InfoWatch Traffic Monitor. Интеграционное решение на основе Microsoft Forefront Threat Management Gateway 2010

С каждым годом даже рядовые нарушители политик корпоративной информационной безопасности становятся всё изощрённее, не говоря уже о профессионалах. Они легко обходят традиционные средства защиты, используя типичные «мёртвые зоны» для передачи конфиденциальных данных. Ярким примером стал шифрованный HTTPS трафик, который с одной стороны защищает сами данные в процессе передачи от внешних угроз, с другой стороны становится недоступен для анализа DLP системой. В настоящее время HTTPS трафик составляет до 50% всего объёма данных в сети Интернет, и не обращать на него внимания означает иметь мнимую уверенность в защищённости конфиденциальной информации.

В потоке шифрованного трафика могут скрываться различные угрозы, как поступающие извне - вредоносные ссылки, программы, запросы подключений, и тому подобное, так и внутренние – утечки конфиденциальной информации за пределы корпоративной сети, инициированные сотрудниками.

Общепринятым и наиболее эффективным решением по контролю за HTTPS трафиком в данном случае является совместное применение прокси-сервера и DLP систем, взаимодействующих по протоколу ICAP.

Прокси-сервер позволяет проводить первичную фильтрацию HTTPS трафика на предмет вредоносного программного обеспечения и передавать в DLP систему HTTP траффик для дальнейшего анализа его содержимого.

Интеграция InfoWatch Traffic Monitor с прокси-серверами, поддерживающими протокол ICAP, позволяет обнаруживать недозволенное содержимое в трафике, передаваемом по протоколам HTTP, HTTPS, при использовании сервисов веб-почты, обмена файлами и социальных сетей.

Компания InfoWatch активно использует интеграционные решения такого типа и постоянно расширяет линейку комплексных решений по защите от внутренних и внешних угроз на базе имеющихся интеграций с Cisco IronPor, BlueCoat Proxy SG и другими прокси-серверами.

Интеграция с Microsoft Forefront Threat Management Gateway 2010

Нетипичным случаем для реализации такого подхода стал Microsoft Forefront Threat Management Gateway 2010 (MS Forefront TMG), не имеющий поддержки протокола ICAP.

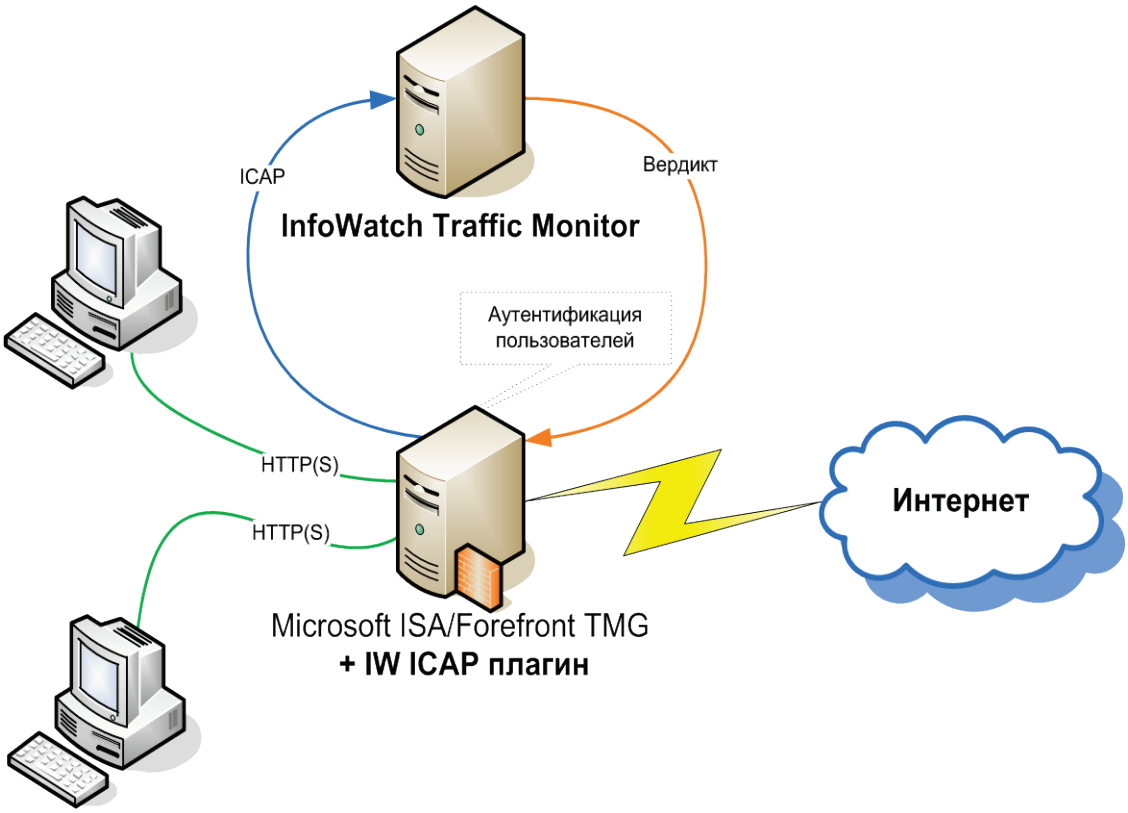
Для обеспечения связи между системами компания InfoWatch разработала специализированный ICAP плагин, который легко устанавливается за несколько минут системным администратором на MS Forefront TMG и позволяет обеим системам взаимодействовать.

MS Forefront TMG дает возможность сотрудникам безопасно и эффективно использовать Интернет для работы, не беспокоясь о вредоносных программах, обеспечивая комплексную защиту от возможных угроз:

- Фильтрация URL-адресов
- Поиск вредоносных программ
- Предотвращение вторжений
- Брандмауэр на уровне приложений и сети
- Проверка HTTP/HTTPS

InfoWatch ICAP плагин позволяет Microsoft Forefront Threat Management Gateway 2010 фильтровать веб трафик и перенаправлять его в InfoWatch Traffic Monitor для дальнейшего анализа на предмет содержания конфиденциальной информации, отсылаемой за пределы компании, и вынесения вердикта о доставке данных или их блокировке.

Схема интеграции



Преимущества интеграционного решения

- Комплексная защита от внешних и внутренних угроз:
  - Защита от вредоносного программного обеспечения
  - Мониторинг загрузок файлов и публикаций на ресурсы Twitter, Facebook, Dropbox и другие социальные сервисы по протоколам HTTP и HTTPS
  - Мониторинг использования сервисов веб почты поддерживающих HTTPS: GoogleMail, ЯндексПочта
- Точная идентификация внутренних нарушителей за счет использования стандартизированных механизмов прокси-сервера для аутентификации пользователей
- Простота внедрения в существующую инфраструктуру организации. Плагин устанавливается как дополнение к существующему прокси-серверу и ответвляет траффик в DLP систему, что не создает новых точек отказа сети
- Снижение затрат на аппаратное обеспечение и персонал в силу отсутствия необходимости использовать дополнительный прокси-сервер с поддержкой ICAP

