УДК 519.687

Бахарева Н.Ф., Полежаев П.Н., Шухман А.Е., Ушаков Ю.А.
Оренбургский государственный университет
E-mail: newblackpit@mail.ru

УПРАВЛЕНИЕ КОРПОРАТИВНЫМИ ПРОГРАММНО-КОНФИГУРИРУЕМЫМИ СЕТЯМИ

Существующие решения для корпоративных сетей обладают целым рядом недостатков. Прежде всего, существует проблема выбора мест установки инструментов защиты информации корпоративной сети, которые, как правило, размещаются на границе подсетей. Это приводит к тому, что они обрабатывают только тот трафик, который через них передается, а это снижает уровень безопасности сети. Также существует проблема эффективной маршрутизации сетевого трафика одновременно с обеспечением качества обслуживания на должном уровне.

Для решения данных проблем предложено использовать технологию программно-конфигурируемых сетей (ПКС). На ее базе разработана архитектура прототипа системы защиты корпоративных ПКС, включающая реализации: алгоритма межсетевого экрана, алгоритма аутентификации пользователей и их компьютеров, алгоритма маршрутизации сетевого трафика и обеспечения QoS.

Алгоритм аутентификации для корпоративных ПКС поддерживает технологии IEEE802.1x, протоколов EAP, RADIUS, LDAP, стандарта WPA2-EAP. ПКС используется для изоляции потоков данных различных пользователей с возможностью создания произвольного количества изолированных виртуальных сетей без ограничений VLAN, а также для контроля разграничения доступа за счет функций межсетевого экранирования.

Проведенные экспериментальные исследования прототипа и анализ их результатов показали эффективность и пригодность разработанных алгоритмов для корпоративных ПКС. Полученные результаты могут быть использованы для развертывания корпоративных ПКС на предприятиях Оренбургской области.

Ключевые слова: программно-конфигурируемые сети, корпоративные сети, аутентификация, маршрутизация, QoS, межсетевое экранирование.

В настоящее время большинство средних и крупных компаний Оренбургской области имеют корпоративные сети, обеспечивающие функционирование их ИТ-инфраструктур. Как правило, они используются для развертывания различных корпоративных и бизнес-приложений, необходимых для эффективной работы компаний.

В рамках данной НИР предлагается реализация корпоративных сетей с помощью инновационной технологии программно-конфигурируемых сетей [1], [2]. Их использование позволит решить ряд проблем: проблему обеспечения безопасности, эффективной маршрутизации и обеспечения QoS, упрощение управления сетью.

Архитектура системы управления корпоративной ПКС

В рамках данного исследования была предложена архитектура системы управления корпоративной программно-конфигурируемой сетью, изображенная на рисунке 1.

Данная архитектура включает в себя ряд модулей [3]–[5]:

а) Модуль аутентификации – поддерживает аутентификацию узлов/пользователей средствами ОС и/или с использованием RADIUS-сервера. Возможен вариант, когда пользователь аутентифицируется средствами IEEE802.1x или с помощью ввода логина и пароля на отдельном сайте.

б) Модуль топологии и состояния сети.

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. Реализованный алгоритм описан детально в статьях [6], [7].

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. В основе работы данного модуля лежит алгоритм, описанный в [8].

д) Web-интерфейс управления корпоративной ПКС.

е) Модуль управления элементами безопасности.

ж) Элементы безопасности – виртуальные машины, содержащие установленные сканеры безопасности потоков данных.

и) БД – база данных.

Более детально принципы работы данных модулей описаны в [5].

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

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.

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.

Описанная архитектура была реализована в разработанном прототипе.

Алгоритм аутентификации пользователей, устройств и приложений корпоративной сети

Пусть $ILANs = \{ILAN_i\}_i$ – множество всех изолированных сетей корпоративной ПКС. Каждая изолированная сеть $ILAN_i$, поддерживаемая ПКС, может быть описана множеством идентификаторов хостов (сетевых устройств) $HostId_{ij}$, которые к ней подключены:

$$ILAN_i = \{HostId_{ij}\}_j .$$

Каждый идентификатор формализуется в виде следующего кортежа:

$$HostId_{ij} = (User_{ij}, MAC_{ij}),$$

где $User_{ij}$ – уникальный идентификатор (логин) пользователя, MAC_{ij} – MAC-адрес сетевого интерфейса его компьютера.

Пусть функция $id(HostId_{ij}) \subseteq ILANs$ возвращает множество изолированных сетей, к которым относится данный хост.

Модуль аутентификации контроллера OpenFlow поддерживает список активных хостов $ActiveHosts$ – хостов пользователей, аутентифицированных в сети. Каждый раз, когда модуль межсетевого экрана получает пакет, он передает его модулю аутентификации, который извлекает из пакета $HostId$ отправителя и $HostId'$ получателя. Затем модуль аутентификации осуществляет следующую проверку:

$$id(HostId) \cap id(HostId') \neq \varnothing ,$$

т. е. проверяет наличие общей изолированной сети. Если утверждение истинное, то модуль

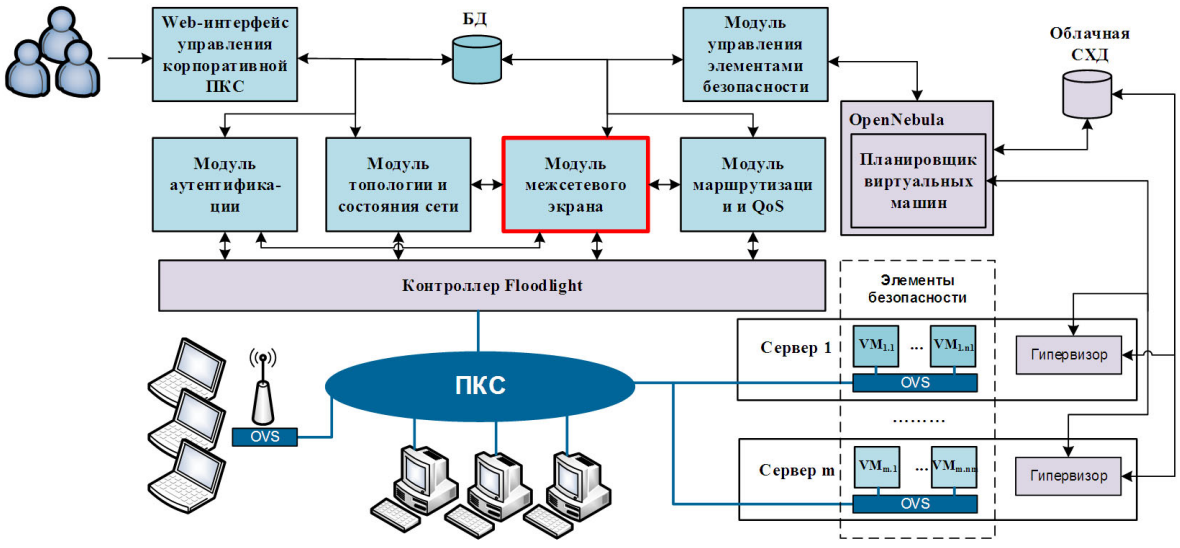

Рисунок 1. Архитектура системы управления корпоративной ПКС

аутентификации возвращает модулю межсетевого экрана положительный ответ, иначе – отрицательный. При отрицательном ответе модуль межсетевого экрана без дальнейших проверок устанавливает блокирующее правило в коммутатор OpenFlow, являющийся источником пакета. Такой подход реализует изоляцию без использования VLAN.

Опишем предложенный алгоритм аутентификации для корпоративной ПКС:

Шаг 1. При присоединении к сети компьютера (беспроводного устройства через WPA2-EAP, проводного компьютера) у пользователя запрашиваются данные для аутентификации на RADIUS-сервере (логин и пароль, сертификат безопасности и т. п.).

Шаг 2. Эти данные аутентификатором (OpenFlow-коммутатором или точкой доступа с поддержкой OpenFlow) пересылаются RADIUS-серверу в виде сообщения «RADIUS Access Request».

Шаг 3. RADIUS-сервер отправляет запрос на получение данных о пользователе LDAP-серверу.

Шаг 4. Если данный пользователь существует в LDAP и данные, предоставленные для аутентификации, верны, то:

Шаг 4.1. RADIUS-сервер сохраняет в LDAP информацию о подключении пользователя.

Шаг 4.2. RADIUS-сервер оповещает модуль аутентификации контроллера OpenFlow об аутентификации нового пользователя и передает ему его $HostId = (User, MAC)$.

Шаг 4.3. Модуль аутентификации контроллера OpenFlow добавляет полученный $HostId$ в список активных хостов:

$$ActiveHosts := ActiveHosts \cup \{HostId\}.$$

Шаг 4.4. RADIUS-сервер шлет аутентификатору ответ «RADIUS Access Accept», тот передает ответ об успешности хосту.

Шаг 4.5. Хост запрашивает через DHCP выделяемый адрес IP, шлюз, IP-адреса первичного и вторичного DNS-серверов и пр. сведения (сообщение DHCPDISCOVER).

Шаг 4.6. Коммутатор OpenFlow, к которому подключен хост, передает пакет DHCP-запроса контроллеру OpenFlow.

Шаг 4.7. Модуль межсетевого экрана определяет тип пакета и проверяет разрешение на выполнение DHCP-запроса, для этого он использует собственную базу правил $FWRules$.

Шаг 4.8. Если запрос разрешен, то:

Шаг 4.8.1. Модуль межсетевого экрана передает его модулю маршрутизации и обеспечения QoS, который прокладывает прямой и обратный маршруты между DHCP-сервером и хостом (путем установки FORWARD-правил в таблицы потоков коммутаторов OpenFlow, расположенных вдоль маршрута).

Шаг 4.8.2. DHCP-сервер выделяет IP-адрес и шлет хосту ответ DHCPOFFER, который передается до хоста по установленному маршруту.

Шаг 4.8.3. Хост, получив настройки, шлет ответ подтверждения выбора DHCPREQUEST по установленному пути.

Шаг 4.8.4. DHCP-сервер, получив от хоста DHCPREQUEST, шлет ему подтверждение DHCPACK по обратному пути.

Шаг 4.8.5. Хост, получив ответ от DHCP-сервера, применяет настройки для своего сетевого интерфейса.

Шаг 4.9. Иначе – если DHCP-запрос запрещен, то в коммутатор OpenFlow, устанавливается правило удаления пакетов потока и соответствующий запрос удаляется.

Шаг 5. Иначе, если пользователь не существует в LDAP или данные, предоставленные для аутентификации, не верны, то:

Шаг 5.1. RADIUS-сервер шлет аутентификатору ответ «RADIUS Access Reject», а тот передает ответ об отказе хосту.

Шаг 5.2. RADIUS-сервер добавляет в журнал сообщение о попытке аутентификации.

При отсутствии поддержки IEEE802.1x на устройстве пользователя, он пускается через неавторизованный порт, но только на сервер Web-аутентификации. При этом ему предварительно в обязательном порядке разрешается доступ к DHCP-серверу, который выделяет IP-адрес устройству пользователя. В этом случае в роли аутентификатора будет выступать приложение Web-аутентификации.

При отключении клиента RADIUS-сервер сохраняет эту информацию в соответствующей записи LDAP-сервера, а также оповещает об этом модуль аутентификации контроллера OpenFlow, передав ему $HostId$. В этом случае контроллер удаляет $HostId$:

$$ActiveHosts := ActiveHosts \setminus \{HostId\}.$$

Разработанный алгоритм аутентификации для корпоративных ПКС поддерживает технологию IEEE802.1x, протоколы EAP, RADIUS, LDAP, стандарт WPA2-EAP.

Методика проведения экспериментальных исследований

Разработанная методика экспериментальных исследований прототипа системы управления корпоративной ПКС включает отдельное исследование следующих разработанных решений: алгоритма маршрутизации и обеспечения QoS, алгоритма межсетевого экрана, алгоритма аутентификации пользователей и их устройств. Для исследования был собран экспериментальный образец корпоративной ПКС, описанный в [5].

Для исследования алгоритма маршрутизации и обеспечения QoS было предложено в дисковый образ виртуальных машин, имитирующих клиентские компьютеры, установить инструмент D-ITG для генерации тестовых потоков. Для экспериментального исследования был создан скрипт, который запускал на каждом узле инструмент D-ITG указанное количество тестовых потоков с заданными требованиями к QoS.

В качестве основного критерия оценки эффективности алгоритмов маршрутизации и обеспечения QoS был выбран V – процент нарушений QoS, который может быть рассчитан по следующей формуле:

$$V = \frac{N_{QoS}}{N_{Flows}} \cdot 100\%,$$

где N_{QoS} – количество потоков данных в сети, для которых нарушены требования QoS, N_{Flows} – общее количество сгенерированных потоков. Единица измерения – %.

Для экспериментального сравнения разработанного алгоритма маршрутизации и обеспечения QoS с существующими аналогами предлагается построить график зависимости среднего значения метрики V от N_{Flows}. Для усреднения в каждой точке значения N_{Flows} эксперимент повторяется 50 раз.

В качестве наиболее эффективного принимается алгоритм, график которого лежит ниже для тех значений N_{Flows}, которые встречаются в реальных корпоративных сетях.

Методика экспериментального исследования алгоритма межсетевого экрана детально описана в ранее опубликованной работе [5].

Для исследования производительности алгоритма аутентификации пользователей и их устройств был написан скрипт, который многократно инициирует от имени пользователя аутентификацию через IEEE 802.1x и протокол EAP. Данный скрипт был развернут на виртуальных машинах, имитирующих клиентские компьютеры.

Основной метрикой оценки производительности алгоритма аутентификации является время ее выполнения T_A, которое определяется по формуле:

$$T_A = T_{Success} - T_{Request},$$

где $T_{Success}$ – момент времени получения подтверждения от DHCP-сервера после получения настроек DHCP и подтверждения успешной аутентификации, $T_{Request}$ – момент времени отправки запроса на аутентификацию. Единицы измерения – мс. Для получения статистически значимых значений данной метрики, эксперимент повторялся 50 раз для каждого узла.

Результаты экспериментальных исследований

Все экспериментальные исследования разработанного прототипа системы управления корпоративной ПКС проводились в соответствии с методикой, описанной в предыдущем разделе.

В экспериментальном исследовании алгоритмов маршрутизации и обеспечения QoS участвовали два алгоритма – разработанный генетический алгоритм (GA) и алгоритм OSPF, которые были реализованы в виде модуля маршрутизации и обеспечения QoS прототипа системы управления корпоративной ПКС.

На рисунке 2 приведен график зависимости процента нарушений QoS в зависимости от количества одновременно передаваемых тестовых потоков данных для разработанного генетического алгоритма и стандартного алгоритма маршрутизации OSPF.

На рисунке видно, что для генетического алгоритма в начале процент нарушения нулевой, затем, начиная с некоторого момента (приблизительно 300 потоков) наблюдается резкий рост процента нарушений. Это связано с эффектом насыщения сети и с небольшим масштабом

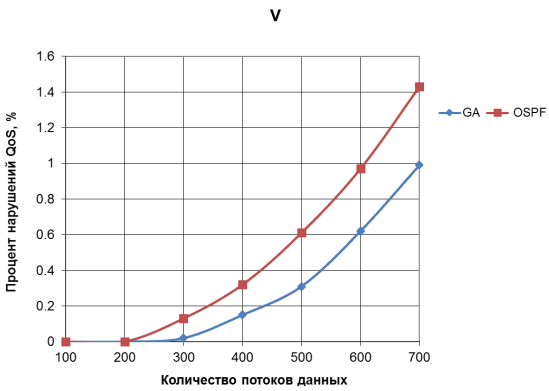

Рисунок 2. График зависимости процента нарушений QoS от количества генерируемых тестовых потоков

экспериментального сегмента. Для протокола OSPF с самого начала наблюдается рост процента нарушений.

Таким образом, можно заключить, что экспериментальное исследование подтвердило эффективность разработанного генетического алгоритма маршрутизации и обеспечения QoS.

Результаты экспериментального исследования алгоритма межсетевого экрана опубликованы в работе [5].

В результате экспериментального исследования алгоритма аутентификации прототипа системы управления корпоративной ПКС было определено следующее среднее значение времени аутентификации $T_A = 314.2$ мс, что является вполне приемлемым.

Результаты проведенных экспериментальных исследований подтвердили эффективность алгоритмических решений, реализованных в рамках прототипа системы управления корпоративной ПКС.

Выводы

Создан прототип системы управления корпоративной сетью на основе ПКС. Детально описана его архитектура в виде структуры разработанных и заимствованных модулей с открытым исходным кодом.

Разработан алгоритм аутентификации для корпоративных ПКС. Его особенностью является поддержка технологии IEEE802.1x, протоколов EAP, RADIUS, LDAP, стандарта WPA2-EAP. ПКС используется для изоляции потоков данных различных пользователей с возможностью создания произвольного количества изолированных виртуальных сетей без ограничений VLAN, а также для контроля разграничения доступа за счет функций межсетевого экранирования.

Проведенные экспериментальные исследования прототипа и анализ их результатов показали эффективность и пригодность разработанных алгоритмов для корпоративных ПКС. Полученные результаты могут быть использованы для развертывания корпоративных ПКС на предприятиях Оренбургской области.

01.12.2012

Исследования выполнены при поддержке РФФИ и Правительства Оренбургской области (проект № 14-07-97034), Президента Российской Федерации, стипендии для молодых ученых и аспирантов (СП-2179.2015.5).

Список литературы:

1. McKeown, N. OpenFlow: Enabling Innovation in Campus Networks / N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, J. Turner // ACM SIGCOMM Computer Communication Review. - New York, 2008. - т. 38, №2. - с. 69-74.
2. Intro to OpenFlow [Электронный ресурс] // Open Networking Foundation. Электрон. дан. - 2015. Режим доступа : https://www.opennetworking.org/standards/intro-to-openflow. Загл. с экрана. (Дата обращения: 15.11.2015)
3. Адрова Л.С., Полежаев П.Н. Защита корпоративных программно-конфигурируемых сетей // Труды XXI Всероссийской научно-методической конференции Телематика'2014. - С.133-134.
4. 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, 2014. - С. 301-305.
5. Shukhman A., Polezhaev P., Ushakov Yu., Legashev L., Tarasov V., Bakhareva N. Development of network security tools for enterprise software-defined networks // Proceedings of the 8th International Conference on Security of Information Networks, September 8-10, 2015 Sochi/Russia. - PP 224-228.
6. Адрова Л.С., Полежаев П.Н. Модель разграничения доступа для корпоративной программно-конфигурируемой сети // Информационные технологии. Проблемы и решения: материалы международной научно-практической конференции. Том 2 / редкол.: Ф.У. Еникеев и др. - Уфа: Изд-во «Восточная печать». - 2015. - С. 192-196.
7. Полежаев П.Н. Реализация алгоритма межсетевого экрана для облачных систем с использованием технологии программно-конфигурируемых сетей // Сборник трудов III Международной научно-практической конференции «Информационная безопасность в свете Стратегии Казахстан-2050». - 2015. - С. 266-271.

8. Полежаев П.Н., Бахарева Н.Ф., Шухман А.Е. Разработка эффективного генетического алгоритма маршрутизации и обеспечения качества обслуживания для программно-конфигурируемой сети. - Вестник Оренбургского государственного университета. - 2015. - № 1 (176). С. 213-217.

Сведение об авторах:

Бахарева Надежда Федоровна, профессор кафедры геометрии и компьютерных наук Оренбургского государственного университета, доктор технических наук
460018, г. Оренбург, пр-т Победы, 13, ауд. 1502, тел.: (3532) 372539,
e-mail: nadin1956_04@inbox.ru

Полежаев Петр Николаевич, преподаватель кафедры компьютерной безопасности и математического обеспечения информационных систем Оренбургского государственного университета
460018, г. Оренбург, пр-т Победы, 13, ауд. 20520, тел.: (3532) 372534,
e-mail: peter.polezhaev@mail.ru

Ушаков Юрий Александрович, доцент кафедры геометрии и компьютерных наук Оренбургского государственного университета, кандидат технических наук
460018, г. Оренбург, пр-т Победы, 13, ауд. 1502, тел.: (3532) 372539,
e-mail: unpk@mail.ru

Шухман Александр Евгеньевич, заведующий кафедрой геометрии и компьютерных наук Оренбургского государственного университета, кандидат педагогических наук, доцент
460018, г. Оренбург, пр-т Победы, 13, ауд. 1502, тел.: (3532) 372539,
e-mail: shukhman@gmail.com