Особенности построения программно-конфигурируемых сетей SDN (Software-Defined Networking)

Современные тенденции развития информационых технологий на глазах меняют корпоративные сети. Идет наращивание объемов сетевого трафика, поэтому все чаще возникает необходимость конфигурирования все более сложных сетевых структур.

Упростить эту задачу могут технологии программно-конфигурируемых сетей SDN (Software-Defined Networking) и функциональной виртуализации сетей NFV (Network Function Virtualization), которые позволяют перевести сетевые элементы под контроль настраиваемого программного обеспечения, сделать их более интеллектуальными и гибкими, облегчить управление ими.

Ключевые принципы программно-конфигурируемых сетей — разделение процессов передачи и управления данными, централизация управления сетью при помощи унифицированных программных средств. Протокол OpenFlow, реализующий независимый от производителя интерфейс между логическим контроллером сети и сетевым инфраструктурой, является одной из реализаций концепции программно-конфигурируемой сети и считается движущей силой её распространения и популяризации (Рисунок 1).

В результате получается гибкая, управляемая, адаптивная и экономичная архитектура, которая способна эффективно адаптироваться под передачу больших потоков разнородного трафика.

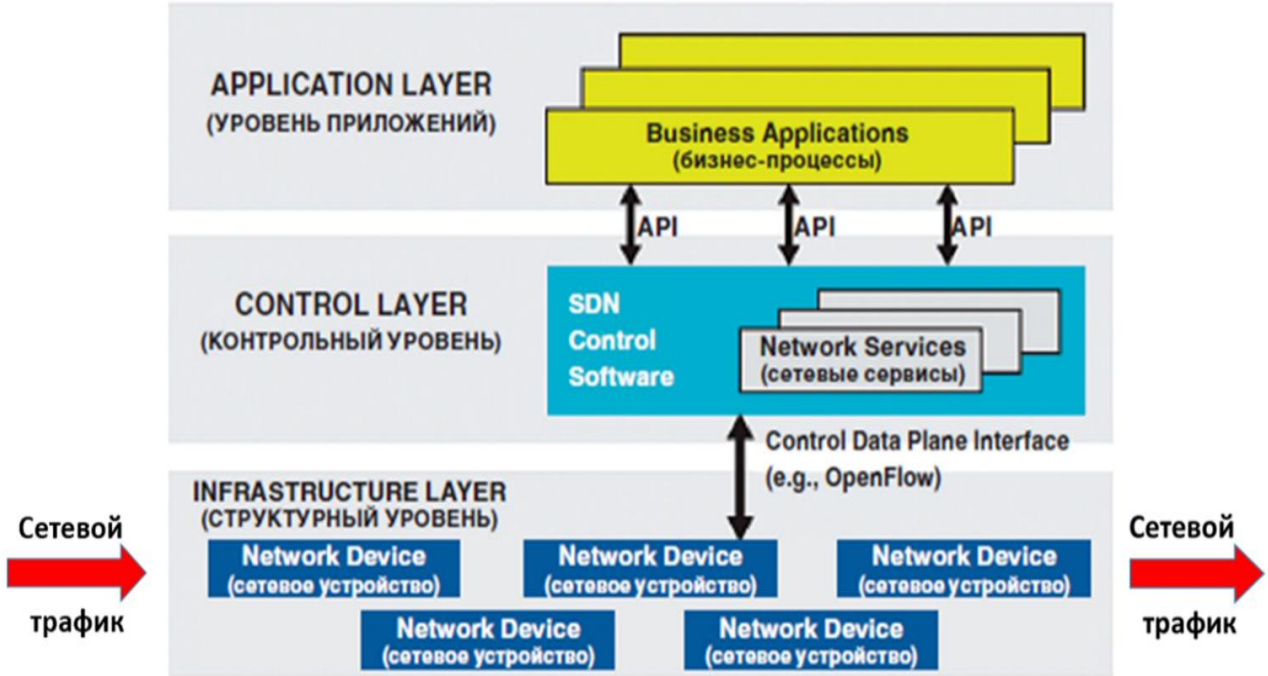

Рисунок 1. Архитектура SDN

Основные идеи SDN включают:

1. Разделение процесса прохождения трафика (структурный уровень) и управление трафиком (контрольный уровень);

2. Контрольный уровень предоставляет собой контроллер, который является централизованной платформой управления для сети, определенной программным обеспечением.

3. Существенное упрощение сетевых элементов уровня инфраструктуры, которые не принимают решение о перенаправлении трафика;

4. Единый, унифицированный, независящий от поставщика интерфейс между контрольним уровнем и уровнем инфраструктуры (протокол OpenFlow);

5. Логически централизованное управление сетью, существляемое с помощью контроллера с установленной сетевой операционной системой и реализованными поверх сетевыми приложениями (уровень приложений);

Таким образом, SDN формирует виртуальный уровень для сети, аналогично тому, как гипервизор или виртуальная машина делает это для серверов или настольных компьютеров. Благодаря этому свойству SDN сетей, революционным образом меняется вся ситуация в сфере ИТ.

Если рассматривать так называемую «ИТ-троицу», состоящую из серверов, систем хранения и сетей, то виртуализация сетей существенно отстает от виртуализации серверов и систем хранения, которые являются доступными уже на протяжении многих лет. Теперь организация сети может, наконец, сравняться с точки зрения виртуализации с двумя другими элементами троицы.

Результат получается значительным. SDN дает возможность предоставлять сетевые ресурсы так же быстро, как и вычислительные платформы и платформы хранения, обеспечивая при этом интеграцию приложений. Наконец, вся ИТ-инфраструктура может начать работать как единое целое и обеспечивать ресурсами всю организацию через Центр обработки данных.

Вместе с тем, существует один из основных сдерживающих факторов для развития SDN – это отсутствие единого стандарта и стремление ряда вендоров навязать рынку «своё» решение, хотя такой подход абсолютно противоречит основным принципам SDN. В результате в SDN еще много неопределенности, и некоторые потенциальные потребители программно-конфигурируемых решений заняли выжидательную позицию, следя за появлением успешных крупных проектов в этой области. Хотя такие проекты появлялись и продолжают появляться.

Появился такой проект и в Учебно-научном центре технологий Hewlett Packard Enterprise (HPE) Государственного университета телекоммуникаций. Реально действующая сеть SDN необходима для проведения научных исследований и, конечно же, для подготовки студентов по этой перспективной технологий. В отличие от других организаций, Учебно-научный центр избавлен от неопределенности, поскольку рассматривает разработки в этой области только компании Hewlett Packard Enterprise (HPE).

Компания Hewlett Packard Enterprise (HPE) стремится к лидерству при содействии в разработке стандартов SDN (Software-Defined Networking), NFV (Network Function Virtualization), OpenFlow и является лидером в организациях и проектах, которые занимаются этими разработками, поэтому есть на что опереться при развертывании сети SDN (Рисунок 2):

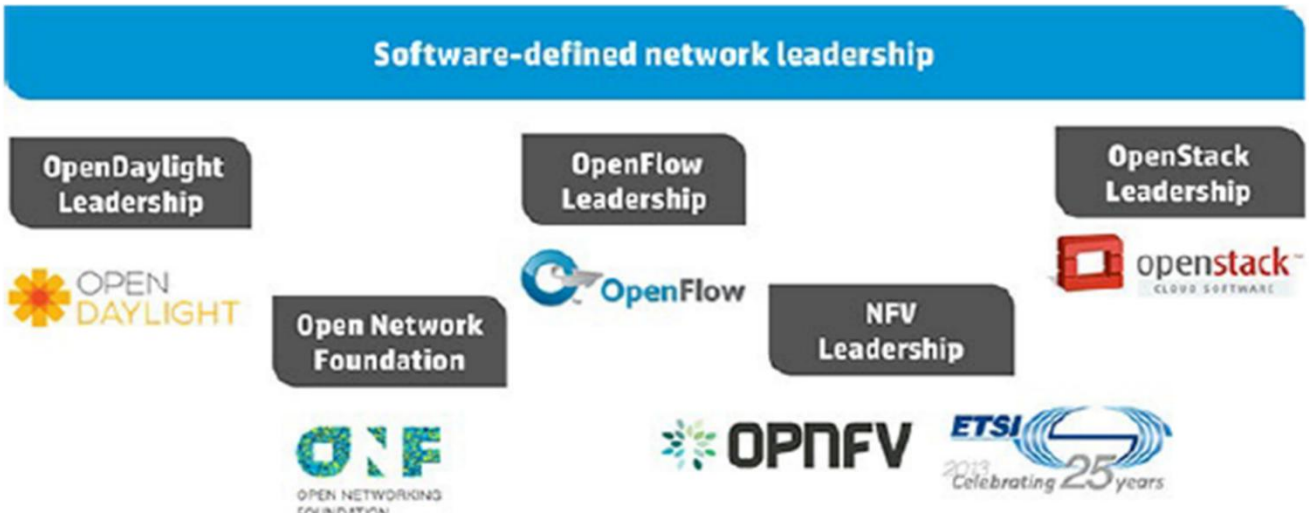

Рисунок 2. Лидерство компании HPE в разработке SDN

Компания Hewlett Packard Enterprise (HPE) является:

1. Членом-основателем организации Open Networking Foundation (ONF), которая фокусируется на развитии концепции SDN и стандартизации протокола OpenFlow;
2. Платиновым членом, высший уровень, проекта OpenDaylight, для создания модульного SDN-контроллера;
3. Платиновым членом, высший уровень, проекта по разработка облачной платформы OpenStack;
4. Разработчиком более 50 сетевых устройств (коммутаторы, маршрутизаторы, точки доступа) с поддержкой протокола OpenFlow.

Главным элементом сети SDN от компании Hewlett Packard Enterprise (HPE) является контроллер HPE VAN SDN. Контроллер свободно, бесплатно и легко скачивается из электронных ресурсов компании. Работает контроллер под управлением операционной системы Linux Ubuntu.

Для установки операционной системы и Контроллера для сети среднего уровня, состоящей из 100-500 сетевых устройств, необходим сервер с параметрами:

8 ядерный процессор;

16 Гбайт оперативной памяти;

150 Гбайт дискового пространства.

Проверка работоспособности установленного контроллера HPE VAN SDN осуществляется с помощью встроенного сетевого эмулятора Mininet. Эмулятор может создавать и эмулировать всю локальную сеть OpenFlow. Mininet позволяет создавать различные топологии, состоящие из коммутаторов и хостов OpenFlow (конечных устройств). Топологии могут варьироваться от одного коммутатора до более сложных топологий, состоящих из нескольких коммутаторов и хостов. Виртуализированные коммутаторы и хосты действуют как реальные устройства. Можно отправлять трафик между хостами, а затем просматривать потоки на коммутаторах. Кроме того, с помощью разных приложений, можно осуществлять измерения производительности в сети (Рисунок 3).

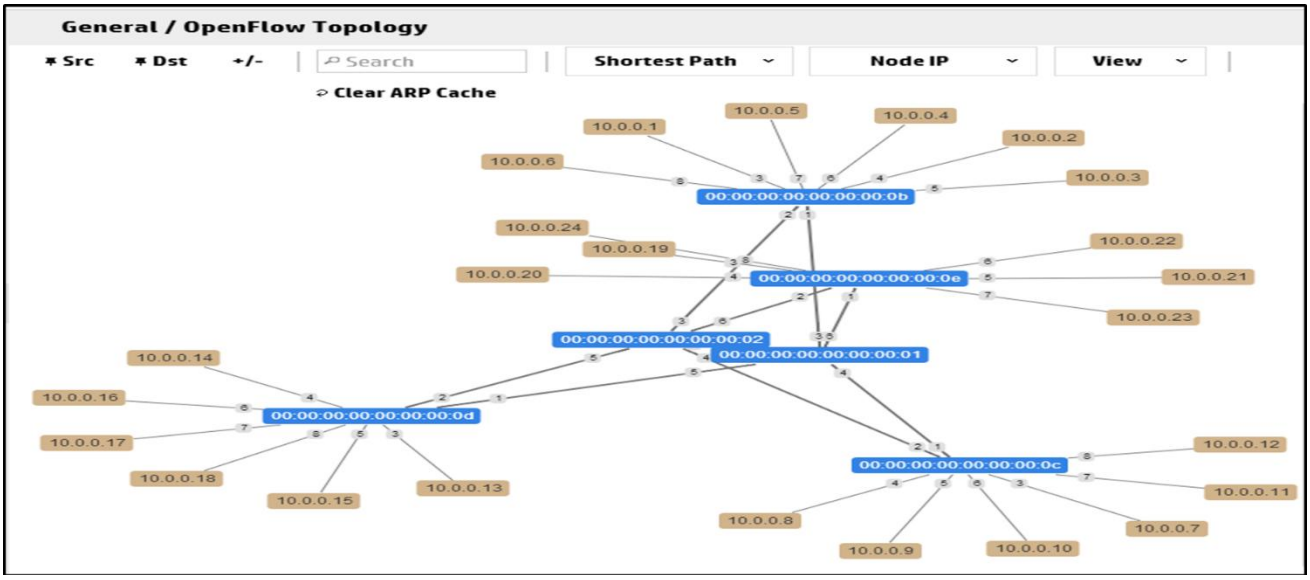

Рисунок 3. Топология сети сетевого эмулятора Mininet.

На заключительном этапе необходимо подключить физическую сеть к виртуальной сети, созданной с помощью эмулятора Mininet. При настройке физических коммутаторов и виртуальных коммутаторов, необходимо использовать одну и ту же систему команд, как будто работа производится в единой однородной сети.

Для построения физической сети необходимо использовать коммутаторы с поддержкой протокола OpenFlow. Таких коммутаторов, разработки компании Hewlett Packard Enterprise (HPE), существует большое количество, поэтому для каждого конкретного случая это не представляется большой проблемой (Рисунок 4).

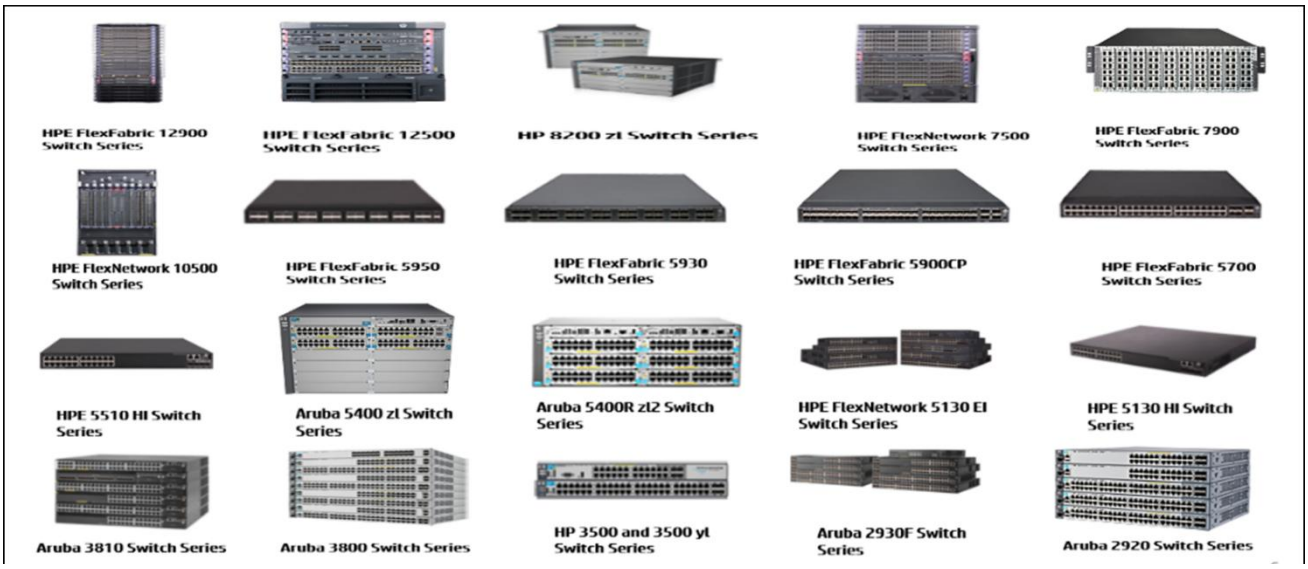

Рисунок 4. Коммутаторы HPE с поддержкой протокола OpenFlow

Таким образом, подготовка к работе и настройка сети SDN Hewlett Packard Enterprise (HPE), не требует чрезвычайных ресурсов, не вызывает особых затруднений и поэтому может быть развернута даже в небольших

организациях. Однако все же ограничения и некоторые проблемы существуют и они связаны со следующим.

Особенностью работы контроллера HPE VAN SDN является то, что он обеспечивает свою полную функциональность при обязательном взаимодействии с тремя основными приложениями:

HP Network Protector SDN Application: обеспечивает защиту от угроз в реальном масштабе времени;

HP Network Optimizer SDN Application: обеспечивает необходимое управляемое качество обслуживания (QoS);

HP Network Visualizer SDN Application: обеспечивает видимость и прозрачность сети, а также проактивный мониторинг сети с целью выявления проблем.

Приложение **HP Network Protector SDN** использует такие технологии как TippingPoint и ArcSight для выработки конвергентного решения, которое устраняет угрозы безопасности совершенно новым способом, используя самую сеть. (Рисунок 4).

HP Network Protector SDN позволяет осуществлять сетевую разведку на сетевых инфраструктурных устройствах. Приложение использует сетевой контроллер HP VAN SDN и OpenFlow для программирования сетевой инфраструктуры с помощью средств безопасности TippingPoint Reputation |rɛpjʊˈteɪʃ(ə)n| Digital Vaccine (RepDV). Это превращает всю инфраструктуру сети в устройство обеспечения безопасности, гарантируя видимость угроз и защиту от угроз более чем одного миллиона вредоносных бот-сетей (ботнетов), вредоносных программ и сайтов-шпионов.

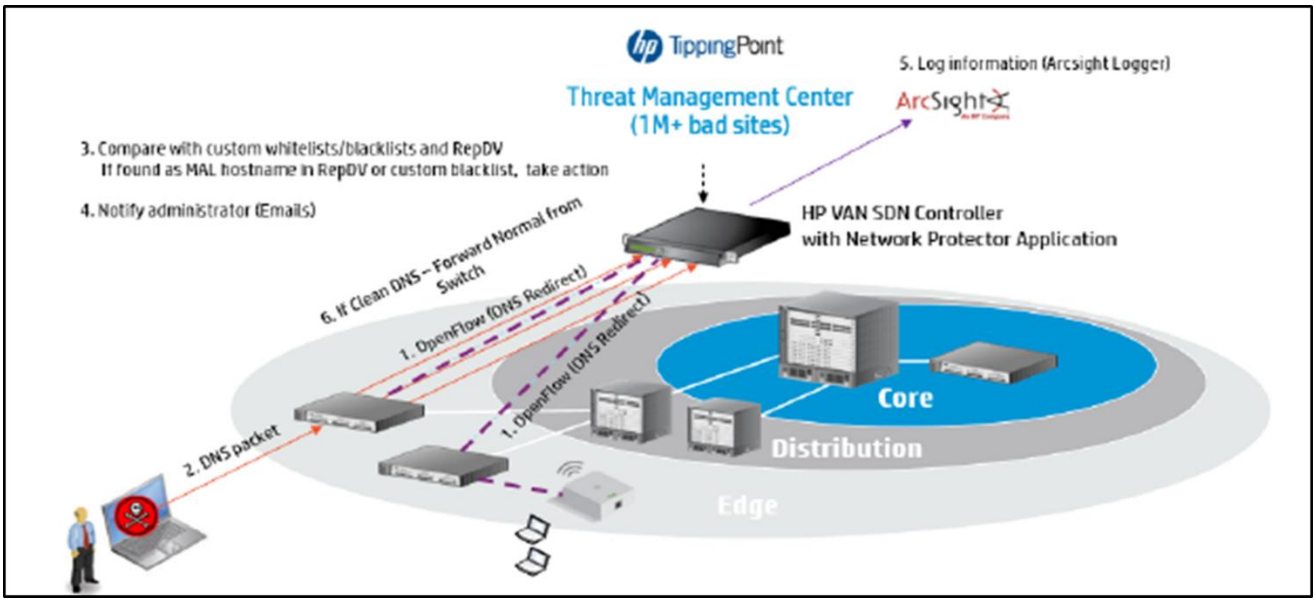

Рисунок 4. Схема организации работы приложения HP Network Protector SDN

TippingPoint Reputation |rɛpjʊˈteɪʃ(ə)n| Digital Vaccine (RepDV) является специальным сервисом, который позволяет организациям отслеживать и блокировать входящие и исходящие сообщения от известных вредоносных и нежелательных узлов. База данных TippingPoint Reputation |rɛpjʊˈteɪʃ(ə)n| Database (RepDV) включает более миллиона известных вредоносных или

нежелательных хостов, собранных из глобальной разведывательной сети HP TippingPoint ThreatLinQ и репозитория вредоносных программ. Каждому элементу присваивается оценка угрозы от 1 до 100, основанная на анализе активности, источника, категории и угрозы. Клиенты могут настраивать политику на основе оценки репутации, категории или геолокации для удовлетворения пользовательских требований безопасности. TippingPoint Reputation |rɛpjʊˈteɪʃ(ə)n| Database (RepDV) обновляется несколько раз в день, чтобы опережать возникающие угрозы и снизить риск безопасности клиентов.

Когда коммутатор получает DNS-трафик, он пересылается контроллеру. На контроллере запрос сравнивается с TippingPoint Reputation |rɛpjʊˈteɪʃ(ə)n| Database (RepDV). Если есть совпадение, то это означает, что трафик есть вредоносным по своей природе. HP Network Protector SDN создает ответ DNS и отправляет его на коммутатор для пересылки клиенту. Это обеспечивает немедленный отказ запрашивающего клиента и **вредоносный трафик будет заблокирован.**

Однако для того, чтобы решить такую задачу, появляются новые требования к аппаратной части SDN сети, то есть требования к характеристике коммутаторов OpenFlow. Требования достаточно жесткие, что существенным образом меняет ситуацию со свободой выбора конкретного коммутатора.

HP Network Protector SDN использует OpenFlow для перенаправления DNS-трафика от коммутатора к приложению и сравнивает его с TippingPoint Reputation |rɛpjʊˈteɪʃ(ə)n| Database (RepDV) для принятия решений о пересылке или блокировании (Рисунок 5).

Тем не менее, пакеты новых потоков необходимо скопировать с помощью процессора коммутатора для обработки, а затем перенаправить их на контроллер, ограничивая производительность коммутатора. Чтобы максимизировать производительность коммутатора, аппаратное обеспечение коммутатора должно давать возможность прямого подключения трафика к контроллеру. Другими словами, пакеты пересылаются аппаратным обеспечением коммутатора не с помощью процессора, а через специальный туннель Service Insertion.

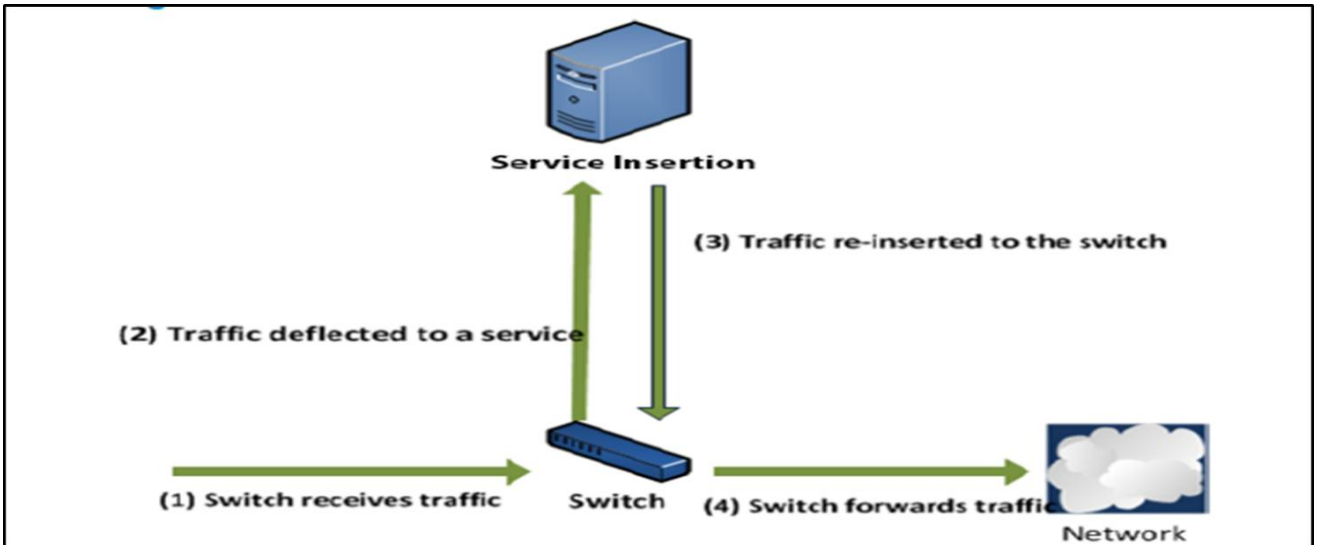

Рисунок 5. Принцип работы туннеля Service Insertion

Желаемая максимальная производительность достигается с помощью коммутаторов, поддерживающих технологию OpenFlow и туннеля Service Insertion.

Комутаторы ProVisin версии KA 15.15 и выше поддерживает эту функцию, называемую Service Insertion, которая помогает отправлять трафик DNS-данных с использованием коммутационного оборудования, минуя процессор коммутатора, тем самым повышая производительность. Обработка пакетов с использованием процессора коммутатора происходит медленнее, чем обработка пакетов с использованием коммутационного оборудования через туннель Service Insertion.

Фактически единственным коммутатором, который в полной мере поддерживает эту функцию, является коммутатор Aruba 3800 Switch Series. Для разворачиваемой сети потребовалось приобретение и использование этого коммутатора, что дало хорошие результаты.

Таким образом, подготовка к работе и настройка полномасштабной сети SDN Hewlett Packard Enterprise (HPE) для небольших организациях является практически выполнимой задачей, несмотря даже на некоторые аппаратные ограничения.