УДК 681.518

ДИНАМИЧЕСКАЯ ОРГАНИЗАЦИЯ БЕЗОПАСНОСТИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Ц.С. Оганнисян

Национальный политехнический университет Армении

Рассматриваются вопросы безопасности телекоммуникационных сетей. Показано, что безопасность сети в значительной степени зависит от защиты хоста и баз данных, а управление доступом к сети должно быть более динамичным. Предлагается комплексная система для обеспечения надежной работы телекоммуникационных сетей – TNSCS (Telekommunication Network Security Control System), описана ее конструкция. TNSCS использует программируемые коммутаторы для управления трафиком в нижних слоях. Система предназначена для динамического определения политики управления сетью и реализована в архитектуре OpenFlow.

Ключевые слова: телекоммуникационная сеть, трафик, контроль доступа, сеть VLAN, база данных.

Введение. TNSCS предназначены для обеспечения безопасности телекоммуникационных сетей. Они используют программируемые коммутаторы [1] для управления трафиком, которые принимают меры по реализации политики безопасности высокого уровня (например, изменение направления трафика). Сложные взаимодействия между протоколами и системами могут вызвать некорректное поведение и медленный ответ на атаки. Эти неполадки позволят устранить внедрение в сеть механизма динамического контроля доступа.

В телекоммуникационных сетях существует множество разнородных и потенциально ненадежных устройств, которые могут быть уязвимы к неполадкам. Несмотря на значительные успехи в локальной безопасности, растут количества и типы сетевых устройств, начиная от настольных компьютеров до ноутбуков, становится все более сложным обеспечение безопасности каждого устройства, подключаемого к сети. Эти устройства работают под управлением различных операционных систем и могут иметь разнообразный набор уязвимостей. В свете вышесказанного, сеть должна проверить подлинность новых устройств, контролировать их подключение и

поведение для обнаружения нарушений различных политик безопасности (например, присутствие посторонних или зараженных хостов). Аутентификация и обеспечение работы для пользователей корпоративных сетей представляют собой сложную задачу, и сетевые операторы, как правило, полагаются на объединение активных, специальных методов. Указанные проблемы вызваны наличием множества независимых, трудных для управления устройств, которые взаимодействуют неожиданным образом, а также слабой системой безопасности, что приводит к неправильной работе (например, неправильная конфигурация [1]).

Проблемы управления телекоммуникационными сетями. Обычно телекоммуникационные сети большие и трудноуправляемые. Как правило, они строятся на VLAN технологиях и управляются с помощью VMPS (VLAN Management Policy Server). Такие сети обладают следующими функциями.

Регистрация. Веб-интерфейс помогает пользователям в процессе регистрации. DNS-сервер возвращает IP-адрес сервера регистрации для всех запросов DNS с целью списка доменов, необходимых для исправления (например, windowsupdate.com). В системе работают два DHCP-сервера: один - для незарегистрированных VLAN и один - для зарегистрированных VLAN. Каждый имеет свои собственные конфигурационные файлы, которые создаются автоматически на основе информации в базе данных.

Сканирование. В процессе регистрации системы проверяются на наличие известных уязвимостей. Если сканирование выявляет уязвимые места, пользователь оповещается об этом, и ему предоставляется возможность обновить систему. Брандмауэр разрешает трафик на соответствующие серверы обновлений.

*Брандмауэр***.** В регистрации VLAN используется брандмауэр для блокирования сетевого трафика незарегистрированных хостов. Брандмауэр позволяет передавать веб - трафик и безопасный веб (т.е. порт 80 и 443) так, что хосты могут достичь обновления сайтов. Различные маршрутизаторы и коммутаторы [2,3] создают необходимые сети VLAN. Локальные коммутаторы определяют VLAN для каждой машины, подсоединенной к сети. Коммутатор периодически будет скачивать VLAN карты от VMPS.

Пример архитектуры телекоммуникационной сети, построенной подобным способом, показан на рис. 1.

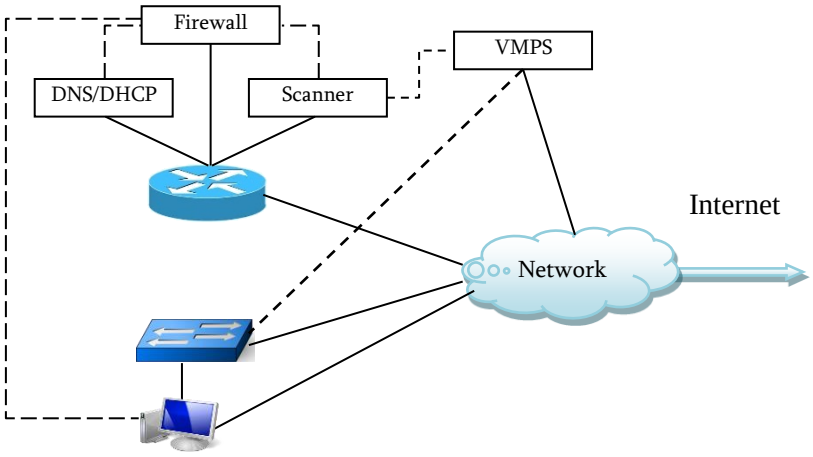

Рис. 1. Архитектура телекоммуникационной сети, построенной по технологии VLAN

Сетевые администраторы часто сталкиваются с ситуациями, когда машины заражены или находятся под угрозой. В настоящее время оператор сети вручную удаляет или помещает в карантин машину, что весьма утомительно. Сеть должна обеспечивать гибкий, быстрый контроль над сетевым трафиком, а также быть масштабируемой для большого числа пользователей и транспортных потоков. По мере возможности, управление сетью должно быть автоматизировано, чтобы облегчить нагрузку сетевых администраторов.

Телекоммуникационные сети с приведенной архитектурой имеют следующие недостатки:

1. Контроль доступа слишком сложный**.** В телекоммуникационных сетях, построенных по технологии VLAN (ТСТВ), имеются две различные сети VLAN для того, чтобы отличить зараженные или взломанные машины от целых машин. В результате такого разделения все зараженные хосты располагаются в одной VLAN. Такая конфигурация не обеспечивает правильную изоляцию, так как эти инфицированные узлы не изолированы друг от друга.

2. Узлы различных частей сети не могут быть динамическими. Когда машина отображается в другой части сети, она должена быть перезагружена, чтобы убедиться, что машина получает внешний IP-адрес, однако это неудобно, так как это происходит путем вмешательства пользователя.

3. Контроль не является непрерывным**.** Аутентификация и сканирование происходят только тогда, когда сетевое устройство впервые введено; если устройство впоследствии находится под угрозой (или иным образом становится источником нежелательного трафика), то оно не может быть динамически переназначено.

Многие из недостатков являются следствием того, что функции

безопасности были добавлены в верхнюю часть существующей инфраструктуры сети. Однако производители коммутаторов начали предлагать стандартный интерфейс - Open-Flow [4], в результате чего внешний контроллер может влиять на коммутатор направленного трафика.

Коммутатор с поддержкой OpenFlow предлагает открытый протокол для программирования таблицы расхода и принимает меры, основанные на записях в этих таблицах. Базовая архитектура состоит из коммутатора, центрального контроллера и пользователя в конце. Коммутатор и контроллер взаимодействуют по защищенному каналу с использованием протокола управления OpenFlow [3,4], который может влиять на записи в таблице коммутатора. В настоящее время все коммутаторы OpenFlow поддерживают три действия: 1) направление пакетов потока в определенный порт или порты. Эта функция гарантирует отправку пакетов; 2) инкапсуляция и пересылка пакетов потока на контроллере. В этом случае пакет доставляется к защищенному каналу, где он инкапсулируется и передается на контроллер; 3) отбрасывание пакетов потока.

Для решения подобных задач предлагается использовать TNSCS. Управление TNSCS трафика происходит с помощью политик, которые устанавливаются в программируемые коммутаторы. Создается динамическая система контроля доступа путем интегрирования контроллера с подсистемами мониторинга. Такая интеграция позволяет оператору определить, как сеть должна контролировать трафик и как происходит изменение состояния сети. Например, TNSCS может автоматически помещать в карантин пользователей или подмножества трафика, когда обнаружены угроза или другое нарушение правил безопасности.

Последние тенденции включают интеграции динамического наблюдения и контроля. Во-первых, программируемые сетевые устройства [5] позволяют более прямой, точный контроль над сетевым трафиком. На первый взгляд, эти устройства представляют еще один источник сложности, но это программирование на самом деле представляет собой возможность для активной защиты на сетевом уровне. Во-вторых, алгоритмы мониторинга распределенной сети могут теперь быстро и точно соотносить движение различных источников для выявления скоординированных атак. Наконец, тенденция логического централизованного управления сетью [2,6] позволяет легко интегрировать распределенный мониторинг сети с динамическим управлением.

Рассмотрим задачу угрозы зараженного хоста, которая включает определение политики безопасности, мониторинг сетевого трафика с целью выявления возможных нарушений, а также принятие соответствующих мер для исправления нарушения. Для решения этой задачи от сетевого администратора требуется: 1) установить на пути брандмауэры, которые выполняют контроль

движения трафика, и 2) обновить правила брандмауэра, когда обнаружен зараженный хост. TNSCS предоставляет интерфейс для распределенных алгоритмов вывода с целью непосредственного контроля поведения сетевого трафика. Распределенная система с помощью существующих подсистем может отслеживать трафик на более высоких уровнях и выявлять зараженные хосты [6,7]. TNSCS может интегрировать эти сигналы с действиями, которые коммутаторы непосредственно реализуют (например, перенаправление, ограничение скорости или удаление трафика).

Несмотря на перспективы дизайна TNSCS и последние тенденции, есть много проблем для развертывания системы. Во-первых, необходимо масштабировать TNSCS до большого числа пользователей и транспортных потоков. Во-вторых, TNSCS должна реагировать на различные изменения в политике сети. Она должна быстро аутентифицировать законные сетевые узлы и устройства и быстро находить проблемные хосты, которые нарушают политику безопасности. В-третьих, контроллеры и программируемые коммутаторы должны быть интегрированы с мониторингом в режиме реального времени и оповещения. Контроллер должен быть в состоянии быстро соотнести и синтезировать предупреждения, быстро отправлять управляющие сообщения и влиять на потоки трафика. Наконец, канал управления должен быть защищенным.

Контроллер реализует политику контроля доступа, устанавливая соответствующие записи таблицы потока в самих коммутаторах. TNSCS использует MAC-адрес, соответствующий интерфейсу пользователя. Все технические характеристики должны быть в начальном состоянии. Впоследствии контроллер устанавливает поток записи таблицы в коммутаторах на основе класса безопасности и состояния каждого MAC-адреса. Затем контроллер получает информацию об обновлении состояния и безопасности класса каждого хоста. Когда пользователь переходит в другое состояние, контроллер изменяет политику на коммутаторах в соответствии с языком спецификации. Контроллер, по существу, "собирает" информацию о динамической спецификации управления доступом в конфигурации коммутатора. Предлагается использовать контроллер для непосредственной настройки коммутатора с помощью OpenFlow и другие методы (например, изменение конфигурации).

Интеграция TNSCS с телекоммуникационными сетями. Для упрощения первоначального проекта считается, что все узлы находятся в том же классе безопасности и их состояния меняются только в результате проверки подлинности.

На рис. 2 показана работа сети, реализованной в TNSCS. Устройство транслирует DHCP - "обнаружение" сообщения. DHCP-сервер посылает обратно

внешний IP-адрес для машины. Чтобы получить доступ к глобальной сети Интернет, машина должна идентифицировать себя с помощью веб-службы. Коммутаторы с поддержкой OpenFlow [4,5] могут перенаправлять все HTTP-запросы от непрошедших машин к началу веб-сайта по умолчанию.

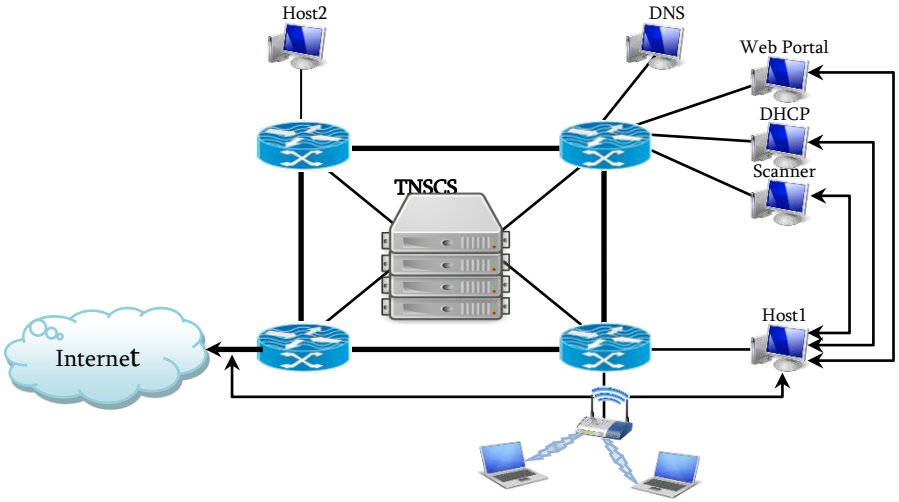

Рис. 2. Применение TNSCS в ТСТВ

После того как пользователь идентифицирует машину, веб-служба сохраняет MAC-адрес записи потока и обновляет его, чтобы обеспечить доступ к ограниченному набору направлений (например, Microsoft Update). В этот момент сканер анализирует устройство. Если машина проходит проверку, ТСТВ веб-сервис посылает запрос на контроллер, чтобы разрешить трафик от той машины, которая будет направлена в любую точку. Сеть выполняет непрерывное сканирование хостов, используя, в случае их необходимости, распределенные методы логического вывода карантина.

Контроллер отслеживает состояние каждого узла и обновляет текущее состояние в соответствии с входами от внешних источников (например, сетевые мониторы). Если клиент аутентифицируется, отправляется сообщение на контроллер, чтобы переместить узел в аутентичное состояние ("успешная аутентификация").

Затем в коммутаторах запускается сканирование хоста (рис. 3). Если клиент проходит проверку, сканер информирует контроллер для перемещения клиента в рабочее состояние ("чистый после обновления").

В противном случае, клиент перемещается в состояние "карантин". В обоих случаях контроллер соответственно обновляет таблицы потока.

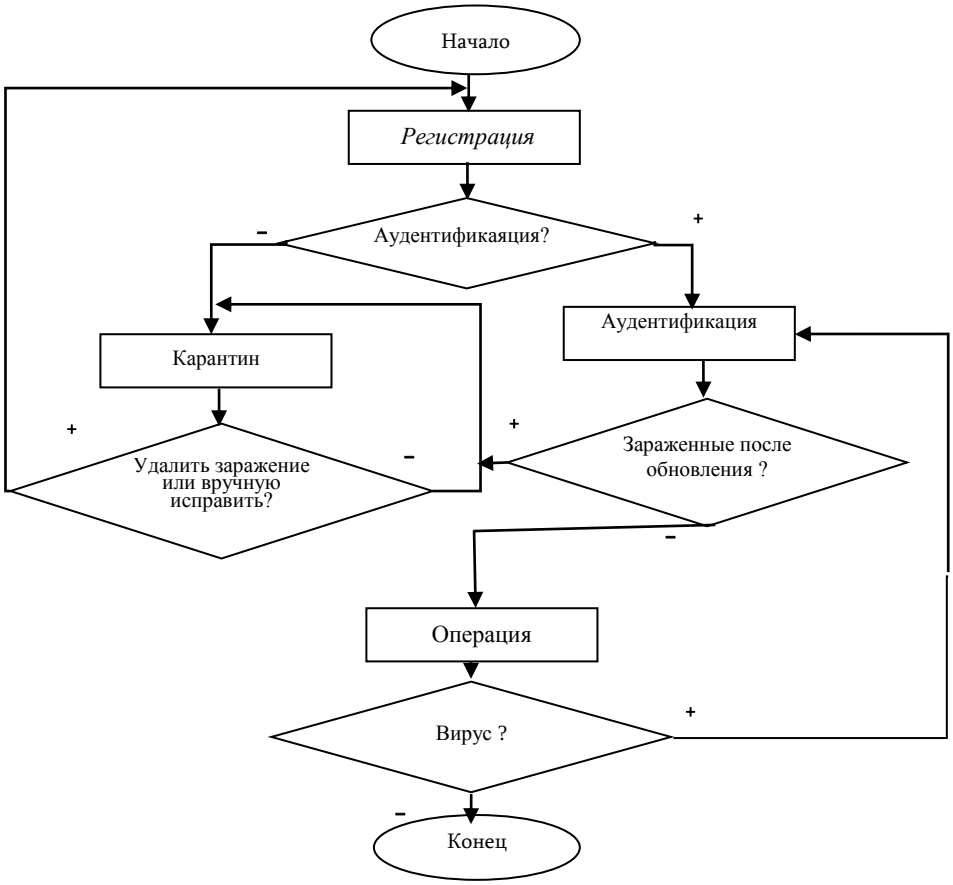

Рис. 3. Переходы состояния для хоста

Выводы. Таким образом, управление доступом к сети должно быть более динамичным и располагать как можно большей информацией о поведении хоста. Существующие телекоммуникационные сети требуют более высокого уровня сетевого мониторинга и контроля доступа (например, DHCP, на уровне приложений обнаружения вторжений и т.д.). Для устранения этих неполадок предлагается комплекс TNSCS для применения политик безопасности. Система TNSCS предназначена для динамического определения политики управления сетью и реализована в архитектуре OpenFlow.

Литература

1. **Тюрин М.В.** Экспертная оценка живучести телекоммуникационных систем и компьютерных сетей (ТСКС) в условиях неполноты информации // Автоматизация в промышленности. - 2008. - № 7. - С.15-18.

2. **Трошин С.В.** Мониторинг работы корпоративных пользователей // Вопросы современной науки и практики / Университет им. В.И. Вернадского. - 2009. - № 2 (16). - С. 59-72.
3. **Олифер В.Г., Олифер В.Г.** Компьютерные сети. Принципы, технологии, протоколы. - 3-е изд. - СПб.: Питер, 2009.- 535 с.
4. http://archive.openflow.org/
5. www.cisco.com/web
6. A clean slate 4D approach to network control and management. ACM Computer Communications Review/ **A. Greenberg, G. Hjalmtysson, D.A. Maltz.** – 2005. - 35(5). – P. 41–54.
7. **Tanenbaum A.S.** Operating systems.- 2006.- 940 p.
8. http://archive.openflow.org/

Поступила в редакцию 11.02.2015.
Принята к опубликованию 22.05.2015.

ՀԵՌԱՀԱՂՈՐԴԱԿՑԱԿԱՆ ՑԱՆՑԵՐՈՒՄ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԴԻՆԱՄԻԿ ԿԱԶՄԱԿԵՐՊՈՒՄԸ

Ծ.Ս. Հովհաննիսյան

Հեռահաղորդակցության ցանցերի անվտանգությունը մեծ հաշվով կախված է հոսթերի և տվյալների բազայի անվտանգությունից: Հեռահաղորդակցության ցանցերի անվտանգության համար առաջարկվում է ՀՑԱՂՀ՝ հեռահաղորդակցության ցանցերի անվտանգության ղեկավարման համակարգ, որն ապահովում է հեռահաղորդակցության ցանցերի հուսալի շահագործումը: ՀՑԱՂՀ-ն օգտագործում է ծրագրավորվող կոմուտատորներ, որոնք նախատեսված են՝ վերահսկելու տրաֆիկը ցանցի ստորին շերտերում: Նկարագրված է ՀՑԱՂՀ-ի կառուցվածքը, ցույց է տրված, թե ինչպես կարող է այն հաղթահարել առկա խնդիրները և ապահովել անվտանգության նոր ֆունկցիաներ:

Առանցքային բառեր. հեռահաղորդակցության ցանց, երթուղավորում, մուտքի վերահսկում, վիրտուալ տարածքային տեղական ցանց, տվյալների բազա:

DYNAMIC ORGANIZATION OF SECURITY IN TELECOMMUNICATION NETWORKS

Ts.S. Hovhannisyan

Issues on telecommunication network safety are considered. It is shown that the network safety significanly depends on the protection of the host and the database, while the network access control should be more dynamic. A complex system for ensuring the reliable operation of telecommunication networks TNSCS (Telecommunication Network Security Control System) is proposed and its structure is described. The TNSCS uses a programmable switch for controlling the traffic in lower layers. The system is intended for the dynamic determination of the network control policy, and is realized in the Open Flow architecture.

Keywords: telecommunication network, traffic, access control, VLAN, database.