9. Осипов М.Н., Попов М.А., Попова Т.А. Поведение выходного сигнала в системе измерения на основе оптоэлектронного интерферометра Майкельсона // Ползуновский вестник. 2011. № 3/1. С. 38–41

10. Осипов М.Н., Хохлов В.А., Чекменев А.Н. Развитие цифровой спекл интерферометрии для исследования динамических процессов в реальном времени // Вестник СамГУ. 2013. № 9/2 (110). С. 109-117.

П.Н. Полежаев, Л.С. Адрова

РАЗРАБОТКА АРХИТЕКТУРЫ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В КОРПОРАТИВНЫХ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЯХ

(Оренбургский государственный университет)

В настоящее время существующие технологии управления корпоративными сетями обладают целым рядом недостатков, включая:

а) ограниченные возможности по управлению трафиком в существующих сетевых протоколах (приоритизация, QoS, управление перегрузками, состоянием полос);

б) проблему выбора мест установки для программно-аппаратных инструментов защиты (IDS, DLP-сенсоров, межсетевых экранов и т.п.);

в) индивидуальное задание правил функционирования для каждого инструмента (ошибки конфигурирования);

г) огромное количество активных протоколов (более 600);

д) необходимость наличия высококвалифицированных специалистов для настройки оборудования и/или разработки собственных сетевых решений;

е) большая стоимость и закрытость сетевого оборудования и инструментов защиты.

Для решения обозначенных проблем может быть использована технология программно-конфигурируемых сетей (ПКС) [1]. Принципы работы ПКС детально описаны в [2], в рамках данной публикации сосредоточимся на описании архитектуры системы защиты информации в ПКС, разрабатываемой в качестве компонента системы управления корпоративными ПКС [3].

В рамках данного исследования была предложена архитектура системы защиты информации в корпоративной программно-конфигурируемой сети, изображенная на рисунке 1. Данная архитектура включает в себя ряд модулей, которые должны быть разработаны для системы защиты информации:

а) Модуль аутентификации – поддерживает аутентификацию узлов/пользователей средствами ОС и/или с использованием RADIUS-сервера.

б) Модуль топологии и состояния сети – собирает информацию о топологии сети и состоянии сети с помощью протоколов ARP, LLDP и SNMP. С помощью SNMP-агентов возможен детальный сбор сведений со всех сетевых устройств, включая загруженность вычислительных ресурсов серверов, состояние очередей на портах коммутаторов.

в) Модуль межсетевого экрана – реализует межсетевой экран (пакетный фильтр), распределенный по всем коммутаторам OpenFlow, что обеспечивает блокировку нелегитимных пакетов на первом коммутаторе сразу после их попадания в сеть. В отличие от решений, ориентированных на размещение экрана на границе сетей, здесь фильтрацию осуществляет каждый коммутатор OpenFlow, что обеспечивает дополнительную защиту от инсайдеров и вирусов, попадающих на компьютеры обычных пользователей.

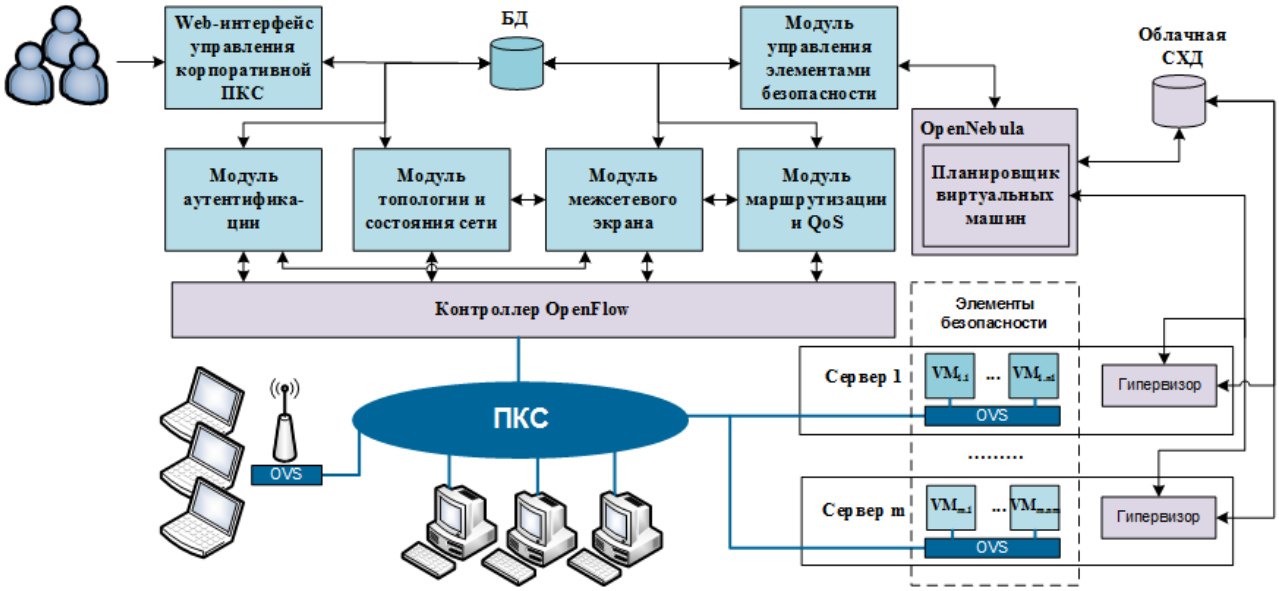

Рис. 1. Архитектура системы защиты информации
в корпоративной программно-конфигурируемой сети

г) Модуль маршрутизации и обеспечения QoS – реализует алгоритм вычисления для потока оптимального маршрута передачи данных с учетом текущего состояния сети и требований к его качеству, например, минимальной гарантированной пропускной способности, максимальной гарантированной задержки, джиттера и т.п. Данный модуль прокладывает вычисленный маршрут путем установки в таблицы потоков коммутаторов OpenFlow правил передачи пакетов. Возможны два режима работы данного модуля: проактивный и реактивный. Проактивный позволяет прокладывать маршруты передачи данных вычислительных распределенных задач до их запуска, при условии, если известен их коммуникационных шаблон. Реактивный – прокладывает маршрут в момент обнаружения одним из коммутаторов OpenFlow первого пакета нового потока данных, что приводит к дополнительным задержкам в его обработке.

д) Web-интерфейс управления корпоративной ПКС – должен быть основан на одной из существующих систем мониторинга корпоративными сетями, например, Zabbix или Nagios. Он будет предоставлять широкий функционал для различных типов пользователей: аутентификацию и управление задачами – для обычных пользователей; мониторинг безопасности сети, средства для настройки межсетевого экрана, создания, настройки и обновления элементов безопасности, задания настроек аутентификации – для специалистов по инфор-

мационной безопасности; настройки параметров маршрутизации и QoS, сбора информации по сетевой статистике, мониторинга сети и т.п. – для системного администратора. По сути Web-интерфейс выступает единой точкой управления программно-конфигурируемой сетью, в том числе для задания в централизованном месте (а не на множестве отдельных сетевых устройств) правил межсетевого экрана, сигнатур системы обнаружения вторжений и т.п.

е) Модуль управления элементами безопасности – решает задачи по запуску/остановке, установке, настройке и обновлению элементов безопасности. Также реализует балансировку нагрузки на однотипные элементы безопасности с учетом статистики SNMP, собираемой с них с помощью модуля топологии и состояния сети. В своей работе модуль взаимодействует с системой управления облачными ресурсами OpenNebula.

ж) Элементы безопасности – виртуальные машины, содержащие установленные сканеры безопасности потоков данных. Они включают систему обнаружения вторжений Snort, прокси-серверы, антивирусы, DLP-анализаторы и т.п. Может быть создано множество экземпляров виртуальной машины каждого типа с целью обработки больших объемов сетевого трафика корпоративной сети. Масштабирование количества экземпляров осуществляется модулем управления элементами безопасности.

и) БД – база данных, содержащая: сведения для идентификации и аутентификации пользователей (могут быть выделены в отдельную БД с точки зрения безопасности); топологию и состояние сети; правила межсетевого экрана; сведения о проложенных маршрутах и выполняющихся вычислительных задачах; информацию, необходимую для Web-интерфейса; сведения о текущем состоянии, типе и размещении элементов безопасности; информацию о политиках безопасности.

Модули а)-г) должны быть разработаны в виде приложений для контроллера OpenFlow.

Заимствованные модули:

а) Контроллер OpenFlow;

б) система управления облачными ресурсами OpenNebula;

в) облачная система хранения данных (СХД);

г) гипервизоры (KVM и Xen);

д) программный коммутатор OpenFlow OVS (OpenVSwitch).

Основная идея предлагаемой архитектуры заключается в том, что для каждого потока данных в разрешающих правилах межсетевого экрана дополнительно могут быть указаны типы элементов безопасности, через которые он должен пройти или на которые он должен быть дублирован (см. рисунок 2). Как правило, модули, на которые трафик дублируется, например, система обнаружения вторжений или DLP-сенсор, вкладывали бы значительную задержку в передачу пакетов потоков данных, если бы трафик проходил через них. В случае же дублированного трафика, они могут его буферизировать и сканировать целиком или делать выборочный анализ. В случае обнаружения угрозы, они должны оповещать о ней модуль управления элементами безопасности.

Заметим, что при этом модуль управления элементами безопасности должен обеспечить нужное количество экземпляров необходимых виртуальных машин. А модуль маршрутизации и обеспечения QoS должен правильно проложить маршруты и реализовать дублирования на определенных коммутаторах OpenFlow.

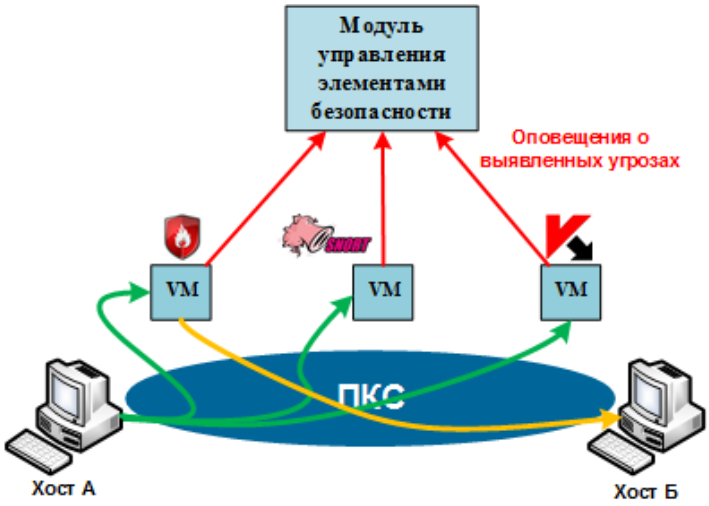

Рис. 2. Прохождение разрешенного потока данных через требуемые элементы безопасности

Основные достоинства предложенной архитектуры системы защиты информации в корпоративной сети:

а) поддержка аутентификации узлов/пользователей;

б) модульность и расширяемость

в) поддержка конфигурирования и мониторинга сети в одном месте;

г) эластичность и масштабируемость – возможность подстраиваться под текущую загруженность сети организации, что приводит к более эффективному использованию вычислительных мощностей;

д) перехват и проверка всех потоков данных между любой парой узлов, а не только на границе – приводит к значительному повышению уровня безопасности корпоративной программно-конфигурируемой сети.

Работа выполнена при поддержке Президента Российской Федерации, стипендия для молодых ученых и аспирантов (СП-2179.2015.5).

Литература

1. Адрова Л.С., Полежаев П.Н. Разработка системы управления корпоративными сетями на основе технологии программно-конфигурируемых сетей // Перспективные информационные технологии (ПИТ 2014):труды Международной научно-технической конференции /под ред. С.А. Прохорова. - Самара: Издательство Самарского научного центра РАН, 2014С. 301-305.

2. McKeown N., Anderson T., Balakrishnan H., Parulkar G., Peterson L., Rexford J., Shenker S., Turner J.; Openflow: enabling innovation in campus networks // ACM SIGCOMM Computer Communication Review, 2008, vol. 38, p. 69-74.

3. Полежаев П.Н., Ушаков Ю.А., Шухман А.Е. Система управления ресурсами для высокопроизводительных вычислений, основанная на использовании программно-конфигурируемой сети // "Системы управления и информационные технологии: научно-технический журнал", 2013. - №4(54). - С. 65-69.

Д.А. Рыбаков

ЗАЩИТА ДОКУМЕНТОВ ПО ПРИНЦИПУ “ЗАПРЕЩЕНО ВСЁ, ЧТО НЕ РАЗРЕШЕНО”

(EPAM Systems)

В 1990х годах сложность систем таких как MS-DOS или Linux была невысокой, и поэтому было под силу разобраться одному специалисту и полностью взять её под контроль. Пара сотен системных функций, небольшие объемы данных, несколько программ вполне укладывались в голове одного человека и было совершенно понятно, что делает система и с чем взаимодействует. На данный момент сложность информационных систем возросла до такого уровня, что трудно достоверно сказать, чем занимается операционная система помимо основных своих обязанностей. Плюс большое количество программ, которые так и лезут в компьютер со всех уголков интернета. Эти тенденции делают жизнь простого пользователя совершенно непредсказуемой, когда дело касается сохранения конфиденциальной информации.

Несмотря на такое возрастающее разнообразие, фирма Microsoft неуклонно реализует принцип защиты “разрешено всё, что не запрещается”, а запрещается не так уж и много, то есть по большому счету информация остается слабозащищённой. Такой подход имеет свои положительные стороны, так как система всегда выполняет множество своих функций, что сильно уменьшает время настройки и развертывания, что выгодно с коммерческой точки зрения и не требует специальных навыков от пользователя. Но за это приходится платить повышенными рисками и необходимостью иметь антивирусы, которые потребляют ощутимую часть ресурсов. Задача администратора системы при таком подходе – затыкать бреши в защите по мере их обнаружения.

Другое отношение к защите имеет операционная система Unix. В ней реализуется принцип “запрещено всё, что не разрешено”. То есть по умолчанию большинство возможностей закрыты, и администратор дает разрешения и открывает доступы к различным службам, файлам, устройствам по мере необходимости. Такой подход увеличивает время развертывания и настройки, зато сокращает последующие расходы на сопровождение и делает систему более предсказуемой.

Не отрицая ни первого, ни второго подхода автор предлагает гибридный подход к защите файлов. Для значимой информации предлагается реализовать жесткий принцип “запрещено всё, что не разрешено”. А для остального боль-