ВИРТУАЛИЗАЦИЯ СЕТИ

Д. А. Ярушин
Пермский государственный национальный исследовательский университет,
614990, Пермь, Букирева, 15

В 2012 году появилась технология виртуализации сети (Network Virtualization, NV), обеспечивающая возможность виртуализации на принципиально новом уровне – уровне сетевого сегмента. В случае серверной виртуализации с небольшими оговорками операционная система (ОС) внутри виртуальных машин (ВМ) работает так, как если бы была установлена на физический сервер и являлась единственной ОС на этом оборудовании. Подобная абстракция позволяет запускать несколько изолированных экземпляров виртуальных серверов на одном физическом. По аналогии виртуализация сети приводит к тому, что виртуальная, а точнее в данном контексте виртуализованная сеть, функционирует так, как если бы она являлась физической сетью. Данный уровень виртуализации позволяет создавать и использовать несколько виртуальных сетей, возможно с перекрывающимися или даже полностью совпадающими пространствами IP-адресов, на одной физической сетевой инфраструктуре. Эта сетевая инфраструктура, может включать в себя произвольное количество физических серверов и сетевого оборудования.

Штатные средства платформы VMware vSphere, использующейся в университетском центре «Интернет», не предоставляют преимуществ масштабируемости, гибкости настройки сети и не реализуют функции, необходимые для безопасной работы сети. Вследствие чего необходимо использовать дополнительные сторонние средства для создания новой системы работы сети.

Целью данной работы была разработка системы виртуализации сети на платформе VMware vSphere с помощью технологий оверлейные сети (Overlay Network, OVN) и программно-конфигурируемые сети (Software-Defined Networking, SDN). Для достижения цели было предложено решение следующих задач:

1) изолировать виртуальные машины;
2) настроить политики зон безопасности (security zones);
3) настроить шлюз канального уровня (L2 gateway);
4) настроить шлюз сетевого уровня (L3 gateway);
5) реализовать автоматическое развертывание перечисленных функций.

Работа выполнялась в университетском центре «Интернет» Пермского ГНИУ. На платформе VMware vSphere использовались: VMware vCenter Server – платформа для централизованного управления средами VMware vSphere, которая обеспечивает автоматизацию и надежное предоставление

виртуальной инфраструктуры; гипервизор VMware ESXi (устанавливается непосредственно на физический сервер и разделяет его на несколько виртуальных машин); SDN – развивающаяся архитектура, в которой уровень управления сетью отделён от устройств передачи данных и реализуется программно; одна из форм виртуализации вычислительных ресурсов. Оверлейная сеть – общий случай логической сети, создаваемой поверх другой сети.

На сегодня решения по виртуализации сети предоставляют крупные корпорации, а именно: VMware NSX – это платформа виртуализации сети для программного ЦОД; Amazon Elastic Compute Cloud (Amazon EC2) – это веб-сервис, предоставляющий масштабируемые вычислительные ресурсы в облаке; Cisco Application Centric Infrastructure (ACI) – инфраструктура, ориентированная на приложения.

Однако на использование этих сервисов требуются значительные финансовые средства, поэтому было принято решение создать собственную систему виртуализации сети. Для демонстрации и тестирования свойств системы была выбрана данная топология сети (рис. 1).

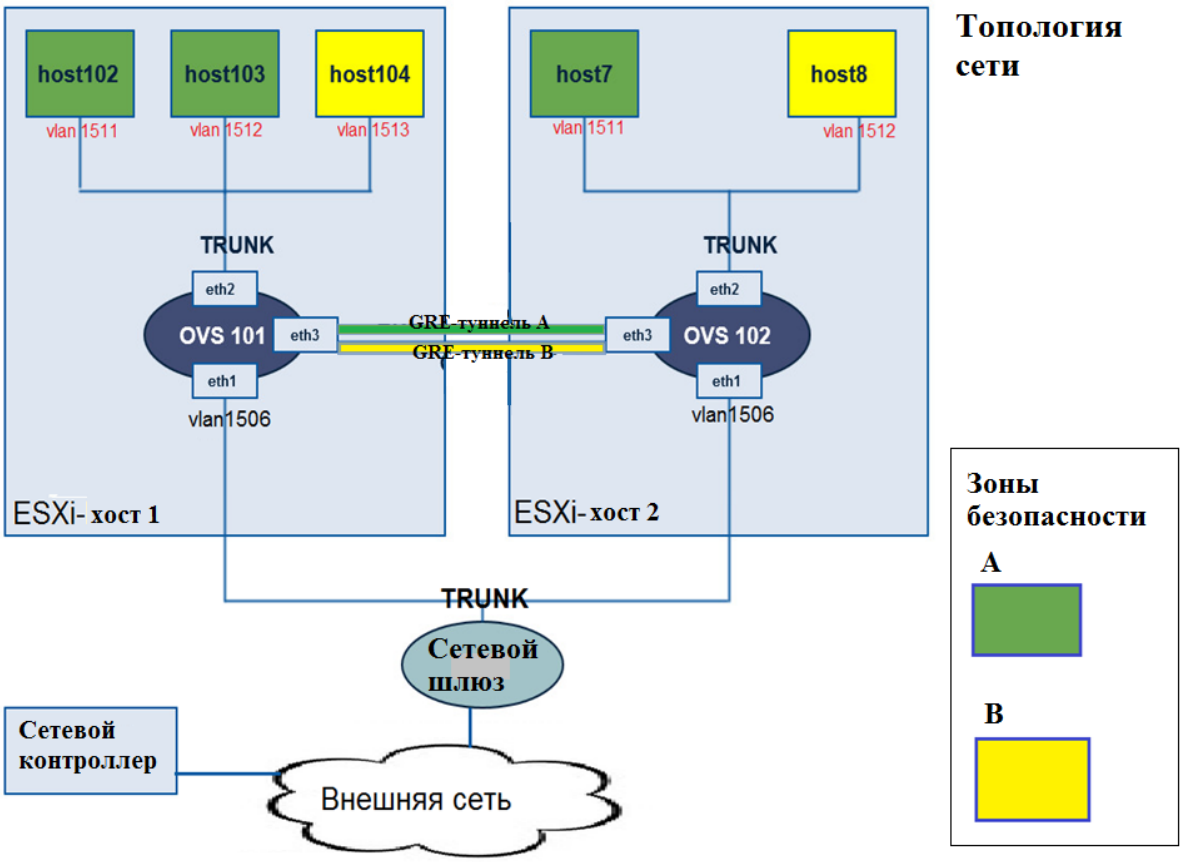

Рис. 1. *Топология сети*

Для решения задачи изоляции каждой ВМ был назначен уникальный в пределах ESXi-хоста VLAN. Для решения остальных задач потребовалось использование технологии SDN и протокола OpenFlow. OpenFlow – протокол управления процессом обработки данных, передающихся по сети маршрутизаторами и коммутаторами, реализующий технологию SDN. Протокол используется для управления сетевыми коммутаторами и маршрутизаторами с центрального устройства – контроллера сети. В качестве элемента управления работой сети была использована виртуальная машина с установленным на ней OpenFlow-контроллером floodlight. Для передачи данных между ВМ в каждом ESXi-хосте был установлен Open vSwitch (реализация OpenFlow switch). Изоляция ВМ между ESXi-хостами была реализована за счет создания GRE-туннелей.

Правила работы OpenFlow switch описаны в таблицах потоков, которые содержатся в его памяти. Таблица потоков состоит из записей, в каждой из которых содержатся поля сравнения, счетчики и инструкции. Когда пакет поступает в OpenFlow switch поля сравнений записей таблицы потоков сравниваются с заголовком пакета в порядке приоритета (одно из полей сравнения). Если найдена совпадающая запись, то к пакету применяются инструкции, ассоциированные с данной записью, и увеличивается значение счетчика.

Таким образом, задача сводится к передаче таблиц потоков в соответствующий Open vSwitch. Чтобы определить, какое содержание таблиц должно быть на каждом Open vSwitch-е, необходимо собрать информацию о системе, т.е. считать информацию о каждой ВМ (ее MAC-адрес, Vlan, на каком ESXi-хосте и в какой зоне безопасности она находится). Для этого был разработан модуль сбора информации с vCenter с использованием средств удаленной командной строки vSphere Command-Line Interface (программа на C++). Модуль также находится в OpenFlow-контроллере. Для передачи записей таблиц потоков был создан модуль для floodlight-контроллера (программа на Java), использующий данные на выходе модуля сбора информации. Информация о шлюзе канального и сетевого уровня также заложена в записи таблиц потоков, передающихся на Open vSwitch-и.

Тестирование работы системы показало, что виртуализованная сеть успешно работает, выполняя описанные функции. В ходе работы были реализованы: способ изоляции виртуальных машин; связь зон безопасности между ESXi-хостами(GRE-туннели); модуль сбора информации с vCenter; разработан модуль логики работы сети и обработки политики безопасности – создание статических потоков; реализованы сервисы – L2 gateway, L3 gateway, изоляция между зонами безопасности.

В качестве рекомендаций было предложено привести систему в соответствии требованиям к МЭ для 3 класса защищенности для ее сертификации в дальнейшем.

Список литературы

1. *Mc Keown, Anderson T., Balakrishnan H., Parulkar G., Peterson L., Rexford J., Shenker S., Turner J.* OpenFlow: Enabling innovation in campus networks // ACM IGCOMM Computer Communications Review, April 2008
2. http://www.vmware.com/ru
3. https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.3.2.pdf