УДК 004

Безопасный Интернет: видимость как необходимое и достаточное

[1,2]*С. В. Конявская*, канд. филос. наук; [2,3]*В. В. Кравец*, [2]*А. Ю. Батраков*
[1] Национальный исследовательский ядерный университет «МИФИ», Москва, Россия
[2] ЗАО «ОКБ САПР», Москва, Россия
[3] Федеральное государственное унитарное предприятие «Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации», Москва, Россия

Предложен подход к обеспечению безопасного доступа к Интернету из защищенной ЛВС организации, основанный на фильтрации трафика не по содержанию, а по типу.

Ключевые слова: безопасный Интернет, фильтр, изображения экрана монитора, нажатия клавиш клавиатуры.

Интернет в чем-то похож на флешку. В том, что это такое неизбежное зло, с которым приходится смириться потому, что плюсы этого зла так очевидны и соблазнительны, что запрещать — просто бесполезно. Если Интернет запрещен на предприятии полностью, то пользователь принесет USB-модем. Хорошо, если он подключит его прямо к рабочему компьютеру, и поскольку тот, конечно, прекрасно оборудован в смысле информационной безопасности, это сразу создаст инцидент, который приведет к блокировке неразрешенного действия и воспитательным мерам в отношении нарушителя. Хуже, ибо сложнее обнаружить, если пользователь использует Интернет на собственном устройстве, не подключенном к корпоративной сети, а значит, неконтролируемом, а затем из лучших побуждений переносит полученную информацию — вместе с вирусами и другими потенциально опасными объектами — в корпоративную сеть. Способов для этого много — от электронной почты, до тех же флешек.

Компромиссным вариантом является решение с выделенными рабочими местами, специально отведенными для работы с Интернетом. При организации разного рода санитарных зон и других полуорганизационных мер это позволяет получать из сети данные только после того, как их безопасность подтверждена, и есть шанс, что не ошибочно. Однако это решение и не до конца безопасное (зависит от строгости организационных мер и качества санитарной зоны), и неудобное для пользователей.

Любой другой способ избежать негативных влияний Интернета, кроме его полного запрета в корпоративной сети, как правило, тоже оказывается не вполне эффективным. В лучшем случае (при наличии ощутимых инвестиций в такие технические средства, как межсетевые экраны и системы обнаружения вторжений, значительных усилий по принятию организационных мер, систематически обновляемых антивирусов, желательно нескольких разных, а также профессиональных и ответственных сотрудников, все это тщательно настраивающих и ответственных пользователей, не старающихся все это обойти) удается добиться того, что инциденты, связанные с атаками из Интернета, становятся редки и не приносят значительного урона. Это очень хороший результат.

Однако такой результат заставляет задуматься над поиском принципиально другого подхода. Такого, который сочетал бы в себе плюсы полной изоляции корпоративной сети от Интернета с плюсами наличия Интернета на каждом рабочем месте и в то же время был лишен минусов обоих подходов.

В поисках подхода к реализации такого решения мы обратились к истории.

На заре своего развития Интернет был безопасным. Это достигалось не за счет того, что были установлены мощные межсетевые экраны и серьезное антивирусное ПО. Все проще — Интернет просто технологически не предоставлял возможности загрузить вирус, выполнить вредоносный код или как-то обмануть пользователя. Но Интернет развивался, "осваивая " все больше и больше различных технологий — javascript, Java-апплеты, свободная возможность скачивать файлы.

Конявская Светлана Валерьевна, заместитель генерального директора, доцент, преподаватель кафедры "Защита информации".
E-mail: cd@okbsapr.ru
Кравец Василий Васильевич, аспирант, программист.
E-mail: vkravec@okbsapr.ru
Батраков Антон Юрьевич, начальник отдела программирования.
E-mail: abatrakov@okbsapr.ru

Статья поступила в редакцию 14 июня 2014 г.

Идеально было бы вернуться в светлое прошлое, когда все эти технологии еще только зарождались и не могли нанести вред пользователям, но так, чтобы Интернет не потерял свой привычный вид.

Слово "вид", на взгляд авторов, ключевое. Визуальная информация — это 90 % всей воспринимаемой человеком информации. Что если ею и ограничиться? Тогда задачу защиты пользователя от всех возможных угроз можно свести к защите передачи изображений. Изображение не может нести с собой угрозу безопасности (на самом деле может, но в рамках решаемой задачи этим весьма специфическим случаем можно и пренебречь). Значит, достаточно организовать пользователю безопасный канал, по которому он может получать изображения, — и безопасный Интернет у нас в кармане. Практически — "серебряная пуля".

В качестве прикладной реализации описанного подхода предлагается технология одновременной изолированной работы пользователя с корпоративной сетью и Интернетом на одном рабочем месте в рамках двух независимых терминальных сессий с их одновременным отображением на экране одного монитора в разных "окнах". Естественно комфортный режим работы пользователя подразумевает использование при работе в обеих сессиях одного и того же комплекта элементов управления и отображения АРМ (клавиатура, мышь, монитор, принтер).

Взаимовлияние между корпоративной сетью и Интернетом в предложенной технологии исключено на 1—4 уровнях модели ISO/OSI.

Это основное, системообразующее требование. Однако для комфортного и "бесшовного" введения технологии в систему необходимо выполнение еще и ряда дополнительных требований:

- активные компоненты системы, обеспечивающие работу в режиме двух терминальных сессий, должны вести журналы событий;
- события должны фиксироваться в аппаратном журнале, память которого доступна только для операции дополнения (т. е. события нельзя удалить или перезаписать);
- должны быть предусмотрены программные средства обработки журналов событий и описан порядок их использования;
- должна быть предусмотрена возможность отправки оперативных оповещений Администратору ИБ в случае наступления критичных с точки зрения безопасности событий;
- порядок работы пользователя в режиме двух терминальных сессий не должен требовать специальных навыков и знаний или оказывать негативное влияние на производительность его труда.

Описание предлагаемого решения

Предполагаемую корпоративную сеть представим в виде терминальной системы, в которой пользователь работает с терминальным сервером по RDP.

Предполагается, что терминальный сервер и терминальный клиент, а также их взаимодействие защищены надлежащим образом, этот аспект не будет рассматриваться, чтобы не запутывать описание решения.

На этом терминальном сервере — будем называть его "функциональный терминальный сервер" (ФТС) — нет ни браузера, ни каких других средств и инструментов работы с Интернетом.

К той же локальной сети, через которую взаимодействуют терминальные клиенты с ФТС, подключен другой терминальный сервер, но не напрямую, а через специальный фильтр, как показано на рис. 1.

Это терминальный сервер (ТС) под управлением ОС Linux, имеющий соединение с Интернетом. На терминальном сервере опубликован браузер.

На рис. 1 в качестве терминального клиента показана ПЭВМ с ОС Windows, однако с тем же успехом может быть тонкий клиент под управлением ОС Linux, в том числе, загружаемой по сети (или локально с отчуждаемого устройства).

Рис. 1. Структурная схема комплекса технических средств решения

Обмен данными между ТС и Интернетом производится в штатном порядке, без ограничения и/или изменений. Для соединения с Интернетом у ТС предусмотрена отдельная сетевая карта.

На терминальный сервер установлен полный комплект средств защиты информации: средства защиты от воздействия вредоносных кодов, средство обнаружения вторжений, межсетевой экран, ПАК СЗИ НСД "Аккорд-X".

Через отдельный сетевой интерфейс (вторую сетевую карту) ТС взаимодействует с аппаратным комплексом с функциональностью фильтра (Фильтр "Рассвет").

Фильтр также оборудован двумя сетевыми картами. Через одну из них Фильтр взаимодействует с ТС. В фильтр передаются все команды и данные от ТС, которые не были заблокированы МЭ, СОВ, СЗ ВВК или ПАК СЗИ НСД "Аккорд-X".

От фильтра на ТС передаются только нажатия клавиш клавиатуры и движение мыши. Все команды и данные, не являющиеся нажатиями клавиш клавиатуры и/или движениями мыши, не передаются на ТС, а попытка их передачи фиксируется в журнале событий.

Через другой сетевой интерфейс (вторую сетевую карту) фильтр взаимодействует с ЛВС предприятия. От фильтра в ЛВС передаются только изображения рабочего стола. Все команды и данные, не являющиеся изображениями рабочего стола, не передаются в ЛВС, а попытка их передачи фиксируется в журнале событий.

От ЛВС в фильтр передаются все данные и команды без ограничений.

Взаимодействие пользователя с ЛВС производится через установленный на АРМ пользователя модифицированный RDP-клиент (далее RDP-клиент "Рассвет"). Для пользователя взаимодействие происходит обычным порядком, без изменений, все изменения взаимодействия от него скрыты. Он работает параллельно в окне браузера и в окне сессии с ФТС.

Схематично взаимодействие компонентов системы показано на рис. 2.

Фильтр "Рассвет"

Очевидно, что главной активной частью решения является Фильтр, поэтому на его описании остановимся подробнее.

Фильтр представляет собой устройство серверного типа с двумя сетевыми картами, минимум двумя USB-портами для подключения аппаратных неперезаписываемых журналов и кнопкой выключения коммутации на внешней стороне корпуса.

Эта кнопка необходима для того, чтобы в случае возникновения нештатной ситуации администратор информационной безопасности (АИБ) (или иное уполномоченное лицо) мог физически отключить сетевое взаимодействие корпоративной сети и Интернета.

Наличие кнопки отключения на внешней стороне корпуса детерминирует размещение фильтра в помещение, для которого обеспечен контроль доступа и приняты меры, не допускающие несанкционированного нажатия этой кнопки.

В состав фильтра входит предустановленное ПО «Фильтр-Рассвет», обеспечивающий фильтрацию RDP таким образом, чтобы от ЛВС на ТС передавались только нажатия клавиш клавиатуры и движения мыши, а от ТС в ЛВС передавались только изображения рабочего стола. Любые другие команды и/или данные блокируются и информация об этом заносится в журнал событий Фильтра.

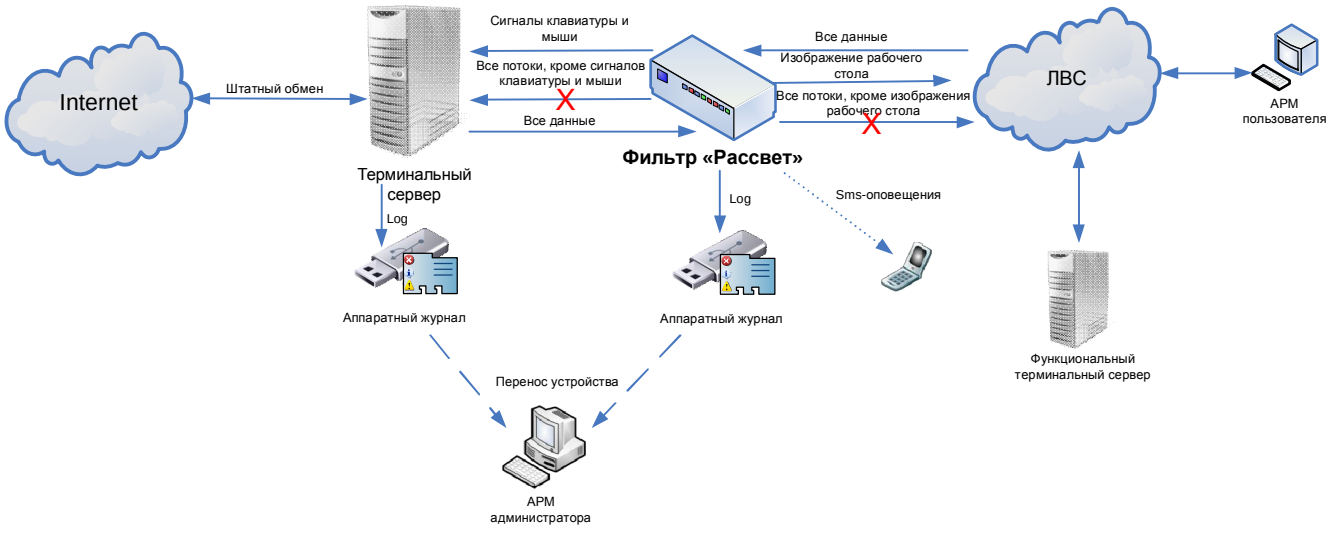

Рис. 2. Функциональная схема решения

Дополнительно данное ПО реализует сервис оперативных оповещений (например, в форме sms-оповещений) о событиях безопасности на телефон АИБ с целью обеспечения возможности безотлагательного принятия мер в случае возникновения необходимости. Перечень событий и способ оповещения настраивается. Одним из событий, о котором настроено оповещение по умолчанию, — заполнение журнала на N % (количество процентов заполнения настраивается).

Также ПО реализует порядок фиксации событий фильтра таким образом, чтобы события сохранялись только на аппаратный неперезаписываемый журнал.

Работа с журналами

Все события, трактуемые любым из средств, установленных на ТС, как события безопасности, фиксируются в журналах событий. Настройками ПАК СЗИ НСД "Аккорд-X" обеспечен режим, при котором журналы событий записываются не на жесткий диск или иное хранилище, а только на подключенный к ТС аппаратный неперезаписываемый журнал.

Все события Фильтра "Рассвет" также записываются не на жесткий диск или иное хранилище, а только на подключенный к ТС аппаратный неперезаписываемый журнал. Это обеспечивается настройками ПО "Фильтр-Рассвет".

Аппаратный неперезаписываемый журнал создан на основе служебного носителя "Секрет" и представляет собой USB-устройство с диском типа mass-storage объемом 4 ГБ. Диск устройства состоит из двух разделов. На открытом разделе диска, которому при производстве присвоен атрибут Read Only, находится ПО "Секретный агент". Закрытый диск предназначен для записи журналов событий и на этапе производства ему присвоен атрибут Add Only. Устройство имеет активный универсальный процессор, внутреннее ПО которого реализует протокол взаимной аутентификации с СВТ, к USB-порту которого его подключают.

Работа с диском аппаратного журнала на чтение или запись возможна только на тех средствах вычислительной техники (СВТ), которые заранее зарегистрированы в журнале в качестве разрешенных. На любых других СВТ диск устройства не будет примонтирован, и оно не будет определяться в системе как "съемный диск", значит, не будет доступно ни на чтение, ни на запись. Рекомендуется, чтобы в качестве разрешенных регистрировались только сами ТС и/или Фильтр "Рассвет", АРМ работы с журналами, и больше никакие.

Все случаи подключений (как успешные, так и неуспешные) записываются в собственный журнал устройства, доступный для просмотра только его администратору.

Для чтения и анализа журналов, записанных на аппаратный неперезаписываемый журнал на ТС или Фильтре, АИБ (или иное лицо, в обязанности которого входит анализ журналов) использует АРМ, на котором установлено специальное ПО "log-Рассвет".

Дополнительно, на случай возникновения событий, требующих незамедлительной реакции от АИБ, в системе предусмотрено оповещение АИБа о событиях Фильтра и/или ТС.

С помощью ПО работы с журналами на ТС и Фильтре реализуется порядок, который предусматривает переход к сохранению событий на последнее подключенное устройство. Когда необходимо обработать данные с одного аппаратного неперезаписываемого журнала, АИБ подключает к свободному USB-порту второе устройство, и записи о событиях автоматически начинают сохраняться на него, а первое устройство можно отключать и переносить на АРМ работы с журналами для анализа.

Для реализации такого порядка работы на ТС и Фильтре должно быть доступно не менее 2-х USB-портов.

RDP-клиент "Рассвет"

Это модифицированный RDP-клиент, имеющий только 3 функции:

1) передача позиции курсора мыши;

2) передача нажатий клавиш клавиатуры;

3) прием и визуализация изображения рабочего стола и лишенный возможности расширения функций за рамки перечисленных.

Такая система позволяет построить технологию работы с двумя терминальными сессиями с обеспечением ключевых требований:

– не снижается защищенность работы пользователей с корпоративной сетью (в описанной модели — с защищенным ФТС),

– повышается комфортность работы пользователей,

– предоставлена возможность аудита и анализа инцидентов.

Защищенность

Защищенность обеспечивается изолированностью сессий друг от друга на уровнях модели ISO/OSI с 1 по 4 включительно (1 уровень — физический —

2 отдельные сетевые карты у ТС и фильтра; 2-й уровень — канальный, преобразование Ethernet-пакетов; 3-й уровень — сетевой, использование МЭ, 4-й уровень — транспортный, фильтр протокола RDP).

Комфортность работы пользователя

Пользователь работает в привычном режиме и при этом нет необходимости переходить на выделенное рабочее место для работы с Интернетом.

Аудит и анализ инцидентов

Предусмотрена возможность защищенного хранения журналов событий, на специальном носителе, исключающим случайное или преднамеренное удаление журналов кем-либо, включая АИБ.

Предусмотрена возможность работы с журналами с помощью специального ПО на специальном рабочем месте. Также предусмотрена возможность ограничения числа компьютеров, на котором аппаратные журналы из состава системы могут быть доступны на запись и/или чтение с целью ограничения доступа к содержащимся в них данным и исключения несанкционированного уничтожения данных (намеренного — с целью сокрытия инцидента, или непреднамеренного — в результате ошибки или воздействия вредоносного кода).

На первый взгляд, решение выглядит несколько экзотически. Однако оно в полной мере воплощает мечту о "старом добром безопасном Интернете", сохраняющим в то же время все столь дорогие пользователю возможности. В зависимости от выбранной политики можно так настроить среду работы пользователя с Интернетом в описанной системе, чтобы создать видимость работы вообще без каких-то особых ограничений. Например, пользователь не сможет "прицепить" к веб-форме файл, находящийся на ФТС, однако если возможность прицеплять файлы действительно нужна пользователю, то можно позволить ему создавать файлы на ТС и прицеплять их, куда необходимо. То же со скачиванием файла — он не сможет скачать его на свою флешку или на ФТС, но если владелец системы сочтет такую возможность уместной и полезной для работы пользователю может быть позволено скачивать файлы на ТС. Это никак не нарушит безопасность функциональной системы, так как все эти файлы будут всегда оставаться за Фильтром, а на терминальный клиент будут передаваться только изображения. Пользователь будет его видеть, а этого ему более чем достаточно.

Harmless Internet: visibility as necessary and sufficient

[1,2]*S. V. Konyavskaya*, [2,3]*V. V. Kravec*, [2]*A. Yu. Batrakov*
[1] National Research Nuclear University "MEPhI", Moscow, Russia
[2] OKB SAPR JSC, Moscow, Russia
[3]All-Russia Scientific Research Institute of Computer Technology and Informatization Problems (VNIIPVTI), Moscow, Russia

The approach for improving harmless Internet work inside of protected LAN is offered in the article, based on filtering the traffic, but in the aspect of the kind of traffic, not the content.

Keywords: harmless Internet, filter, screenshots, button press.

Received June 14, 2014