Sourcefire Company

Компания Sourcefire теперь входит в состав корпорации Cisco

Система Sourcefire® IPS нового поколения

Основные возможности

- Система обнаружения и предупреждения вторжений Snort
- Интеллектуальный анализ сети
- Оценка влияния
- Идентификация пользователя
- Автоматизированная настройка политик
- Анализ поведения сети
- Экспертиза на уровне пакетов
- Определение типа файлов
- Контроль приложений
- Фильтрация URL-адресов
- Усовершенствованная защита от вредоносных программ

«По мнению экспертов Gartner, изменение характера угроз и меняющиеся бизнес- и ИТ-процессы будут заставлять руководителей в области обеспечения сетевой безопасности более активно использовать возможности IPS-систем нового поколения на следующем цикле обновления межсетевых экранов или IPS-систем»[1], —

Джон Пескаторе (John Pescatore), Gartner Greg Young, Gartner

Система IPS следующего поколения от Sourcefire устанавливает новый стандарт защиты от угроз благодаря интеграции функций учета контекста в реальном времени, интеллектуальной автоматизации и обеспечению непревзойденной производительности систем предотвращения вторжений. Никакое другое решение не обеспечивает такой же уровень контроля, автоматизации, гибкости и масштабируемости для защиты динамичных сред от изощренных угроз.

Система предотвращения вторжений (IPS) нового поколения

Система предотвращения вторжений нового поколения от Sourcefire (NGIPS) может использоваться ИТ-отделами для обеспечения того уровня защиты, который необходим в современной быстро меняющейся среде. Система NGIPS основана на механизмах учета контекста и автоматизации, которые, по мнению экспертов Gartner, являются ключевыми компонентами системы IPS следующего поколения, а также на высокопроизводительной платформе Sourcefire FirePOWER™ и механизме интеллектуального анализа сети Sourcefire FireSIGHT®. Система NGIPS обеспечивает следующие возможности:

- **Учет контекста в реальном времени: возможность просмотра и сопоставления больших объемов данных событий, связанных с элементами ИТ-среды — приложениями, пользователями, устройствами, операционными системами, уязвимостями, службами, процессами, поведением сети, файлами и угрозами.**
- **Усовершенствованная защита от угроз: защита от современных угроз благодаря передовой технологии предотвращения угроз, эффективность которой подтверждена независимым тестированием и опытом использования тысячами заказчиков по всему миру.**
- **Интеллектуальная автоматизация: значительное сокращение совокупной стоимости владения и обеспечения соответствия меняющимся потребностям бизнеса благодаря автоматизации оценки влияния событий, настройки политик IPS, управления политиками, анализа поведения сети и идентификации пользователей.**

1 Источник: «Определение технологии предотвращения вторжений следующего поколения» (Defining Next-Generation Network Intrusion Prevention), Gartner, 7 октября 2011 года.

- **Беспрецедентная производительность и масштабируемость: специализированные устройства обеспечивают малое время задержки, высокую производительность и масштабируемость.**
- **Дополнительные средства контроля приложений, фильтрации URL-адресов и защиты от вредоносных программ: сокращение области поражения благодаря детализированному контролю более 1800 приложений и 180 миллионов URL-адресов в более чем 80 категориях. Обнаружение, отслеживание и блокировка подозрительных файлов и вредоносных программ для предотвращения вирусных эпидемий и повторного заражения.**

В реальном мире угрозы постоянно развиваются. Так же происходит и в вашей сети. У вас ограниченные ресурсы, а сделать надо много всего. Вам требуется адаптивная система IPS, которая обеспечит защиту не только сегодня, но и в будущем по мере развития вашего бизнеса и усложнения угроз.

Учет контекста в реальном времени

Вы не можете защитить то, что не видите. Представьте агента спецслужбы, который охраняет президента и при этом носит повязку на глазах. Аналогичным образом устройство обеспечения безопасности сети не может защитить вашу уникальную среду, если настроено с использованием политик по умолчанию. Оно не может обеспечить эффективную защиту, поскольку неизвестно, что нужно защищать.
Но устройство Sourcefire работает по-другому. С 2003 года Sourcefire собирает данные о работе сети для предоставления контекста системам обеспечения безопасности сети.

Технология Snort®

- Открытый исходный код, стандарт для систем IPS.
- Разработано в 1998 году Мартином Рёшем (Martin Roesch), основателем и директором по технологиям Sourcefire.
- Самая широко распространенная технология IPS: более 4 миллионов загрузок.
- Используется в более чем 100 крупнейших компаниях мира.
- Используется более чем в 30 крупнейших государственных учреждениях США.
- Сообщество Snort стало целой экосистемой:
  - » около 400 000 зарегистрированных пользователей;
  - » опубликованы десятки книг, посвященных Snort;
  - » организуются обучающие курсы в колледжах и университетах;
  - » группы пользователей;
  - » обсуждения и форумы.

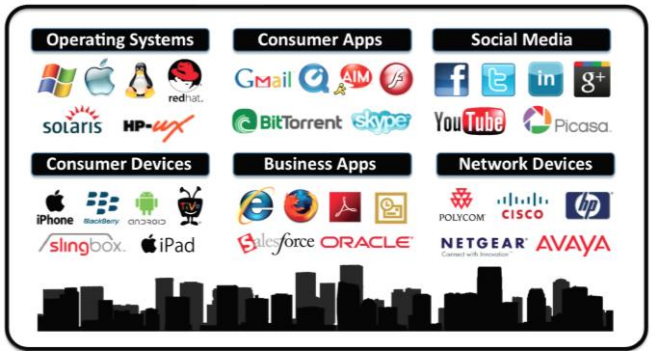

Рис. 1. Примеры обнаружения с помощью технологии FireSIGHT™

Технология Sourcefire FireSIGHT™ обеспечивает полный контроль над сетью, включая физические и виртуальные хосты, операционные системы, приложения, пользователей, контент и потенциальные уязвимости хоста.

Средство Context Explorer позволяет визуализировать и изучить всю контекстуальную информацию, которую предоставляет FireSIGHT, включая часто используемые приложения и хосты. Оно создает динамически обновляемые представления вашей среды, благодаря которым можно получить детальную информацию.

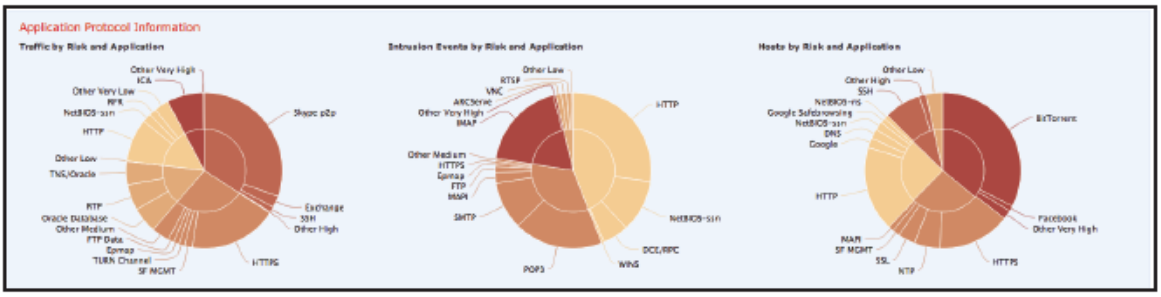

Рис 2. Context Explorer

Усовершенствованная защита от угроз

Sourcefire помогает бороться с современными угрозами для безопасности сети с помощью технологии FirePOWER. Создание черных списков IP-адресов на основе оценки репутации позволяет предотвратить подключение к ботнетам, источникам спама и другим вредоносным IP-адресам. Усовершенствованная технология сетевой защиты, доступная опционально для устройств FirePOWER, обеспечивает обнаружение и блокировку вредоносных программ, непрерывный анализ, ретроспективное оповещение и использует механизм интеллектуального анализа Sourcefire Collective Security Intelligence. Вы можете воспользоваться этими дополнительными средствами защиты, когда будете готовы и посчитаете это необходимым.

Благодаря комбинации правил IPS с учетом уязвимостей, пользовательских правил, интеллектуального механизма анализа IP-адресов и возможностей оценки файлов пользователи Sourcefire имеют в своем распоряжении более широкий арсенал средств для защиты своих систем, чем предлагают большинство поставщиков систем IPS. И это не просто слова, они подтверждены фактами.

Sourcefire является лидером на карте NSS Lab Security Value Map для систем IPS за 2013 год по показателям безопасности и общей стоимости владения. На рисунке 3 приведены результаты последних тестов в сравнении со средними показателями по отрасли (всего протестировано 10 поставщиков)

	SOURCEfire	Среднее значение по отрасли
Уровень защиты	98,9%	92,76%
Совокупная стоимость владения (защищено, Мбит/с)	$15,23	$37,82

Рис. 3. Результаты исследования систем IPS, проведенного NSS Labs в 2012 году

Система Sourcefire NGIPS поддерживается исследовательской группой Sourcefire VRT®, в которую входят ведущие в отрасли эксперты по вопросам безопасности. Они создают официальные правила Snort®, используемые системой Sourcefire NGIPS. Sourcefire VRT:

- **Обнаруживает, оценивает и реагирует на последние тенденции в области взломов, вторжения и использования злоумышленниками уязвимостей;**
- **Разрабатывает основанные на уязвимостях правила для защиты от потенциальных угроз;**
- **Обеспечивает защиту для критически важных уязвимостей Microsoft.**

Зона действия технологии обнаружения FireSIGHT™

- Физические/виртуальные хосты.
- Операционные системы.
- Приложения.
- Смартфоны и планшеты.
- VoIP-телефоны.
- Сетевые принтеры.
- Маршрутизаторы.
- Потенциальные уязвимости.
- Сетевой поток и пропускная способность.
- Сетевые аномалии.
- Идентификация пользователя.
- Типы файлов и протоколы.
- Вредоносные подключения.

[2] Источник: Отчет об исследовании систем IPS 10 поставщиков, проведенном NSS Labs в 2013 году.

Sourcefire Company

Компания Sourcefire теперь входит в состав корпорации Cisco

Решение Sourcefire NGIPS обеспечивает комплексную защиту от следующих вредоносных программ и видов атак:

- **Черви**
- **Трояны**
- **Атаки через черный ход**
- **Шпионское ПО**
- **Сканирование порта**
- **VoIP-атаки**
- **Атаки IPv6**
- **DoS-атаки**
- **Переполнение буфера**
- **P2P-атаки**
- **Статистические аномалии**
- **Аномалии протокола**
- **Аномалии приложений**
- **Вредоносный трафик**
- **Недействительные заголовки**
- **Смешанные угрозы**
- **Угрозы на основе оценки**
- **Совершенно новые угрозы**
- **Сегментация TCP и фрагментация IP**

«Сопоставление имени пользователя с IP-адресом отвлекало нас от других важных задач. Раньше этот процесс занимал несколько часов. Сейчас на это уходит одна-две секунды. Я могу быть уверена в том, что я могу связаться с пользователем немедленно в случае, если его сеть подвергнется атаке», —

Тамара Фишер (Tamara Fisher), инженер по безопасности, AutoTrader.com

Автоматизация интеллектуальных технологий защиты

Автоматизация имеет большое значение для борьбы с угрозами в ситуации, когда ресурсы ограничены. Группы ИТ-безопасности должны стремиться к тому, чтобы соответствовать требованиям бизнеса и использовать для достижения этой цели современные интеллектуальные средства, а не просто выполнять большой объем работы. Система Sourcefire NGIPS использует механизм учета контекста для более эффективного использования интеллектуальной автоматизации следующим образом:

FireSIGHT®

Пример автоматизации

- Обновления политик и правил предотвращения угроз
- Оценка ущерба, нанесенного угрозой
- Сопоставление пользователей и событий
- Сопоставление событий с пользователями, устройствами, сервисами и приложениями
- Экспорт событий в систему SIEM
- Создание отчетов

- **Оптимизация защиты и производительности системы посредством автоматизации обновления политик защиты с учетом изменений сети.**
- **Снижение количества событий безопасности, требующих принятия мер, на 99 % посредством сопоставления угроз с целевыми операционными системами и приложениями и их уязвимостями.**
- **Получение представления о том, к кому обращаться, когда внутренний хост подвергается атаке со стороны клиента.**
- **Получение оповещений о нарушениях политики конфигурирования или попытках несанкционированного доступа к системе.**
- **Обнаружение распространения вредоносного ПО посредством мониторинга сетевого трафика и обнаружения аномалий в сети.**

FireSIGHT гарантирует надлежащее развертывание средств защиты сети и автоматическую поддержку по мере развития сетей и угроз. FireSIGHT повышает уровень безопасности сети и помогает сократить эксплуатационные расходы.

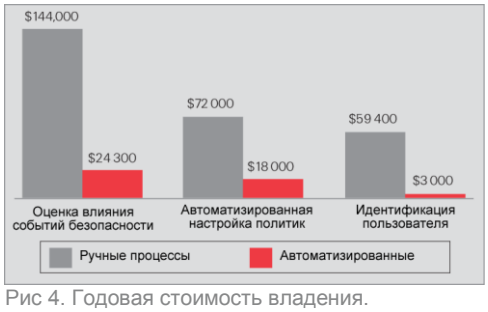

Рис 4. Годовая стоимость владения.

Снижение совокупной стоимости владения за счет автоматизации

Благодаря автоматизации стандартных функций предотвращения угроз организация может сэкономить десятки тысяч долларов в год.

Sourcefire Company

Компания Sourcefire теперь входит в состав корпорации Cisco

Беспрецедентная производительность и масштабируемость

Система Sourcefire NGIPS работает на базе лучшего в своем классе оборудования и обеспечивает пропускную способность от 50 Мбит/с до 60+ Гбит/с. В основе устройств серии FirePOWER лежит передовая технология ускорения, которая позволяет достичь максимальной для отрасли производительности при высокой энергоэффективности.

Устройства Sourcefire FirePOWER 8000 обеспечивают высокую пропускную способность, модульность сети, расширяемость и масштабируемость. Уровень производительности достаточен для эффективного использования данных устройств в самых требовательных средах. Модульность сети обеспечивает низкую входную стоимость, позволяет выбирать количество портов и типы носителей для вашей сети и использовать различные типы интерфейсов по мере необходимости. Благодаря расширяемости пользователи получают возможность эффективно использовать сетевые интерфейсы по мере роста. А масштабируемость позволяет наращивать вычислительную мощность во всем стеке устройств.

Центр управления Sourcefire FireSIGHT® является центральной нервной системой решений Sourcefire для обеспечения безопасности сети. Именно здесь выполняется настройка всех политик доступа и защиты и оценка всех событий безопасности и соответствия нормативным требованиям.

Центр управления FireSIGHT позволяет также создавать отчеты с использованием различных шаблонов. Sourcefire предлагает настраиваемые панели мониторинга, которые имеют интерфейс, как у портала, с библиотекой виджетов для мониторинга событий безопасности и соответствия нормативным требованиям, а также состояния и производительности устройств FirePOWER.

Возможности центра управления FireSIGHT Management Center

- Централизованный мониторинг событий
- Управление физическими и виртуальными устройствами Sourcefire FirePOWER
- Настраиваемые панели мониторинга с разнообразными виджетами
- Администрирование и рабочие процессы на основе ролей
- Уведомления с помощью системного журнала, по электронной почте и по протоколу SNMP
- Интеллектуальные отчеты с возможностью индивидуальной настройки
- API-интерфейсы для интеграции с решениями других поставщиков
- Поддержка LDAP, AD и RADIUS.
- Автоматизированное обновление системы предотвращения угроз

Дополнительная защита за счет контроля приложений, фильтрации URL-адресов и усовершенствованной защиты от вредоносных программ

Sourcefire NGIPS выводит защиту на новый уровень благодаря дополнительным возможностям контроля приложений, фильтрации IP и усовершенствованной защиты от вредоносных программ.

Атаки через приложения — один из излюбленных приемов злоумышленников на сегодняшний день. Организации могут достичь более высокого уровня защиты, если будут не просто выявлять вредоносные приложения, но контролировать использование приложений и доступ к ним.

Кроме того, организации могут снизить риск атак на стороне клиента и улучшить производительность сотрудников посредством контроля доступа к более чем 280 миллионам URL-адресов в 80 категориях.

Наконец, Sourcefire предоставляет пользователям системы NGIPS возможность обезопасить себя от вредоносных программ и новейших целенаправленных угроз. Непрерывный мониторинг, анализ больших объемов данных, ретроспективный анализ событий безопасности и оценка активности вредоносных файлов обеспечивают беспрецедентный контроль над угрозами.

Благодаря детальному контролю приложений и доступа к веб-страницам организации могут повысить безопасность своей сети в целом и сократить область поражения атаками. Пользователи системы NGIPS могут осуществлять непрерывный мониторинг, выполнять ретроспективный анализ событий безопасности и оценку активности вредоносных файлов. Благодаря использованию такого уникального подхода к обеспечению безопасности они могут быть уверены в том, что их сеть защищена до, во время и после атак.

Беспроблемная интеграция со сторонними решениями

Благодаря открытому исходному коду и различным API-интерфейсам систему Sourcefire NGIPS можно без труда интегрировать со сторонними решениями, включая системы управления уязвимостями, системы управления событиями безопасности (SIEM), системы контроля доступа к сети (NAC), средства расследований и экспертизы сети и т. п. Совместимость системы со сторонними технологиями обеспечивает следующие преимущества:

- **Повышение эффективности инвестиций без дополнительных усилий или применения обновлений.**
- **Упрощение процесса развертывания средств защиты и планирования действий.**
- **Обеспечение гибкости для гарантии безопасности в любой ИТ-среде.**

«В ходе тестирования система одного поставщика генерировала оповещения для 80 % трафика, а система Sourcefire не создала ни одного оповещения. Мы обратились к инженеру Sourcefire, потому что нам казалось, что система не работает. По его словам, система не создавала оповещения, потому что объекты, подвергаемые атаке в ходе теста, никак не могли пострадать от тех угроз, которые использовались в ходе тестирования... Он доказал, что система работает — и это было приятно!» —

Джереми Пратт (Jeremy Pratt), администратор сети, L.A. Times

Защита для физических и виртуальных сред

Sourcefire предлагает широкий спектр специализированных устройств для защиты сети и предотвращения угроз с пропускной способностью от 50 Мбит/с до 60 Гбит/с и более. В стандартную комплектацию любого устройства Sourcefire FirePOWER входит обходной (открытый или закрытый при отказе) медный и/или оптоволоконный интерфейс с возможностью программирования. Большинство моделей также оснащены дополнительными функциями отказоустойчивости: двойными блоками питания, дисками RAID и системами дистанционного управления (LOM).

Sourcefire также предлагает решения по обеспечению безопасности для платформ VMware, Citrix Xen и Red Hat. Виртуальные устройства Sourcefire FirePOWER предоставляют возможность проверки взаимодействия между виртуальными машинами, чтобы обеспечить им контроль и защиту на уровне физических компьютеров.

Устранение «слепых зон» в сети посредством дешифрования SSL-трафика

Шифрование SSL-трафика используется все более активно и широко в связи с распространением облачных технологий и ростом числа веб-приложений.

Устройство Sourcefire SSL может выполнять дешифрование и повторное шифрование SSL-трафика. Оно обеспечивает проверку уровня безопасности с учетом требований к производительности сети. Кроме того, данное устройство упрощает процесс централизованного управления ключами для различных функций обеспечения безопасности (таких как предотвращение вторжений, защита от утечек данных, экспертиза сети) в пределах одного развертывания.

Рис. 5. Устройство Sourcefire SSL 8200

Sourcefire Company

Компания Sourcefire теперь входит в состав корпорации Cisco

Дальнейшие шаги по реализации адаптивной защиты сети

Для получения дополнительной информации о системе IPS следующего поколения от Sourcefire и других решениях, которые обеспечивают адаптивную безопасность, свяжитесь с участником программы Sourcefire Global Security Alliance™, чтобы просмотреть демонстрационные материалы, запросить оценку на объекте или запланировать встречу. Кроме того, вы можете посетить сайт **www.sourcefire.com** или написать на эл. почту: security-request@cisco.com.

SSL-трафик часто становится мишенью для киберпреступников, которые используют следующие вредоносные программы и типы атак:

- Атаки, нацеленные на входящий трафик
- Шпионское и вредоносное ПО
- Вирусы и черви
- Фишинг
- Хищение личных данных
- Утечка информации

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