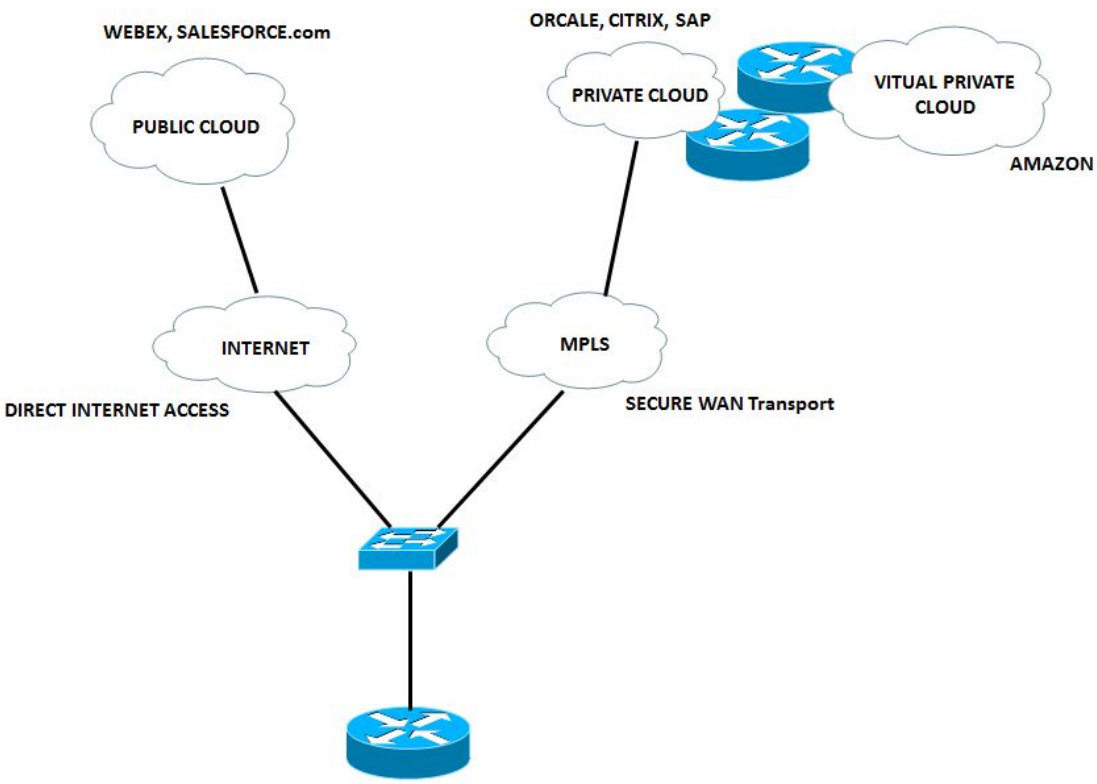
Содержание

IWAN

Интеллектуальная глобальная сеть (WAN) Cisco (IWAN) является системой, которая улучшает совместную работу и производительность "облачного" приложения при сокращении текущих расходов глобальной сети (WAN). Решение IWAN предоставляет руководство разработки и реализации для организаций, надеющихся развертывать транспортную независимую глобальную сеть (WAN) с интеллектуальным управлением маршрутом, оптимизацией приложения, и защищать подключение к Интернету и расположениям ответвления при сокращении текущих расходов глобальной сети (WAN). IWAN в полной мере пользуется премиальной глобальной сетью (WAN) и экономически эффективными интернет-сервисами для увеличения ширины полосы пропускания, не ставя под угрозу производительность, надежность или безопасность совместной работы или основанных на облачных вычислениях приложений. Организации могут использовать IWAN для усиления Интернета как транспорта глобальной сети (WAN), а также,



R1 предпочтет, чтобы голос и видеотрафик взяли оптимальный путь с относительно меньшей задержкой, дрожанием и/или потерей среди двух ссылок, доступных ему. Другой трафик с балансировкой нагрузки для максимизации пропускной способности.

Голос и видео перенаправлены, если текущий путь ухудшается (MPLS), и затем ссылка DIA выбрана.

IWAN позволяет вам:

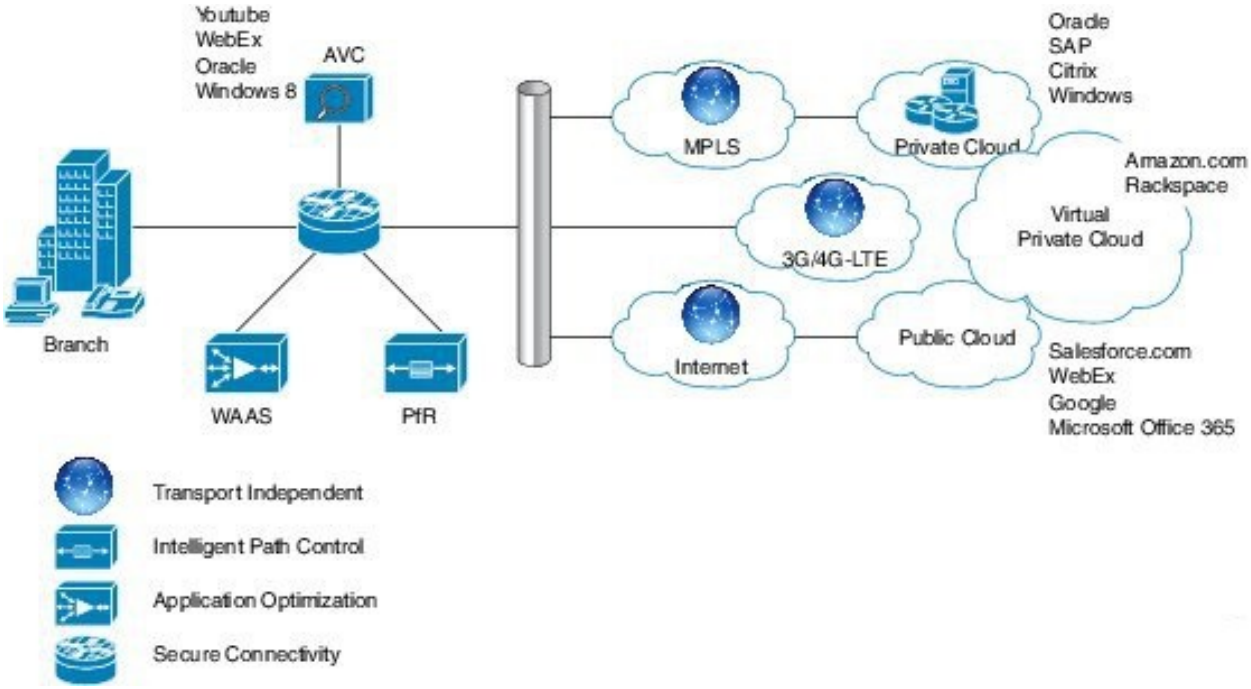
- Соединитесь с режимом снижения затрат как INTERNET для менее важных данных.
- Позволяет глобальной сети (WAN) использовать оптимизацию приложения, интеллектуальное кэширование и очень безопасный прямой доступ в Интернет.

До сих пор единственный способ получить надежное подключение с прогнозируемой производительностью состоял в том, чтобы использовать преимущества частной глобальной сети (WAN) с помощью сервиса выделенной линии или MPLS. Однако основанный на носителе MPLS и сервис выделенной линии могут быть дорогими и являются не всегда экономически эффективными для организации для использования для транспорта глобальной сети (WAN) для поддержки требований Растущей пропускной способности для подключения удаленного узла. Организации ищут способы понизить текущий бюджет, соответственно предоставляя сетевой транспорт для удаленного узла.

Cisco Интеллектуальная глобальная сеть (WAN) (IWAN) может позволить организациям отправить не поставивший под угрозу опыт по любому соединению. С Cisco IT-организация IWAN может предоставить больше пропускной способности их соединениям филиала компании с помощью менее дорогих опций транспорта глобальной сети (WAN), не влияя на производительность, безопасность или надежность. С решением IWAN трафик динамично маршрутизируется на основе соглашения об уровне обслуживания (SLA) приложения, типа оконечной точки и состояний сети для отправки опыта высшего качества.

С IWAN можно быстро развернуть приложения с интенсивным использованием полосы пропускания, такие как видео, инфраструктура виртуального рабочего стола (VDI) и гостевые сервисы Wi-Fi. И это не имеет значения, какую транспортную модель вы предпочитаете, ли Многопротокольная коммутация по меткам (MPLS), Интернет, сотовая связь или гибридная модель Доступа через WAN.

Следующий рисунок выделяет компоненты решения IWAN. Маршрутизация производительности является ключевым столбом этой инициативы:



Четыре компонента Cisco Интеллектуальная глобальная сеть (WAN):

- **Безопасный и гибкий независимый от транспорта дизайн**: Использование Динамической многоточечной VPN (DMVPN) IWAN предоставляет возможности легкой множественной адресации по любому предложению службы доставки, включая Многопротокольную коммутацию по меткам (MPLS), широкополосный доступ и сотовый 3G/4G/LTE.
- Технология: дизайн наложения DMVPN/IPsec

- **Интеллектуальное управление маршрутом: При помощи Производительности Cisco, Направляющей (PfR)**, этот компонент улучшает эффективность глобальной сети (WAN) и поставка приложения. PfR динамично управляет решениями по перенаправлению пакета данных путем рассмотрения типа приложения, производительности, политики и состояния маршрута. В то время как интеллектуальное распределение нагрузки трафика по лучшему выполнению соединяет каналом на основе правила приложений, PfR защищает бизнес - приложения от колеблющейся производительности глобальной сети (WAN). PfR контролирует производительность сети - дрожание, потерю пакета, задержку - и принимает решения направить критически важные заявления по лучшему пути выполнения на основе правила приложений. Cisco PfR состоит из граничных маршрутизаторов, которые соединяются с сервисом широкополосной передачи данных и приложением главного контроллера, поддерживаемым программным обеспечением Cisco IOSÂ® на маршрутизаторе. Граничные маршрутизаторы собирают трафик и информацию о пути и передают его к главному контроллеру, который обнаруживает и принуждает политику обслуживания для соответствия с требованием к приложению. Cisco PfR может выбрать выходной путь глобальной сети (WAN), чтобы разумно распределить нагрузку трафик на основе затрат канала, уменьшить полные расходы связи компании. IWAN интеллектуальное управление маршрутом является ключом к обеспечению глобальной сети (WAN) бизнес-класса по интернет-транспорту. Технология: Производительность, направляющая (PfR). PfR развивается к основному новому выпуску по имени PfRv3.

- **Оптимизация приложения**: Видимость Приложения Cisco и Контроль (AVC) и Сервисы WAAS (WAAS) Cisco предоставляют видимость производительности приложения и оптимизацию по глобальной сети (WAN). С приложениями, становящимися все более и более непрозрачной должный увеличить повторное использование известных портов, таких как HTTP (порт 80), классификация статических портов приложения больше не достаточна. AVC Cisco предоставляет осведомленности приложения глубокую проверку пакетов трафика, чтобы определить и контролировать производительность приложений. Видимость и контроль на прикладном уровне (уровень 7) предоставлены через технологии AVC, такие как Сетевое распознавание приложений 2 (NBAR2), NetFlow, качество обслуживания (QoS), Мониторинг производительности, Medianet и т.д. Технологии: видимость приложения и контроль (AVC), WAAS, подключение Akamai

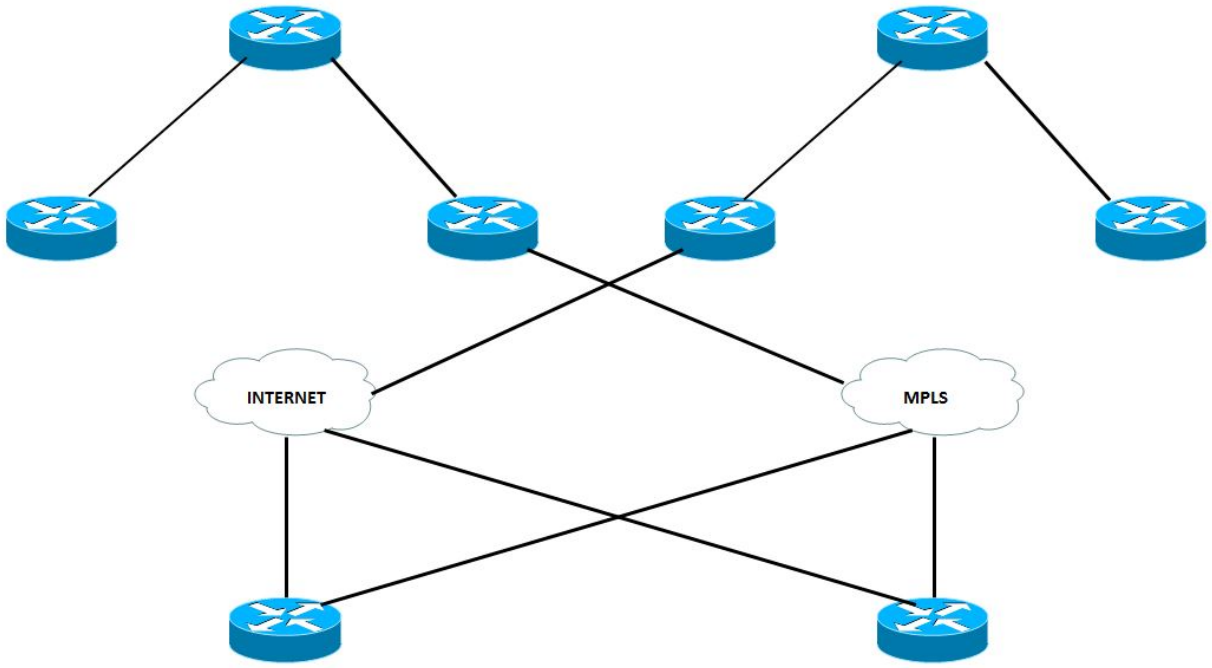
- **Безопасное подключение**: Это защищает глобальную сеть (WAN) и разгружает трафик пользователя непосредственно к Интернету. Сильное IP - безопасное шифрование, зональные межсетевые экраны и строгие списки доступа используются для защиты глобальной сети (WAN) по общедоступному Интернету. Маршрутизация пользователей ответвления непосредственно к Интернету улучшает производительность приложения открытого облака при сокращении трафика по глобальной сети (WAN). Сервис Облачной веб-безопасности (CWS) Cisco предоставляет основанный на облачных

вычислениях веб - прокси, чтобы централизованно управлять и защитить трафик пользователя, обращающийся к Интернету. Технологии:/IP Межсетевого экрана Cisco IOS, Облачная веб-безопасность (CWS)

ПОЧЕМУ ИСПОЛЬЗУЕТСЯ DMVPN

IWAN использует предписывающий дизайн с Гибридным Транспортным Независимым дизайном на основе DMVPN. DMVPN развернута через интернет-Транспорт и MPLS. Это значительно упрощает маршрутизацию при помощи одиночного домена маршрутизации, который охватывает оба транспорта. Маршрутизаторы DMVPN используют туннельные интерфейсы, которые поддерживают одноадресный IP - трафик, а также групповую IP-адресацию и широковещательный трафик, включая использование протоколов динамической маршрутизации. После того, как начальный туннель оконечного устройства - концентратора активен, возможно создать динамические туннели конечного маршрутизатор - конечного маршрутизатора, когда потоки IP - трафика от узла к узлу требуют его.

Транспортный Независимый Дизайн основывается на одном облаке DMVPN на поставщика. В этом руководстве два поставщика используются, один рассматриваемый как основного (MPLS) и один рассмотренный как вторичное устройство (Интернет). Узлы филиала связаны и с облаками DMVPN и с обоими туннелями, подключены.



Как показано в вышеупомянутой схеме, каждый Маршрутизатор для филиалов связан и с поставщиками, каждый - MPLS, который является основным и другой, INTERNET, который вторичен.

В зависимости от типа трафика каждый поставщик используется для передачи трафика. Пример: данные, которые имеют более высокий приоритет, могут быть отосланы через MPLS, и данные с меньшим приоритетом могут маршрутизироваться по INTERNET, это делает его, более эффективные с точки зрения затрат и свободные доступные ресурсы могут быть использованы для более инновационных бизнес-целей.

Сводка дизайна

Дизайн предоставляет активно-активные пути глобальной сети (WAN), которые в полной мере пользуются DMVPN для последовательного наложения IPsec. MPLS и Интернет-соединения могут быть завершены на одиночном маршрутизаторе или завершены на двух отдельных маршрутизаторах для дополнительной упругости. Тот же дизайн может использоваться по MPLS, Интернету или транспортам 3G/4G, делая транспорт дизайна - независимым.

Рекомендуется использовать концентратор DMVPN (PfRv3 BR) на поставщика и транспортировать на концентраторе. Это делает настройку маршрутизации намного легче.

DMVPN требует использования интернет-интервалов проверки активности версии 2 (IKEv2) Протокола управления ключами для Dead Peer Detection (DPD), который важен для упрощения быстрого повторного схождения и для лучевой регистрации для функционирования должным образом в случае, если повторно загружен концентратор DMVPN. Этот дизайн позволяет лучу обнаружить, что одноранговое шифрование отказало и что сеанс IKEv2 с тем узлом является устаревшим, который тогда позволяет новому быть созданным. Без DPD контекст безопасности IPSec должен испытать таймаут (по умолчанию составляет 60 минут), и когда маршрутизатор не может пересмотреть новый SA, новый сеанс IKEv2 инициируется. Максимальное время ожидания составляет приблизительно 60 минут.

Сводка фазы DMVPN

DMVPN имеет множественные фазы, которые суммированы ниже:

Фаза 1 DMVPN основывается на Концентраторе и Лучевой функциональности.

- Упрощенная и меньшая конфигурация на концентраторах
- Поддержка динамично обратилась к CPE (NAT)
- Поддержка протоколов маршрутизации и групповой адресации.
- Спицам не нужна полная таблица маршрутизации, может суммировать на концентраторе.

Фаза 2 DMVPN не имеет никакого суммирования на концентраторе:

Каждый луч имеет следующий переход (лучевой адрес) для каждого лучевого префикса получателя.

PfR имеет всю информацию для осуществления пути с динамическим PBR и корректной информацией о следующем переходе

DMVPN phase3 позволяет объединение маршрутов:

- Когда родительский поиск маршрута выполнен, только маршрут к концентратору доступен.
- NHRP динамично устанавливает туннель ярлыка и следовательно заполняет RIB/CEF.
- PfR все еще имеет информацию о следующем переходе концентратора и в настоящее

время не знает об изменении следующего перехода.
PfRv3 поддерживает все Фазы DMVPN.

Для получения дополнительной информации на DMVPN, см. ссылку:

http://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/DMVPN_Overview.pdf