УДК 67.05

УПРАВЛЕНИЕ МНОГОУРОВНЕВОЙ СЕТЕВОЙ ИНФРАСТРУКТУРОЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ CISCOSD-WAN

Примбек Айбек Батырбекұлы
Aybek.primbek@mail.ru
МагистрантРЭТ ЕНУим Л.Н. Гумилева,Казахстан, г. Нур-Султан
Научный руководитель – Канымгазиева И.А.

Корпоративная сетевая инфраструктура принимает Цифровое преобразование и быстро внедряет технологии для повышения производительности, снижения затрат и изменения клиентского опыта. Традиционная роль глобальной сети (WAN) заключалась в подключении пользователей филиала или кампуса к приложениям и для обеспечения безопасности и надежной связи использовались специальные схемы MPLS. Это больше не работает в цифровом мире, где приложения перемещаются из центра обработки данных в облако, и пользователи, которые потребляют эти приложения, становятся более мобильными, используя различные наборы устройств. Взрыв требований к пропускной способности оказывает значительное давление на пропускную способность сети, заставляя организации постоянно обновлять отдельные сети глобальной сети.

Для решения этих задач были разработаны программно-определяемые решения глобальной сети (SD-WAN). SD-WAN является частью более широкой технологии программно-определяемых сетей (SDN). По сравнению с традиционными сетевыми решениями, которые полагаются на интегрированные плоскости данных, контроля и управления в одной платформе, SDN отделяет плоскость пересылки от плоскости контроля и управления, что позволяет централизовать сетевой интеллект[3].

SD-WAN - это централизованный подход к управлению сетью, который абстрагирует базовую сетевую инфраструктуру от ее приложений. Это обеспечивает большую автоматизацию сети, упрощение операций, подготовку, мониторинг и устранение неполадок. SD-WAN - это применение этих принципов SDN к глобальной сети[2].

С самого начала технология SD-WAN была сосредоточена на четырех ключевых требованиях[4]:

- Увеличьте пропускную способность за счет активации неработающих резервных каналов и динамической балансировки нагрузки.
- Обеспечение более быстрый облачный и локальный доступ, включив прямой доступ в Интернет.
- Снижение операционных и управленческих затрат за счет централизованного управления, которое обычно осуществлялось на основе облачных технологий.
- Сокращение затрат на WAN, используя более дешевый Интернет или LTE-соединение в качестве альтернативы MPLS.

Цифровой бизнес эволюционировал, и сегодняшняя рабочая сила становится все более распределенной, а приложения, которые они потребляют, становятся все более децентрализованными, переходя от центра обработки данных к мультиоблачной среде. В сочетании с растущим числом пользователей, устройств и местоположений, нуждающихся в доступе к облачным приложениям, это создает огромную сложность для ИТ-служб. Cisco SD-WAN –это облачная архитектура, предназначенная для удовлетворения сложных потребностей современных глобальных сетей в трех ключевых областях[1]:

- Расширенная оптимизация приложений, обеспечивающая предсказуемый опыт работы приложений по мере развития стратегии бизнес-приложений;
- Многоуровневая безопасность, которая обеспечивает гибкость для развертывания нужной безопасности в нужном месте, будь то локальная или облачная;
- Простота в масштабе предприятия, которая обеспечивает сквозную политику от пользователя к приложению на тысячи сервисов.

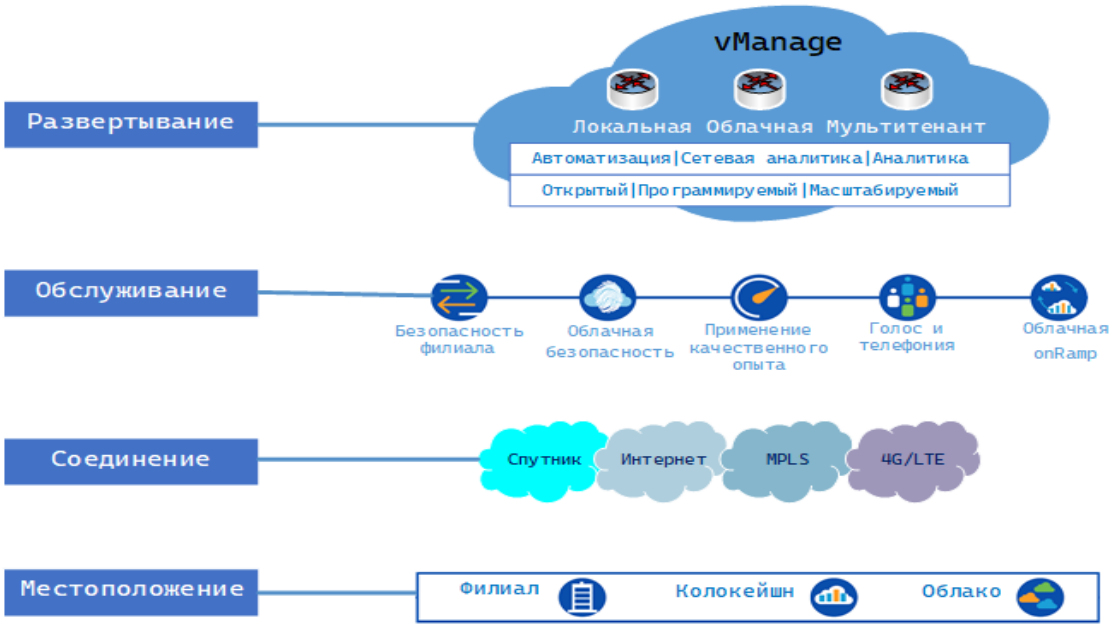

Рисунок - 1. Общая схема работы технологий SD-WAN

Решения SD-WAN следует использовать таким образом, чтобы снизить вероятность возникновения проблем с качеством приложений, но в случае их возникновения сеть должна реагировать автоматическим исправлением, чтобы минимизировать или устранить любое неблагоприятное воздействие. Обеспечение оптимального опыта для критически важных для бизнеса приложений требует понимания приложений в сети и соответствующих средств управления, которые должны быть применены для достижения желаемых результатов.

Решение Cisco SD-WAN представляет собой облачную архитектуру наложения Глобальной сети (WAN), которая расширяет принципы программно-определяемой сети (SDN) в WAN. Решение разбито на четыре плоскости: данные, контроль, управление и оркестровка[8].

Решение Cisco SD-WAN содержит четыре ключевых компонента, ответственных за каждую уровень организации:

Cisco vManage. В уровне управления Cisco vManage представляет пользовательский интерфейс решения. Сетевые администраторы и операторы выполняют здесь действия по настройке, подготовке, устранению неполадок и мониторингу.

Cisco vBond. Cisco vBond находится в уровне оркестровки. Контроллер vBond в значительной степени отвечает за процесс инициализации нулевого касания, а также за аутентификацию первой линии, распределение управляющей информации и облегчение обхода преобразования сетевых адресов (NAT). Когда маршрутизатор загружается в первый раз в неконфигурированном состоянии, v Bond отвечает за включение устройства в структуру SD-WAN. Задача vBond состоит в том, чтобы понять, как построена сеть, а затем поделиться этой информацией между другими компонентами.

Cisco vSmart. Cisco vSmart является "мозгом" решения и существует в плоскости управления. Поскольку политики создаются в vManage, vSmart является компонентом, ответственным за централизованное применение этих политик. Когда филиалы подключаются к сети, их маршрутная информация обменивается с интеллектуальным контроллером, а не напрямую с другими филиалами. С помощью политик информация о маршрутизации подвергается влиянию и совместно используется с другими местоположениями, что определяет, как отдельные ветви будут взаимодействовать друг с другом. Поскольку маршруты принимаются через протокол управления наложением (OMP) из филиалов, контроллер vSmart может вызывать политику, созданную на vManage, в отношении этих маршрутов и управлять тем, как трафик проходит через структуру SD-WAN.

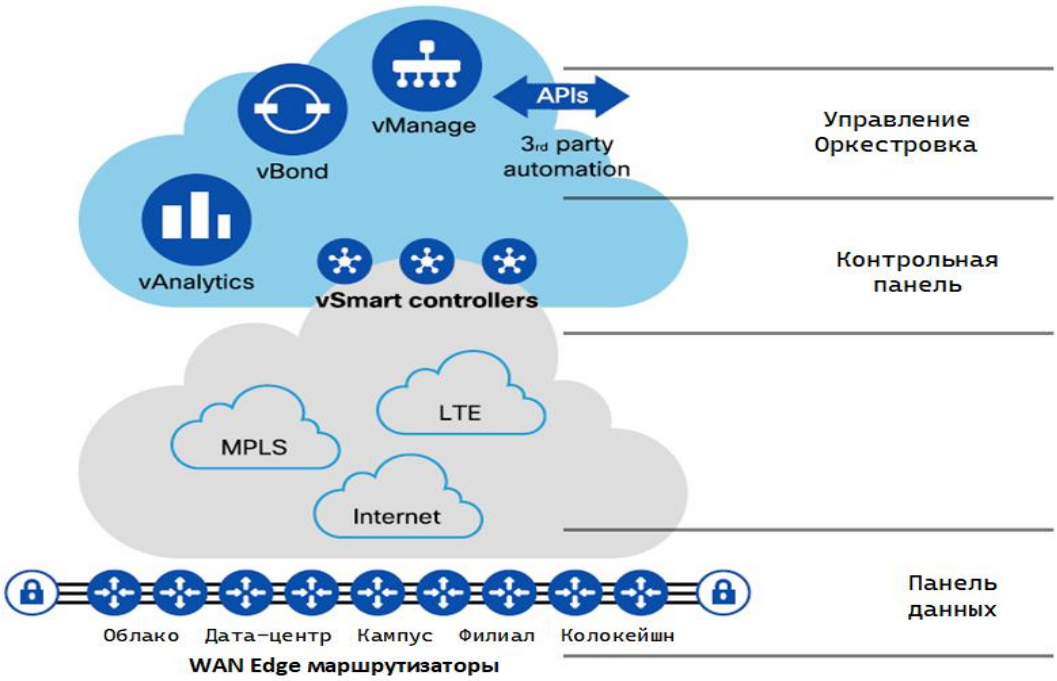

Рисунок – 2. Архитектура технологий CiscoSD-WAN

Маршрутизаторы Cisco WAN Edge. Маршрутизаторы Cisco WAN Edge отвечают за создание сетевой структуры и перенаправление трафика. Пограничные маршрутизаторы Cisco WAN бывают нескольких форм, виртуальных и физических, и выбираются на основе подключения, пропускной способности и функциональных потребностей сайта.

Все эти компоненты объединяются, чтобы сформировать Cisco SD-WAN fabric. Пограничные маршрутизаторы WAN образуют туннели Internet Protocol Security (IPSec) друг с другом, образуя наложение SD-WAN. Кроме того, между пограничными маршрутизаторами WAN и каждым из элементов управления устанавливается канал управления. Через этот канал управления каждый компонент получает информацию о конфигурации, подготовке и маршрутизации.

Высокая доступность и избыточность

Решение CiscoSD-WAN разработано с учетом доступности и производительности приложений в качестве краеугольного камня. Цель любого решения высокой доступности – обеспечить устойчивость сетевых служб к сбоям. Ядро решения CiscoSD-WANвысокой доступности достигается за счет сочетания трех факторов:

Резервирование устройств: Стратегия состоит из установки и подготовки резервных устройств и резервных компонентов в аппаратном обеспечении. Эти устройства соединены защищенной плоскостью управления, которая работает в активном/активном режиме.

Надежная конструкция сети: Поддержка нескольких протоколов (таких как VRRP, BGP и OSPF) и избыточных физических соединений как с сегментами LAN, так и с сегментами WAN.

Программные механизмы: Программные механизмы обеспечивают быстрое восстановление как от прямого, так и от косвенного отказа. Чтобы обеспечить устойчивую плоскость управления, решение регулярно отслеживает состояние всех пограничных маршрутизаторов WAN в сети и автоматически подстраивается под изменения топологии по мере присоединения маршрутизаторов к сети и выхода из нее. Для обеспечения устойчивости плоскости данных программное обеспечение CiscoSD-WAN реализует стандартные механизмы протокола, в частности BFD, который работает на защищенных туннелях IPSec между пограничными маршрутизаторами WAN.

Решение Cisco SD-WAN может быть развернуто на нескольких различных платформах, обычно называемых WAN Edge маршрутизаторами, которые доступны в различных форм-факторах. Пограничные маршрутизаторы WAN могут использоваться как в филиале, кампусе, центре обработки данных, публичном облаке, так и в частном облаке. Независимо от того, какое развертывание выбрано, все пограничные маршрутизаторы WAN будут частью структуры наложения SD-WAN и управляться через vManage. Существует два типа платформ, которые могут быть развернуты как часть Cisco SD-WAN[5]:

1. *Аппаратные платформы*

- Cisco vEdge (ранее Viptela wedge) Маршрутизаторы под управлением ОС Viptela
- Маршрутизатор интегрированных услуг (ISR) серии 1000 и 4000 под управлением программного обеспечения IOS XE SWAN
- Маршрутизатор служб агрегации (ASR) серии 1000 под управлением программного обеспечения IOS XE SD-WAN

2. *Виртуальные платформы*

- Маршрутизатор облачных сервисов (CSR) 1000v под управлением IOS XE SD-WAN Software
- vEdge Cloud Router подуправлением Viptela OS

Виртуальныеплатформымогутбытьразвернутынавычислительныхплатформах Cisco x86, например, Enterprise Network Computer System (ENCS) серии 5000, Unified Computing System (UCS) и Cloud Services Platform (CSP) серии 5000. Виртуальные платформы также могут работать на любом устройстве x86 с использованием гипервизора, такого как KVM или VMware ESXi.

Безопасность

Архитектура Cisco SD-WAN обеспечивает надежную защиту для операций плоскости управления, плоскости данных и плоскости управления. Чтобы ветви SD-WAN могли иметь прямой доступ в Интернет (DIA) без зависимости от другого устройства или решения для обеспечения безопасности, в пограничный маршрутизатор WAN встроены мощные механизмы защиты от угроз. Это обеспечивает защиту пользовательского трафика в филиальных сетях от интернет-угроз, а также повышает производительность приложений, позволяя трафику безопасно использовать DIA, когда это оптимальный путь. Ниже приведены функции защиты от угроз, доступные на пограничном маршрутизаторе WAN[6]:

- Брандмауэр приложений с отслеживанием состояния
- Защита и обнаружение вторжений (IPS/IDS)
- Фильтрация URL-адресов
- Cisco Advanced Malware Protection (AMP) и ThreatGRID
- Cisco Umbrella DNS
- Туннелирование для защиты интернет-шлюзов в облаке (третьи лица)

Пользователи и филиальная сеть могут быть защищены от Интернета путем реализации функций безопасности Cisco SD-WAN. Функции безопасности включают брандмауэр с поддержкой приложений, защиту от вторжений, фильтрацию URL-адресов, расширенную защиту от вредоносных программ и безопасность DNS. Эти функции безопасности могут быть развернуты либо на самом пограничном маршрутизаторе WAN, либо в качестве интегрированной сторонней службы безопасности.

Управление и операции

Ключевыми преимуществами решения Cisco SD-WAN являются автоматизированное управление и упрощение операций. Cisco vManage предлагает единое стекло для всех аспектов управления, мониторинга и устранения неполадок решения Cisco SD-WAN. Cisco vManage позволяет администраторам предоставлять новые сайты, развертывать политики, предоставлять глубокое понимание видимости и производительности приложений, проверять работоспособность устройств, выполнять обновления программного обеспечения и многое другое. Cisco vManage использует управление доступом на основе ролей (RBAC) для разделения обязанностей путем назначения различных прав доступа[7].

Cisco vManage предоставляет богатый набор REST API, которые могут управлять всем решением Cisco SD-WAN. Эти API также могут использоваться для пользовательской автоматизации и интеграции в другие системы или инструменты оркестровки.

Cisco vAnalytics предлагает дополнительный сервис на основе SaaS для предоставления дополнительной информации о работоспособности и доступности сети, производительности приложений и аномалиях, а также прогнозирования использования сети и приложений для лучшего планирования пропускной способности.

Cisco SD-WAN поддерживает мультитенантность, предлагая предприятиям гибкость сегрегированной работы. Multitenancy также может использоваться партнерами и поставщиками услуг для предоставления услуг Cisco SD-WAN своим клиентам.

Сетевая среда включает в себя центр обработки данных, кампус, филиал и внешних облачных провайдеров. Как часть меняющегося ландшафта сети, безопасность должна присутствовать и применяться от начала до конца. Преимущества интеграции технологий SD-WAN с существующим доменом позволяют ИТ-специалистам гибко распределять свои рабочие нагрузки по всей среде, сохраняя при этом надежный и безопасный доступ к пользователям и устройствам. Поскольку компании стремятся развить свою WAN от традиционных MPLS, Cisco SD-WAN предлагает как управляемое обслуживание, безопасность, так и оптимизацию приложений. API позволяют ИТ-специалистам легко интегрировать существующую операционную среду с Cisco SD-WAN и обеспечивают высокий уровень гибкости для предоставления новых возможностей. Это обеспечивает более целостное представление о системе, позволяя быстрее устранять неполадки.

Список литературы

1. Дэвид У. Ван. Software Defined-WAN для цифровой эпохи смелый переход к сетям следующего поколения / Международный Стандартный Книжный Номер-13: CRC Press Taylor & Francis Group. - Бока-Ратон: Флорида., - С.29-33
2. Технология SD-WAN [Электронный ресурс]. SD-WAN. URL: https://en.wikipedia.org/wiki/SD-WAN
3. Что такое технология SD-WAN[Электронный ресурс]. URL: https://www.silver-peak.com/sd-wan/sd-wan-explained
4. What is SD-WAN, and what does it mean for networking, security, cloud? [Электронный ресурс]. URL: https://www.networkworld.com/article/3031279/sd-wan-what-it-is-and-why-you-ll-use-it-one-day.html
5. Anshuman Awasthi. SDWAN (Software Defined-WAN) Network Engineering and Project Management. Semiconductor Science and Information Devices[Электронныйресурс]. 16.07.2020г.URL:https://www.researchgate.net/publication/341761695_SDWAN_Software_Defined-WAN_Network_Engineering_and_Project_Management
6. Anshuman Awasthi. SDWAN (Software Defined-WAN) Technology Evaluation and Implementation. Semiconductor Science and Information Devices [Электронныйресурс]. 16.07.2020г. URL: https://www.researchgate.net/publication/343073964_SDWAN_Software_Defined-WAN_Technology_Evaluation_and_Implementation
7. What Is SD-WAN. Choosing an SD-WAN Vendor [Электронныйресурс]. www.silver-peak.com/sd-wan/choosing-an-sd-wan-vendor
8. SD-WAN architecture [Электронныйресурс]. www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan