на других системах политика будет продолжать предотвращение сценариев. Сделайте такие исключения частью санкционированной сервером политики, чтобы они охватывали только инженерную часть.

Исключения позволяют сократить число предупреждений о ложных положительных результатах и минимизировать объем бесполезных и ненужных данных, передаваемых на консоль. Уменьшив помехи, вы сможете проще выявлять важные события во время ежедневного мониторинга.

Совет: сделайте исключение достаточно универсальным, чтобы оно работало на всех аналогичных системах в одних и тех же или схожих обстоятельствах.

Создание надежных приложений

Надежные приложения — это такие процессы приложений, которые всегда разрешены. Надежные приложения отличаются в зависимости от профиля потребления. Вы можете потребовать некоторые программные приложения для обеспечения нормальной деятельности только на некоторых, но не на всех участках компании. Например, вы можете разрешить передачу мгновенных сообщений в отделе техподдержки, но предотвратить ее в финансовом отделе. Чтобы разрешить использование этого приложения, вы можете установить его как надежное на системах отдела техподдержки. Более подробно см. *Configuring a Trusted Applications Policy* («Конфигурирование политики надежных приложений») в руководстве по продукту.

Для получения информации о конкретном элементе и фильтрации данных для конкретных подмножеств этой информации используйте запросы, например, события высокого уровня, о которых сообщили определенные клиенты в течение определенного промежутка времени. Обращайте внимание на сигнатуры, которые были инициированы наиболее часто. Являются ли они ежедневными законными деловыми функциями, которым можно дать разрешение? Для таких сигнатур выполните понижение уровня опасности. Некоторые исключения настольных ПК являются ошибочным поведением законных приложений, поэтому вам не нужно разрешать такое поведение. Убедитесь в корректной работе приложения пользователя и продолжайте блокирование.

И, наконец, фактор качества: получали ли вы жалобы от пользователей? Беседовать нужно непосредственно с пользователями, чтобы убедиться, что их приложения работают нормально.

Принимая решения относительно настройки во время пилотного периода, придерживайтесь следующего порядка действий:

- *Редактирование политик* — используйте программу ePO для редактирования и создания политик и ответов.
- *Выборочное применение правил* — используйте программу ePO для применения правил к целевым системам (не автоматически).
- *Активизация изменений* — при изменении политик Host IPS в консоли ePO эти изменения влияют на управляемые системы в следующей связи агента с сервером. По умолчанию этот интервал составляет 60 минут. Для немедленного применения политик возможно выполнить активизацию агента с консоли ePO.
- *Тестирование изменений* — перепроверьте успешность работы этих изменений, включая совместимость с системами решения коммерческих задач (разрешение законной активности). Убедитесь, что трафик сети IPS минимизирован и что число намеченных ложных положительных результатов сокращаются.
- *Более широкое применение правил* — если новые правила работают, примените их к соответствующим системам.
- *Продолжайте ежедневный мониторинг*

См. конкретные инструкции по настройке политик в разделах *Working with IPS Rules Policies* («Работа с политиками правил IPS»), *Working with IPS Exceptions* («Работа с исключениями IPS») и *Managing IPS Events* («Управление событиями IPS»).

Конфигурирование панелей мониторинга и отчетов

Теперь, когда вы навели порядок и добились точности в событиях, можете использовать программное обеспечение ePO для улучшения организации и обеспечения связи информации IPS.

- Если вы используете программу ePO версии 4, выполните конфигурацию панелей мониторинга ePO для быстрого обзора текущего соответствия политике, тенденций событий, результатов запросов и проблем. Сохраните уникальные панели мониторинга для отражения ежедневного наблюдения, еженедельных обзоров и любых отчетов управления.
- Выполните конфигурацию уведомлений для предупреждения определенных лиц о возникновении конкретного события. Например, уведомление может быть отправлено в случае инициирования события высокой степени опасности на определенном сервере.
- Создайте график автоматического составления отчетов и их рассылки соответствующим сторонам в виде электронного письма.

Более подробно см. в разделе *Management of Information and Notifications for Host IPS Events* («Управление информацией и уведомления о событиях Host IPS»).

Обслуживание и наблюдение

В течение следующих двух или более недель ведите ежедневное наблюдение за событиями, проверяйте запросы службы технической поддержки, отклонения от нормальной работы и ложные положительные результаты. С нашей относительно консервативной стратегией развертывания не должно возникать много запросов на поддержку или проблем, поэтому не должно быть большого числа корректировок.

Блокирование обходных путей

Блокируйте указанные ниже временные решения, в результате чего пользователи и вредоносные программы не смогут обходить защиту IPS:

- Передача конечному пользователю полномочий блокирования модулей
- Разрешение конечным пользователям при необходимости полностью удалять Host IPS

Шаг 5 (необязательно): активация адаптивного режима

Тем временем, ваши наиболее сложные и специализированные системы, очевидно, находились в *режиме регистрации данных*. Как только закончен рабочий цикл записи событий в журнал, можно начинать внедрение правил с адресной направленностью с целью создания специальных политик для этих систем. Такие политики можно определять вручную, однако мощным инструментом создания правил IPS на основе активности узла, без участия администратора, является *адаптивный режим*. По мере использования приложения будет создаваться правило для разрешения каждого действия. Адаптивный режим не инициирует никаких событий IPS и не блокирует активность, за исключением злоумышленных проникновений (сигнатуры высокого уровня опасности). Исключения, которые инициируют правила, будут зарегистрированы программным обеспечением ePO как *правила клиента IPS*, но таким образом, чтобы позволить вам наблюдать ход выполнения.

Установив репрезентативные узлы в адаптивном режиме во время пробного развертывания, вы сможете создать конфигурацию настройки для каждого профиля пользования или приложения. Затем IPS позволит вам взять любое правило клиента, или все правила, или никаких и преобразовать их в санкционированные сервером политики. По окончании настройки выключите адаптивный режим с целью ужесточения системы предотвращения вторжений. (В дополнение к адаптивному режиму функции брандмауэра и блокирования приложений имеют также *обучающий режим*, который требует, чтобы администратор или конечный пользователь одобрили правила до их применения).

С помощью режима записи событий в журнал вы получили представление о частоте активности. Соответственно, адаптивный режим даст вам представление о полном диапазоне активности и ее типе. Эти два инструмента, используемые вместе, обеспечивают хорошую функциональную базу для законной деловой активности вашей организации. Нужно ожидать, однако, появления необычной активности, незафиксированная во время пробного цикла, поэтому необходимо быть готовым к пересмотру исключений и периодическому созданию правил вручную. Например, пользователь может запускать приложение собственного производства раз в четыре месяца и пропустить циклы как режима режим записи событий в журнал, так и адаптивного режима.

Обратите внимание, что адаптивный режим по умолчанию блокирует все предупреждения высокой степени опасности. Если вы проводили мониторинг только до этого момента, будьте наготове на тот случай, если контроль за соблюдением новых правил повлияет на поведение системы, особенно это касается приложений обственного производства.

Используйте адаптивный режим для управления сигнатурами как средней, так и высокой степени опасности. Такое сочетание обеспечит хороший обзор активности без лишних помех.

Адаптивный режим весьма эффективен в создании правил исключения. Однако вряд ли нужно разрешать любую активность на какой-либо системе, иначе вы не стали бы рассматривать применение новых видов защиты. Поэтому следует использовать адаптивный режим в течение ограниченного времени, тщательно просматривать каждое созданное правило (есть только один случай для каждого правила), а также деактивировать неприемлемые правила, создаваемые адаптивным режимом.

Активируя адаптивный режим, выбирайте параметр политики *Retain Client Rules* (Сохранить правила клиента). Иначе новые правила будут удаляться во время каждого интервала контроля за соблюдением политики и их необходимо будет восстанавливать. В итоге, когда вы отключите адаптивный режим и перейдете к внедрению правил, вам понадобится отключить параметр *Retain Client Rules* (Сохранить правила клиента) и удалить все правила, не утвержденные политиками ePO.

Необходимо соблюдать определенную последовательность:

1. Активировать адаптивный режим на некоторый период времени (от недели до 30 дней)
2. Оценить исключения и адаптивные правила
3. Деактивировать несоответствующие правила
4. На вкладке *IPS Client Rules* (Правила клиента) переместить законные правила непосредственно в политику для применения другими клиентами
5. Деактивировать адаптивный режим
6. Если установлен параметр *Retain Client Rules* (Сохранить правила клиента), отключить его

Важно: адаптивный режим разрешает и законную, и неприемлемую активность. Правила, разрешающие эту активность, будут созданы без одобрения администратора. На каждое созданное правило регистрируется только одно событие исключения, поэтому после создания правила одна и та же активность может проходить, будучи незарегистрированной. Вы получите только одно уведомление, поэтому необходимо выполнять тщательный просмотр и реагировать с целью предотвращения неприемлемых правил.

Оптимальные методы работы с адаптивным режимом

Для обеспечения максимальной защиты вы можете заранее сделать так, чтобы некоторые сигнатуры никогда не отменялись. Просто отредактируйте правила для этих сигнатур с целью деактивации параметров *Allow Client Rules* (Разрешить правила клиента).

- Выполняйте прогон приложений клиентов в адаптивном или обучающем режиме не менее недели, чтобы увидеть всю нормальную активность. Запланируйте время для таких действий как, например, резервирование или обработка сценариев.
- Как и в режиме записи событий в журнал, вы сможете проследить исключения клиента в консоли ePO, просматривая их в обычном, фильтрованном и совокупном видах.
- Используйте автоматически созданные правила клиента для каждого исключения, чтобы определить новые, более детальные политики или добавить новые правила к существующим политикам, затем примените обновленные политики к другим клиентам.
- При включении адаптивного режима выберите параметр политики *Retain Client Rules* (Сохранить правила клиента). В противном случае правила будут удаляться после каждого интервала контроля за соблюдением политики.
- Используйте адаптивный режим в течение конкретного периода времени, во время которого вы сможете проверить созданные исключения и правила. Если проверить правила невозможно, деактивируйте адаптивный режим во избежание разрешения сомнительных действий.
- Адаптивный режим поможет вам при необходимости создать правила для нового приложения. Включите адаптивный режим на короткое время для применения приложения и затем примените соответствующие правила.

Совет: не забудьте деактивировать адаптивный режим, чтобы без вашего ведома не создавалось никаких правил.

См. раздел *Working with IPS Policies* («Работа с политиками IPS») или обращайтесь к партнерам McAfee или в профессиональную сервисную организацию для получения детальной консультативной помощи с точной настройкой политик и применением адаптивного режима.

Шаг 6: усиление защиты и более сложная настройка

Когда установлены и настроены базовые ответы на активность, можно приступать к повышению уровня защиты и контроля за соблюдением правил. Действия по настройке можно выполнять в контексте ежедневного наблюдения или можно повторять формальные повторяющиеся действия пилотного цикла. После каждого действия подождите не менее двух недель перед тем, как принять решение о внесении дополнительных изменений. Такой период времени даст возможность убедиться в корректной работе систем при существующем уровне защиты.

Перевод стандартизованных персональных компьютеров с базовой защиты на усиленную с помощью *Prepare for Enhanced Protection (Подготовка к усиленной защите)*

Повышенный уровень защиты предотвратит сигнатуры высокой и средней степени опасности и будет игнорировать все остальные. Используя *Prepare for Enhanced Protection* (Подготовка к усиленной защите), вы сделаете промежуточный шаг, зарегистрировав вначале средние уровни опасности. Как обсуждалось в случае с серверами и персональными компьютерами ключевых пользователей, запись событий в журнал дает подробное представление о том, какая активность будет затронута при повышении уровня защиты, обеспечивая при этом точное управление политиками и уменьшая количество сюрпризов.

Когда вы будете уверены в том, что работа организации продолжается бесперебойно, измените установки на усиленный уровень защиты. Повторите этот алгоритм действий для всех остальных систем сети. Максимальная защита подходит для наиболее специализированных условий, отличающихся повышенными требованиями к надежности и отказоустойчивости систем. Так как максимальная защита блокирует сигнатуры даже низкой степени опасности, она должна быть развернута весьма осмотрительно, после обширного тестирования. И вновь, до активизации максимальной защиты используйте *Prepare for Maximum Protection* (Подготовка к максимальной защите) в качестве испытательного полигона для выяснения влияния изменений.

Чрезвычайно консервативные организации могут развертывать каждое изменение уровня защиты в качестве собственной пилотной программы, выполняя рассмотренные выше повторяющиеся действия. Не забудьте активировать и деактивировать обходные пути и адаптивный режим до и после циклов тестирования, утверждающих изменения.

Продолжение настройки

Выполните обзор исключений и любых возникающих проблем. Поступайте в их отношении в соответствии с рекомендациями, рассмотренными при обсуждении начального этапа настройки.

- Следите за запросами службы техподдержки и замечаниями пользователей, обращая внимание на любые жалобы или проблемы в работе организации, вызванные блокированием доступа, ложными положительными результатами или поведением новых приложений. Таких проблем должно быть очень мало, но новые требования возникают всегда.
- Регулярно проверяйте созданные исключения.
- Выполняйте соответствующую настройку политик. Не забывайте использовать программу ePO для отправки обновлений политики на системы узла. Необходимо осознанно применять их к системам, на которые вы хотите повлиять.

Шаг 7: обслуживание и расширение

В предыдущих шагах был обозначен основной процесс развертывания. Когда на ваших системах будут развернуты средние уровни защиты, у вас будет установлена усовершенствованная система защиты. Необходимо продолжать регулярное наблюдение, обновление политик и обслуживание систем. Теперь рассмотрите также расширение защищенных систем и усиление защиты с целью включения более жестких политик и других функций Host IPS.

Обслуживание

McAfee часто выпускает обновления содержимого для новых сигнатур, а также периодические обновления функций и пакеты исправления. Рекомендации по оптимальным методам:

- Установите график регулярных обновлений, чтобы программа ePO опрашивала репозиторий McAfee на предмет обновлений, а ваши клиенты их получали.
- Если у вас большое количество специализированных приложений, которые, как выяснилось в процессе начального развертывания, требуют настройки, возможно забрать контент Host IPS в оценочную ветвь вашего репозитория с целью тестирования по сравнению с пробной группой систем. Как только ваша пробная группа утвердит новое содержимое, можно переместить его в текущую ветвь для широкого развертывания.
- Если вы пользуетесь продуктами Microsoft, запланируйте загрузку содержимого, чтобы оно совпадало с обновлениями «вторника пакетов исправления Microsoft».
- На некоторых компьютерах могут периодически устанавливаться новые приложения, и у вас может не оказаться времени или ресурсов для немедленного выполнения их настройки. Используйте адаптивный режим для профилирования конкретных компьютеров и отправляйте на сервер созданные в результате правила клиента. Возможно преобразование этих правил клиента в существующую или новую политику, а затем применение политики к другим компьютерам для работы с новыми программами.
- Включите тестирование IPS в процессы управления изменениями и выпуска программ. При подготовке к развертыванию пакета исправления или обновления или продукта Microsoft протестируйте и отработайте их на системах IPS, чтобы выполнить надлежащую настройку до массового развертывания.

Вообще, когда появляются новые приложения, пользователи или профили пользования, желательно выполнить мини-пилотную отработку на нескольких компьютерах, чтобы определить и протестировать политики, а затем выполнить более широкое развертывание.

Расширение

В зависимости от особенностей вашей организации рассмотрите один из нижеприведенных вариантов расширения развертывания. Не забывайте продолжать развертывать изменения медленно и осмотрительно, чтобы вы могли быстро минимизировать нарушения работы пользователей и диагностировать аномальное поведение. Лучше медленно двигаться вперед, чем совершать ошибки или упускать из виду полезные параметры защиты.

Для этого вам необходимо:

- Развернуть одну и ту же защиту на дополнительных системах с тестируемыми профилями пользования. Вы можете легко управлять развертыванием Host IPS на тысячи компьютеров, так как большинство компьютеров укладываются в несколько профилей пользования. Управление крупномасштабным развертыванием сводится к нескольким правилам политики.
- Если выполнялся пробный цикл только для стандартизованных персональных компьютеров, следует повторить процесс для ключевых пользователей и серверов, начиная с записи событий в журнал и пользуясь преимуществами адаптивного режима.

- Добавить новые профили пользования и сообщества пользователей.
- Применить правила брандмауэра, затем рассмотреть блокирование приложения — именно в таком порядке. Выполнять пилотный процесс, используя руководство по продукту на предмет особенностей правил и обучающего режима.
  - » Брандмауэр является важнейшим компонентом многоуровневого обеспечения безопасности. Он блокирует весь непредусмотренный трафик к системам, таким образом значительно снижая возможность удаленных атак. В развертывании для переносных компьютеров эта программа должна стать приоритетной.
  - » Блокирование приложений обычно развертывается весьма избирательно, но базовое понимание может оказаться полезным, даже если вы думаете, что оно вам не понадобится. Блокирование приложений может быть критически важным инструментом, если вам необходимо немедленно блокировать конкретную угрозу или блокировать приложение по причинам конфиденциальности или регламентации.

Следующие шаги

В настоящем руководстве предоставлен стратегический план успешного внедрения Host IPS. С помощью вдумчивого и добросовестного применения функций IPS и настройки политик администраторы смогут развернуть IPS с минимальными доработками, без разочарований для себя и своих пользователей. Более подробно см. руководства по установке и продуктам и не забывайте поддерживать актуальность своей защиты с помощью загрузки обновлений с сервисного портала McAfee и веб-сайтов для скачивания программ. Если вам требуется практическая помощь, обращайтесь к партнерам McAfee или в профессиональную сервисную организацию.

ООО «МакАфи Рус»

Компания McAfee, Inc., штаб-квартира которой расположена в г. Санта-Клара, является крупнейшей в мире компанией, специализирующейся на технологиях безопасности. McAfee непрерывно борется с самыми сложными в мире проблемами безопасности. Она предоставляет проверенные упреждающие решения и службы, которые обеспечивают безопасность систем и сетей по всему миру, позволяя пользователям безопасно подключаться к Интернету, более безопасно работать и совершать покупки в Интернете. Благодаря исследовательской команде, удостоенной многочисленных наград, компания McAfee создает решения, которые позволяют индивидуальным пользователям, компаниям, общественным организациям и поставщикам услуг Интернета соответствовать нормативам, защищать данные, предотвращать нарушение работы, определять уязвимости, а также постоянно наблюдать за уровнем собственной безопасности и повышать его. Получить более подробные сведения можно посетив http://www.McAfee.ru.

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
Бизнес центр «Башни на набережной»
4ый этаж, офис 405 – 409
Телефон: +7 (495) 967 76 20
Факс: +7 (495) 967 76 00
www.McAfee.ru

8145wp_dtp_hips-best-prac_0110_ETMG