Защита от внутренних и внешних угроз информационной безопасности с помощью InfoWatch Traffic Monitor и Cisco IronPort S-Series

Неконтролируемое использование электронных каналов связи представляет собой одну из главных угроз безопасности корпоративной сети.

Через заражённые веб-сайты на компьютеры сотрудников попадают различные вирусы и шпионское ПО, а через чаты и форумы происходят утечки информации. Кроме того, нецелевое использование интернета на рабочем месте для просмотра развлекательных сайтов снижает продуктивность сотрудников и резко повышает вероятность заражения ПК различными вредоносными программами.

При построении систем защиты информационных активов компании важно сочетать традиционно-актуальные средства защиты от внешних угроз и технологии, позволяющие контролировать распространение конфиденциальных данных. Последняя задача сегодня становится все более актуальной, так как ее решение не только минимизирует риски, которые возникают в связи с умышленной или случайной утечкой информации, но и позволяет государственным и частным компаниям и организациям **соответствовать требованиям** различных стандартов и законодательных актов, в том числе **федерального закона № 152-ФЗ «О персональных данных»**.

Внешние и внутренние угрозы информационной безопасности

Информационные активы компании подвергаются постоянной угрозе, как извне, так и изнутри.

Ко внешним угрозам относятся вирусы, шпионские программы, DoS-атаки и др. Так называемый «переход к «Web 2.0» привел к образованию огромной «тёмной области» Интернет («Dark Web»), в которой более 80% содержимого не внесено в каталоги традиционных коммерческих прокси-серверов, что практически обессмыслило эти системы.

Ко внутренним угрозам информационной безопасности относятся случайные или намеренные утечки конфиденциальных корпоративных данных, нецелевое (в том числе и в криминальных целях) использование корпоративных ресурсов.

Комплексное решение для обеспечения информационной безопасности

Чтобы обеспечить защиту информационных активов компании от внешних и внутренних угроз, компании InfoWatch и Cisco представляют совместное решение – InfoWatch Traffic Monitor и Cisco IronPort S-Series.

Совместное решение InfoWatch и Cisco защищает компьютеры сотрудников и серверы компании от заражения вирусами, позволяет контролировать трафик, передаваемый по различным электронным каналам (корпоративную почтовую систему, веб, интернет-пейджеры, зашифрованный HTTPS-канал) и обрабатываемый на рабочих станциях (копируемый на съемные носители или отправляемый на печать) на предмет утечки информации и нецелевого использования корпоративных ресурсов.

Независимо от того, какого рода конфиденциальную информацию (технологическая информация, секреты производства, патентуемые изобретения или персональные данные, номера телефонов или кредитных карт и т.п.) нужно защитить, совместное решение InfoWatch и Cisco эффективно пресекает любые несанкционированные действия как со стороны сотрудников компании, так и со стороны внешних злоумышленников.

Таким образом, совместное решение успешно противодействует всем внешним и внутренним угрозам информационной безопасности в режиме реального времени.

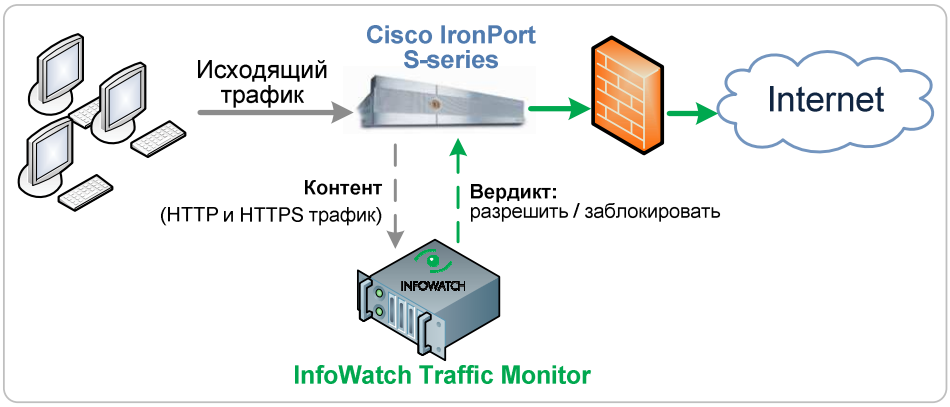

Схема работы решения

Компоненты решения

Совместное решение включает в себя систему защиты конфиденциальной информации InfoWatch Traffic Monitor и инновационную высокопроизводительную платформу безопасности Cisco IronPort, интегрированные по протоколу ICAP. Это позволяет тщательно анализировать содержимое трафика для обеспечения соответствия требованиям регулирующих органов и защиты конфиденциальных данных, проведения расследований и оптимизации бизнес-процессов.

InfoWatch Traffic Monitor осуществляет:

- мониторинг и анализ данных, отсылаемых пользователями за пределы компании,
- предотвращение утечки данных путем блокирования процесса передачи при обнаружении нарушения политики безопасности (например, пересылка конфиденциальных данных пользователем, не уполномоченным на их распространение),
- хранение и анализ всех перехваченных данных и информации об инцидентах для проведения расследований по нарушениям политик информационной безопасности.

Web-шлюзы Cisco IronPort S-Series обеспечивают безопасность входящих и исходящих данных, совмещая в себе функциональные возможности целого ряда отдельных сетевых устройств: традиционную фильтрацию URL, репутационную фильтрацию и защиту от вредоносного ПО на базе высокопроизводительного кэширующего прокси-сервера. Это позволяет существенно облегчить установку, настройку и управление безопасностью сети и снизить затраты на ее обеспечение.

Преимущества комплексного решения

- мониторинг и анализ данных, отсылаемых за пределы компании, в том числе с использованием https-протокола как на предмет обнаружения вредоносного ПО в зашифрованном трафике, так и на предмет передачи по такому каналу конфиденциальной информации
- точное детектирование конфиденциальной информации благодаря совместному использованию нескольких технологий контентного анализа и защита данных на любом этапе их жизненного цикла, в том числе и сразу после создания, когда еще не существует никаких родственных или похожих документов
- предотвращение утечки данных благодаря блокировке процесса передачи конфиденциальной информации в случае обнаружения ее несанкционированного использования
- защита от уязвимостей WEB 2.0
- анализ HTML кода на наличие вредоносных скриптов и уязвимостей в web-страницах, web почте и теле электронных сообщений и блокирование вредоносного кода
- ведущая антивирусная система, комбинирующая несколько технологий сканирования для обеспечения надежной защиты от широчайшего спектра Web-угроз
- анализ структурированных и неструктурированных данных (Deep Packet Inspection)
- контроль активности приложений на сетевом уровне
- фильтрация URL на основе сравнения web-запросов пользователя с обширной базой Web-страниц и комплексного анализа более 50-ти различных параметров, связанных с Web-трафиком и сетевой активностью
- централизованное хранение всех перехваченных данных для обеспечения доказательной базы при расследовании инцидентов в области информационной безопасности (ИБ)
- ретроспективный анализ для расследований нарушений политик ИБ (forensics)
- гибкая система отчетности
- обеспечение соответствия требованиям регулирующих органов и стандартов информационной безопасности, в том числе PCI DSS, Basel II, SOX (Sarbanes-Oxley), Федерального закона «О персональных данных» № 152-ФЗ
- сертификация ФСТЭК

Контакты:
тел.: **+7 495 22 900 22**
Российская Федерация, 123458, Москва, проезд №607, дом 30, офис 507
www.infowatch.ru
sales@infowatch.ru