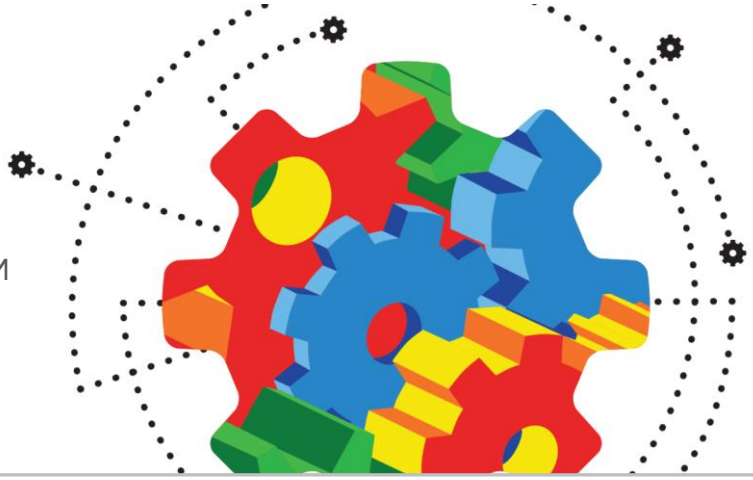
Sourcefire Company

Компания Sourcefire теперь входит в состав корпорации Cisco

Виртуальные устройства Sourcefire и виртуальный центр защиты Sourcefire™

ВЫСОЧАЙШИЙ УРОВЕНЬ КОНТРОЛЯ И ГИБКОСТИ В ЗАЩИЩЕННЫХ ВИРТУАЛЬНЫХ СЕТЯХ



Общие сведения о виртуальных устройствах Sourcefire

Преимущества

- Полный контроль над ИТ-инфраструктурой в виртуализированной среде.
- Виртуальное развертывание выполнять проще, чем физическое.
- Обеспечение соответствия стандартам PCI и требованиям ФСТЭК в виртуальных средах.
- Возможность выполнять проверку с использованием до двух ядер ЦП (VMware, Xen) или до четырех ядер ЦП (RHEV).
- Управление до 25 физическими и/или виртуальными устройствами с помощью виртуального центра защиты.

Области применения

- Защита серверов в соответствии со стандартом PCI или требованиями ФСТЭК.
- Небольшие филиалы.
- Удаленные офисы (например, розничные магазины).
- Организации с распределенными отделами ИТ-безопасности.
- Среды с аппаратными ограничениями (например, передвижные телевизионные станции, военный транспорт, развертывания на открытом воздухе).
- Организации со строгими требованиями к сертификации оборудования.
- Среды с ограниченным пространством — мало свободного места в стойках в ЦОД.
- Расширенная сеть реального времени, технологии обнаружения пользователей и ВМ.
- Лаборатории или обучающие центры.
- Вычислительные среды MSSP/облачные среды.

Виртуальное устройство Sourcefire® и виртуальный центр защиты Sourcefire™, доступные на платформах VMware, Red Hat и Xen, позволяют развертывать ведущие решения по кибербезопасности Sourcefire в виртуальных средах, обеспечивая повышенный уровень защиты как физических, так и виртуальных ресурсов. С помощью виртуальных устройств Sourcefire организации могут проверять трафик между виртуальными машинами (ВМ), а также без труда развертывать и управлять устройствами в удаленной среде, где ресурсы могут быть ограниченными. Теперь пользователи продуктов Sourcefire имеют возможность выбирать физическое или виртуальное решение, которое соответствует их конкретным требованиям к инфраструктуре.

Преимущества виртуализации

Виртуализация обеспечивает значительные преимущества для бизнеса. В их числе снижение расходов, ускорение развертывания и повышение доступности систем. Кроме того, виртуализация помогает снизить потенциальные риски для безопасности. Однако в процессе виртуализации создаются «слепые зоны», вследствие чего существует более высокая вероятность неправильной конфигурации, чем в физических сетях. Виртуальная инфраструктура объединяет функции, которыми ранее управляли другие группы, например отделы ИБ, служба развития ЦОД и сетевой отдел. Это создает дополнительный риск неправильной конфигурации. Наконец, в отсутствие адекватного координирования или контроля происходит разрастание числа ВМ.

Виртуальные устройства Sourcefire помогают устранить риски, связанные с виртуализацией: слепые зоны, отсутствие разделения обязанностей и бесконтрольный рост числа ВМ. Эти динамичные и гибкие средства защиты сети обеспечивают следующие три основных преимущества.

- **Полный контроль над ИТ-инфраструктурой в виртуализированной среде.**
- **Упрощение процесса развертывания: виртуальное развертывание выполняется проще, чем физическое.**
- **Обеспечение соответствия стандартам PCI и требованиям ФСТЭК в виртуальных средах.**

Полный контроль над ИТ-инфраструктурой в виртуализированной среде

При развертывании на физических хостах, содержащих ВМ, виртуальные устройства помогают устранить «слепые зоны». «Слепые зоны» представляют собой большую проблему в виртуальных сетях, поскольку существует риск того, что изменения топологии или конфигурации не будут обнаружены. Вследствие динамичной природы виртуальных сетей такие случайные изменения вполне вероятны. На рисунке 1 показано виртуальное устройство Sourcefire, подключенное к двум различным виртуальным сетям на том же хосте. В первой сети осуществляется обмен производственными данными, во второй — данными о разработке. Хосты в сети, где происходит обмен данными по разработке, содержат исходный код, и они не должны взаимодействовать с производственной сетью.

В случае неправильной конфигурации или непреднамеренного нарушения политики эти две сети оказываются взаимосвязанными (показано пунктирной линией). Виртуальное устройство Sourcefire обнаруживает такие изменения, а также любой вредоносный трафик между двумя сетями.

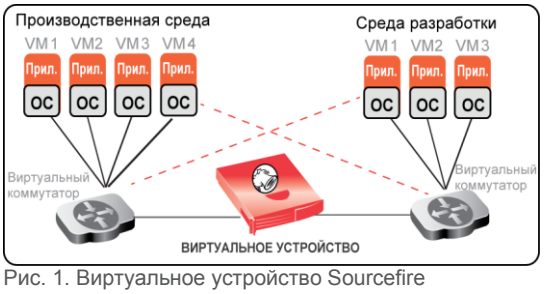


Рис. 1. Виртуальное устройство Sourcefire осуществляет мониторинг различных виртуальных сетей на том же хосте

Виртуальное развертывание выполнять проще, чем физическое

Поскольку виртуальные устройства Sourcefire основаны на программном обеспечении и не имеют аппаратных компонентов, их проще развернуть, чем физические устройства. Однако физические устройства по-прежнему широко используются для развертываний с целью обеспечения безопасности сети. Специализированное оборудование обеспечивает высокую производительность, которая необходима в мультигигабитных средах, таких как производственный центр обработки данных. Но физические устройства имеют свои особые требования.

- **Пользователи должны выделить мощность и место в стойке для таких устройств.**
- **В некоторых средах существуют строгие требования к оборудованию, связанные либо с процессом сертификации, либо с жесткими условиями эксплуатации. Физические устройства могут не соответствовать этим требованиям.**
- **Физические устройства должны быть доставлены в то место, где они будут эксплуатироваться. В некоторых странах установлены очень жесткие таможенные требования относительно ввоза оборудования, что выльется в значительные затраты времени или денег.**

Виртуальные устройства не имеют подобных ограничений. Их можно развернуть немедленно на базе существующего оборудования и сразу же начинать контролировать трафик. Так как виртуальные устройства не зависят от физического оборудования, они могут осуществлять мониторинг местоположений или сегментов сети, которые невозможно было отслеживать ранее.

Другое преимущество использования виртуальных устройств Sourcefire состоит в том, что с помощью одной и той же консоли центра защиты Sourcefire® можно управлять как физическими, так и виртуальными устройствами. При добавлении виртуального устройства на физический хост его можно зарегистрировать в существующей консоли и немедленно начать передачу данных. Пользователям не нужно будет устанавливать новую консоль управления и обучаться использованию отдельного приложения для управления. Кроме того, использование той же консоли центра защиты для управления виртуальными устройствами обеспечивает разделение обязанностей. Аналитики в сфере безопасности могут продолжать осуществлять управление системой обеспечения безопасности сети как виртуальной, так и физической.

Обеспечение соответствия стандартам PCI и требованиям ФСТЭК в виртуальных средах

Защита виртуальных платежных систем, информационное дополнение, опубликованное группой по вопросам виртуализации Совета по стандартам безопасности индустрии платежных карт, содержит рекомендации о том, как обеспечить и поддерживать соответствие стандартам PCI в виртуальных средах. Новое руководство устанавливает специальные требования в области безопасности для виртуализированных сред данных о владельцах карт (CDE). Аналогичные требования по безопасности виртуализированных сред установлены и ФСТЭК России.

Например, требования к обеспечению безопасности сети распространяются на виртуальную среду. Требование PCI 11.4 обязывает использовать системы IDS/IPS для отслеживания критических областей в среде CDE. Согласно новому руководству организациям могут потребоваться специализированные средства IDS/IPS для соответствия данному требованию, поэтому они могут осуществлять мониторинг виртуальных сетей и/или данных, которыми обмениваются ВМ. Виртуальное устройство Sourcefire может отслеживать критически важные сети, содержащие данные о владельцах карт или сведения личного характера, и проверять трафик между ВМ.

На рисунке 2 показано, как виртуальное устройство Sourcefire может выполнять мониторинг среды CDE. Обратите внимание, что среды CDE и не CDE предоставляются на отдельных виртуальных коммутаторах и подключены к отдельным физическим сетевым интерфейсам. Кроме того, отдельные интерфейсы используются для критически важных функций, таких как перенос ВМ, хранение виртуальных образов и управление виртуальными средами.

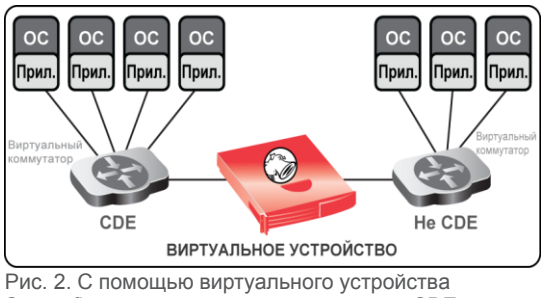


Рис. 2. С помощью виртуального устройства Sourcefire можно выполнять мониторинг CDE и обеспечить соответствие требованию PCI DSS 11.4

Согласно требованию PCI 6.3.2 среды разработки, тестирования и производства должны быть отделены друг от друга. Виртуальное устройство Sourcefire помогает отслеживать выполнение данного требования, поскольку данное устройство может генерировать оповещения в случае, когда происходит обмен данными между этими средами.

Виртуальное устройство Sourcefire

Виртуальные устройства Sourcefire помогают защитить те сегменты сети, которые оказываются недосягаемы для традиционных средств ИТ-безопасности, или обеспечить безопасность там, где использование физических устройств не является целесообразным (например, в удаленных офисах). Виртуальное устройство можно развернуть в пассивном или промежуточном режиме.

Одно виртуальное устройство способно использовать до двух ядер ЦП (VMware или Xen) или до четырех ядер ЦП (RHEV) и обеспечивает тот же уровень контроля и защиты, что и физическое устройство. Виртуальное устройство Sourcefire совместимо с платформами VMware ESX/ESXi 4.1/5.0 и Xen 3.3.2/3.4.2 (требуется как минимум одно ядро ЦП и 1 Гбайт памяти), а также с платформой RHEV 3.0 (требуется как минимум четыре ядра ЦП и 4 Гбайт памяти). Виртуальное устройство Sourcefire 64 бита для VMware совместимо с платформой VMware ESX 4.1/5.x или более поздней версии (требуется как минимум четыре ядра ЦП и 4 Гбайт памяти).

Виртуальное устройство Sourcefire

- Возможность выполнять проверку с использованием до двух ядер ЦП (VMware, Xen) или до четырех ядер ЦП (RHEV).
- Идентичные функциональные возможности виртуального устройства в промежуточном или пассивном режиме.
- Уровень контроля и защиты, сопоставимый с тем, который обеспечивает физическое устройство.
- Производительность (зависит от оборудования и количества ВМ, конкурирующих за ресурсы).
- Поддерживает платформы VMware ESX/ESXi 4.1/5.x, RHEV 3.0 и Xen 3.3.2/3.4.2.

Виртуальный центр защиты Sourcefire

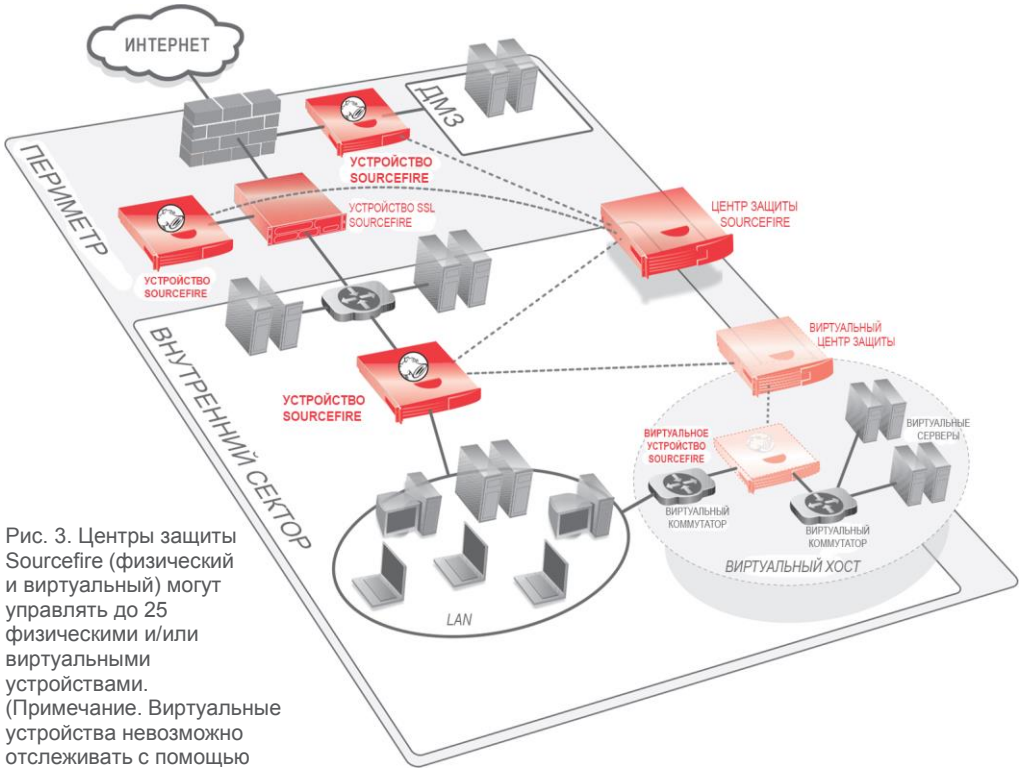


Рис. 3. Центры защиты Sourcefire (физический и виртуальный) могут управлять до 25 физическими и/или виртуальными устройствами. (Примечание. Виртуальные устройства невозможно отслеживать с помощью нескольких центров защиты одновременно).

Как и виртуальное устройство Sourcefire, виртуальный центр защиты Sourcefire доступен как виртуальное устройство на базе платформ VMware, Red Hat и Xen. С помощью виртуального центра защиты можно управлять до 25 физическими и/или виртуальными устройствами, что делает процесс управления устройствами в удаленных офисах проще и удобнее. Пользователи могут выполнять мониторинг виртуальных устройств с помощью того же виртуального центра защиты, который они используют для мониторинга физических устройств.

Поставщики управляемых услуг в области безопасности (MSSP) могут разместить на одном сервере VMware, RHEV или Xen несколько виртуальных центров защиты для различных пользовательских сред, что снижает риск смешивания событий безопасности, обеспечивает соответствие нормативным требованиям и эффективность управления.

Виртуальный центр защиты совместим с платформами VMware ESX/ ESXi 4.1/5.0 и Xen 3.3.2/3.4.2 (требуется как минимум два ядра ЦП и 2 Гбайт памяти), а также с платформой RHEV 3.0 (требуется как минимум четыре ядра ЦП и 4 Гбайт памяти). Виртуальное устройство Sourcefire 64 бита для VMware совместимо с платформой VMware ESX 4.1/5.x или более поздней версии (требуется как минимум четыре ядра ЦП и 4 Гбайт памяти).

Виртуальный центр защиты Sourcefire

- Идентичная функциональность центра защиты (нет режима главного центра защиты).
- Управление до 25 физическими и/или виртуальными устройствами.
- Производительность (зависит от оборудования и количества ВМ, конкурирующих за ресурсы).
- Поддерживает платформы VMware ESX/ESXi 4.1/5.x, RHEV 3.0 и Xen 3.3.2/3.4.2.

Дальнейшие шаги по защите вашей среды

Виртуальные устройства Sourcefire повышают уровень защиты как физических, так и виртуальных ресурсов. Виртуальные устройства Sourcefire могут использоваться для проверки трафика на двух ядрах ЦП. Они обеспечивают высокий уровень контроля и гибкости для безопасности вашей виртуальной среды. Развертывание виртуального центра защиты Sourcefire не представляет особых трудностей. Небольшие виртуальные центры защиты можно развернуть в удаленных офисах, или несколько виртуальных центров защиты можно разместить на одном физическом хосте. С помощью виртуального центра защиты можно управлять до 25 физическими и/или виртуальными устройствами, что делает процесс управления устройствами в удаленных офисах проще и удобнее.

Виртуальные устройства Sourcefire обеспечивают три основных преимущества.

- **Полный контроль над ИТ-инфраструктурой в виртуализированной среде.**
- **Упрощение процесса развертывания: виртуальное развертывание выполнять проще, чем физическое.**
- **Обеспечение соответствия стандартам PCI в виртуальных средах.**

Для получения дополнительной информации о виртуальных устройствах Sourcefire и виртуальном центре защиты Sourcefire посетите сайт **www.sourcefire.com**, свяжитесь с компанией Sourcefire или обратитесь к одному из членов всемирного союза по безопасности Sourcefire Global Security Alliance™ или напишите на эл. почту security-request@cisco.com.

Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауэрс»,
Космодамианская наб., д. 52, стр. 1, 4 этаж
Телефон: +7 (495) 961 1410,
факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова, д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230,
факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»,
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600,
факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691,
факс: +375 (17) 269 1699
www.cisco.ru

Казахстан, 050059, Алматы,
бизнес-центр «Самал Тауэрс»,
ул. О. Жолдасбекова, 97, блок А2, 14 этаж
Телефон : +7 (727) 244 2101,
факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, Лэндмарк здание III, 3-й этаж
Телефон: +994-12-437-48-20,
факс: +994-12-437 4821

Узбекистан, 100000, Ташкент,
бизнес центр INCONEL,
ул. Пушкина, 75, офис 605
Телефон: +998-71-140-4460,
факс: +998-71-140 4465

© Компания Cisco и (или) ее дочерние компании, 2014 г. Все права защищены. Cisco и логотип Cisco являются товарными знаками или зарегистрированными товарными знаками компании Cisco и (или) ее филиалов в США и ряде других стран. Для просмотра перечня товарных знаков Cisco перейдите по адресу www.cisco.com/go/trademarks. Прочие товарные знаки, упомянутые в настоящем документе, являются собственностью соответствующих владельцев. Использование слова "партнер" не означает наличия партнерских отношений компании Cisco с какой-либо другой компанией.