

Особенности построения корпоративных сетей на базе SD-WAN-решений



Дмитрий ПЛЕШАКОВ,
заместитель технического директора,
компания ИЦ «ТЕЛЕКОМ-СЕРВИС»

SD-WAN: предпосылки появления и предшествующие технологии

Когда-то (к слову, не так уж давно) большинство корпоративных сетей естественным путем ограничивалось рамками ИТ-инфраструктуры офисов, где размещались штаб-квартиры компаний. Впоследствии рост пропускной способности каналов связи глобальной сети (WAN) сделал возможным объединение сетей центрального офиса и филиалов с уровнем комфорта для пользователей, сравнимым с работой внутри локальной сети.

Однако уже на этом этапе развития стали возникать определенные сложности и проблемы. Традиционное WAN-подключение,

Концепция программно-определяемых распределенных сетей (Software-defined wide area network – SD-WAN) появилась относительно недавно – всего восемь лет назад и с момента своего появления вызывает интерес не только как очередной этап цифровой трансформации бизнеса, но и как новая точка роста рынка информационных технологий.

Так, например, анализируя общемировые тенденции развития рынка SD-WAN, специалисты Gartner ожидают, что к 2025 г. около 50% всех вновь приобретаемых SD-WAN-решений будут частью портфеля пограничных сервисов безопасного доступа (SASE), включающего предоставление услуг сети передачи данных и сетевой безопасности одним поставщиком. В нынешнем году этот показатель по всему миру составит не более 10%. Кроме того, предполагается, что к 2026 г. около 30% новых приобретений в сфере SD-WAN так или иначе будет распространяться по модели NaaS («сеть как сервис»). В настоящее время этот сегмент рынка находится в стадии формирования.

Анализ данных по отечественному ИТ-пространству показывает, что развитие сегмента SD-WAN серьезно тормозится санкционной изоляцией российского рынка от решений лидеров отрасли. Вместе с тем нельзя не отметить наличие отдельных успешных внедрений и российских разработок в этой области. Рассмотрим суть технологии SD-WAN и особенности ее применения.

при его сравнительно невысокой эксплуатационной стоимости, не могло гарантировать как 100%-ной доступности канала, так и необходимого качества передачи данных между точками, связанными по открытым каналам.

Для обеспечения надежности связи в офисах стали практиковаться избыточные подключения, которые осуществлялись одновременно через несколько каналов связи от разных операторов.

Если требовалось жесткое соблюдение качества соединения (гарантированные значения

разброса задержки, потери пакетов, важные для передачи голоса и видео), использовались операторские VPN-решения с гарантированным качеством на базе протокола MultiProtocol Label Switching (MPLS).

Несмотря на явные преимущества MPLS-подключений, высокая эксплуатационная стоимость услуг операторов, предоставляющих каналы гарантированного качества, не позволила полностью удовлетворить запросы компаний на связь с мелкими и средними периферийными офисами. А увеличение



Рис. 1. Общая схема топологии SD-WAN

количества малых офисов и домашних корпоративных пользователей сформировало потребность в создании и поддержке разветвленной структуры каналов связи и снижения затрат на управление распределенной сетью с множеством избыточных соединений.

Что такое технология SD-WAN и какие задачи она решает

Термин SD-WAN появился в 2014 г. для описания сетей, в которых механизм управления распределенной сетью (Control plane) отделялся от непосредственно сетевого оборудования, осуществляющего передачу данных (Data Plane).

В их основе находится выделенный контроллер, который в автоматическом режиме, согласно определенным заранее политикам, реализует управление трафиком внутри распределенной корпоративной сети.

Принято считать, что технология SD-WAN должна решать четыре обязательные задачи:

- поддерживать различные типы соединений для передачи данных, такие как MPLS, оптоволоконные сети последней мили и радиоканалы высокоскоростных сотовых сетей, использующие, например, технологии 4G LTE и 5G;
- динамически выбирать пути для распределения нагрузки и обеспечения отказоустойчивости каналов связи;
- иметь возможность централизованной настройки и управления сетью через простой единый интерфейс;
- поддерживать VPN-технологии и дополнительные сервисы, например, балансировщики

нагрузки, межсетевые экраны, веб-шлюзы и продукты для обеспечения сетевой безопасности.

Таким образом, внедренное в компании решение SD-WAN позволяет в реальном времени анализировать состояние каналов связи между узлами сети, в автоматическом режиме выбирая оптимальные пути для передачи различных типов данных на основе заранее определенных правил.

Кроме того, использование централизованного контроллера обеспечивает возможность не только существенно сократить затраты на ввод в эксплуатацию и повседневное администрирование маршрутизаторов в удаленных офисах, но и значительно повысить уровень безопасности сети в целом, поскольку граничные устройства внутри общей сети не обмениваются между собой служебной информацией напрямую.

Архитектура решений SD-WAN

В обобщенной архитектуре решений SD-WAN (рис. 1) можно выделить три основных компонента:

- оркестратор — основной узел управления сетью. Как правило, включает в себя портал управления, средства управления политиками и сетевыми устройствами, мониторинг сети и аналитику;
- контроллеры — управляющие узлы, ответственные за формирование таблиц маршрутизации и доставку информации на оконечные устройства;
- оконечные устройства — шлюзы, отвечающие за непосредственное подключение удаленного офиса к внешним каналам связи и корпоративной сети.

Для большинства решений доступна как On-premise модель, когда все компоненты приобретаются и размещаются в сети заказчика, так и облачное внедрение, когда заказчик покупает только оконечные устройства, а используемые управляющие компоненты уже развернуты в облаке производителя. Заказчик при этом оплачивает решение как услугу на регулярной основе и получает доступ к управлению своими устройствами.

Ключевые игроки. CISCO, VMware, Fortinet. Сходство и отличия

Согласно данным отчета компании Gartner, который опубликован в сентябре 2022 г. (рис. 2), лидерами в области разработки технологий SD-WAN на сегодняшний день являются компании Cisco Systems, VMware и Fortinet.

При этом каждая из компаний-лидеров прошла собственный уникальный путь разработки продукта, который определяется философией развития и существующей



Рис. 2. «Магический квадрат» Gartner, SD-WAN 2022 г.

линейкой продуктов. Рассмотрим их подробнее.

Cisco Systems вошла на рынок решений SD-WAN после приобретения компании Viptela, уже имея наработки в области программно-определяемых распределенных сетей (Cisco Intelligent WAN) и портфолио сетевого оборудования, закрывающего потребности заказчика любого уровня.

Для заказчиков, которые уже имеют в инфраструктуре оборудование на базе Cisco IOS XE, возможность использования существующих маршрутизаторов является несомненным преимуществом. Большая часть новых маршрутизаторов поддерживает полный набор средств сетевой безопасности.

Кроме того, существует решение, позволяющее использовать отечественные криптоалгоритмы взамен иностранных. Вместе с тем, именно наличие продвинутых технологий Cisco Systems, уже реализованных в оборудовании, зачастую тормозит приобретение функционала SD-WAN, так как выгоды, получаемые от сокращения затрат на обслуживание сети и оптимизации каналов, на фоне действующей сети не всегда очевидны для бизнеса.

VMware, как и Cisco Systems, для пополнения продуктового портфеля приобрела примерно в то же время компанию VeloCloud. Имея огромный опыт разработки систем виртуализации (в том числе сетевых устройств), компания сделала акцент на распознавании приложений, генерирующих сетевой трафик на оконечных устройствах, и фирменной технологии DMPO (Dynamic Multi-Path Optimization), которая позволяет гибко управлять распознанными потоками данных. Не будем забывать и о технологиях коррекции ошибок для транзакционных и realtime-приложений.

Также следует отметить простоту и продуманность механизма подключения новых оконечных точек ZTP (Zero-Touch Provisioning). Однако с точки зрения реализации механизмов сетевой безопасности решение полагается

больше на внешние средства, чем на встроенные механизмы. Его можно порекомендовать компаниям с высокой степенью внедрения продуктов и механизмов виртуализации на платформе VMware. Ярким примером успешного внедрения SD-WAN от VMware можно назвать совместный проект «ИТ-ГРАД» и CloudMTS.

При разработке своего SD-WAN-решения компания Fortinet пошла по пути интеграции механизмов управления потоками данных в существующее решение Fortinet Security Fabric, объединяющее все продукты производителя. Несмотря на то что в решении отсутствуют выделенные контроллеры, отвечающие за работу Control Plane, централизованное управление на базе ПО FortiManager позволяет отслеживать состояние каналов передачи данных и перераспределять трафик между различными каналами. Кроме того, следует отметить продуманную линейку оконечных устройств, простоту развертывания локальной системы управления и сравнительно низкую в сравнении с конкурентами стоимость внедрения.

А что у нас? Перспективы российского сегмента рынка. Отечественные разработки

Поскольку работа решения SD-WAN зависит как от аппаратного обеспечения, так и от программной части решения, создание подобной системы с нуля является серьезной задачей даже для крупных игроков зарубежного сетевого рынка.

Однако и российские разработки не стоят на месте. 25 марта 2021 г. компания BI.ZONE представила первое отечественное решение BI.ZONE Secure SD-WAN, включающее поддержку шифрования по ГОСТ. С его помощью можно построить центр управления сетью SD-WAN в локальной архитектуре либо с использованием облачных

сервисов BI.ZONE или провайдеров-партнеров. BI.ZONE Secure SD-WAN внесено в реестр российского ПО, а также имеет собственный протокол управления и маршрутизации.

Решение включает в себя систему управления и пограничные устройства BI.ZONE CyberEdge для подключения удаленных площадок. Граничное устройство CyberEdge совмещает в себе функции маршрутизатора с поддержкой LTE-связи, межсетевой экран, криптошлюз, сервер удаленного доступа мобильных пользователей, коммутатор и точку доступа.

Резидент фонда «Сколково», компания «Программируемые сети» Brain4Net, с 2015 г. ведет активные разработки в области программно-определяемых сетей. Флагманским продуктом в этом направлении является ее платформа B4N Service Platform, первоначально предназначенная для управления провайдерскими сетями. B4N Service Platform включает в себя все традиционные для архитектуры SD-WAN компоненты управления сетью (B4N Controller), оркестрации инфраструктуры и сервисов (B4N Orchestrator), а также организации высокоскоростной обработки трафика (B4N SwitchOS). На этой платформе уже был реализован проект программно-определяемых сетей для «Tele2» (совместно с компанией «Буллат»).

«Лаборатория Касперского» 27 октября 2021 г. завершила сделку по приобретению компании Brain4Net, а в июне 2022 г. анонсировала свое решение класса SD-WAN, построенное на базе приобретенных технологий.

В условиях, когда российские компании фактически отрезаны от сервисной поддержки западных производителей, наличие отечественных решений с круглосуточной технической поддержкой открывает новые перспективы развития SD-WAN-технологий не только для госкомпаний, обладающих критической информационной инфраструктурой, но и для российского бизнеса в целом. ■