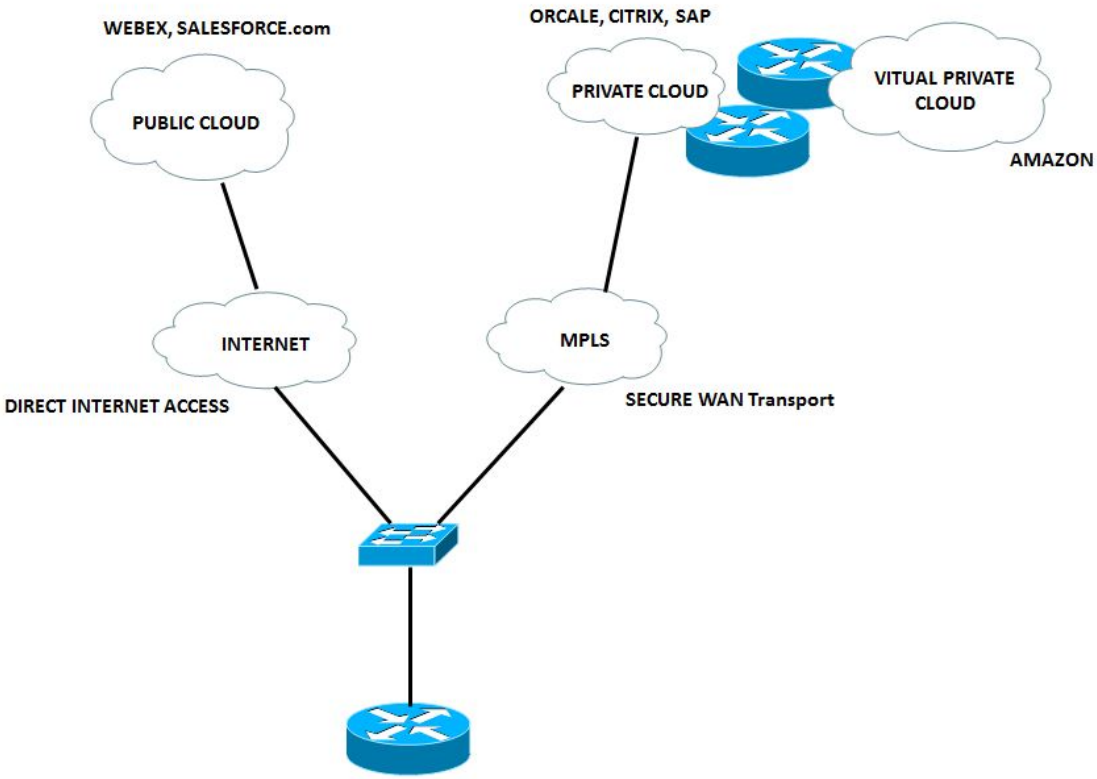
Introducción a IWAN y a PfRv3

Contenido

IWAN

Cisco WAN inteligente (IWAN) es un sistema que aumenta la Colaboración y el rendimiento de la aplicación de la nube mientras que reduce el costo operativo de WAN. La solución de IWAN proporciona la dirección del diseño y de la implementación para las organizaciones que miran para desplegar a una independiente WAN del transporte con el control de trayecto inteligente, la optimización de la aplicación, y la conectividad segura a Internet y a las redes derivadas mientras que reduce el costo operativo de WAN. IWAN aprovecha completo de WAN superior y de los servicios de Internet rentables para aumentar la capacidad de ancho de banda sin el funcionamiento, la confiabilidad, o la Seguridad de compromiso de la Colaboración o de las aplicaciones nube-basadas. Las organizaciones pueden utilizar a IWAN para leverage Internet como transporte PÁLIDO, así como, para el acceso directo a las aplicaciones públicas de la nube.



El r1 preferirá la Voz y el tráfico de video para llevar el mejor trayecto con relativamente poco retardo, jitter y/o pérdida entre los dos links disponibles ella. El otro tráfico es carga equilibrada para maximizar el ancho de banda.

Se rerrutea la Voz y el vídeo si el degrades(MPLS) del trayecto actual y entonces el link diámetro se elige.

IWAN le permite a:

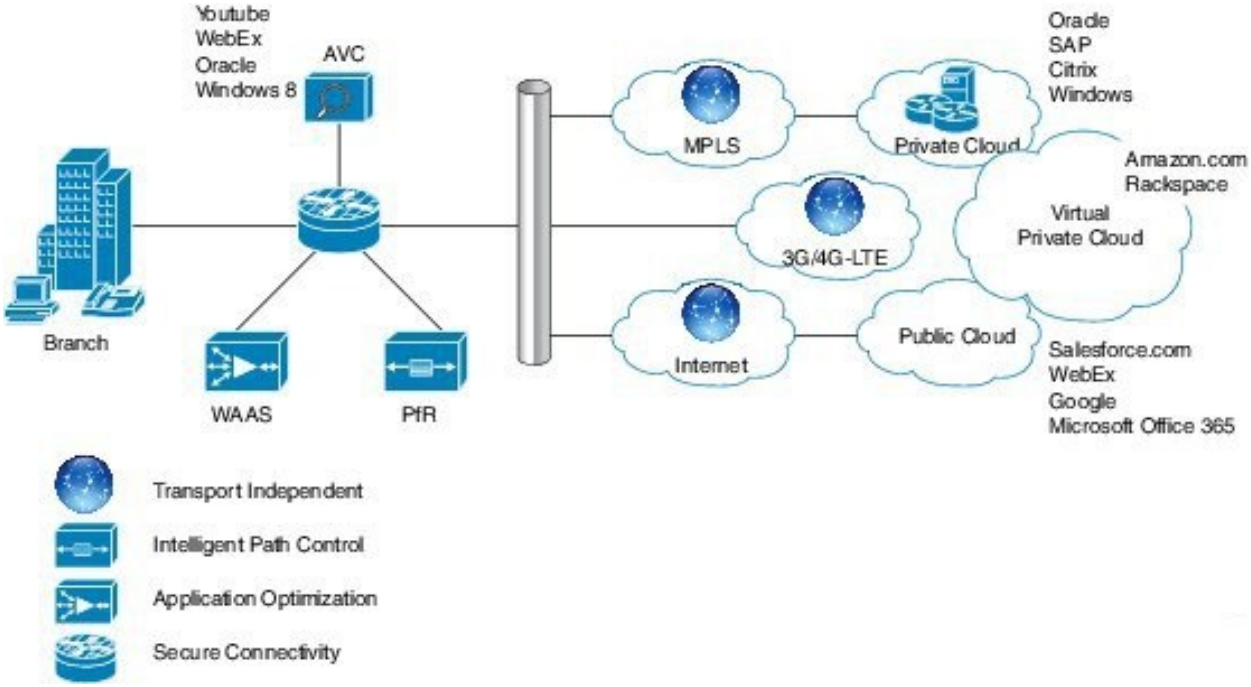
- Conecte con un modo más barato como INTERNET para los datos menos importantes.
- Permite que WAN utilice la optimización de la aplicación, almacenamiento en memoria inmediata inteligente, y que asegure altamente el acceso a internet directo.

Hasta ahora, la única forma de conseguir la conectividad confiable con el rendimiento predecible era aprovecharse de WAN privado usando el MPLS o el servicio de la línea arrendada. Sin embargo, el MPLS portador-basado y el servicio de la línea arrendada pueden ser costosos y no son siempre rentables para que una organización utilice para que el transporte PÁLIDO soporte los requisitos del ancho de banda creciente para la Conectividad del sitio remoto. Las organizaciones están buscando las maneras de bajar el presupuesto de funcionamiento mientras que adecuadamente proporcionan al transporte de la red para un sitio remoto.

Cisco WAN inteligente (IWAN) puede permitir a las organizaciones para entregar una experiencia uncompromised sobre cualquier conexión. Con Cisco IWAN LAS TIC la organización puede proporcionar más ancho de banda a sus conexiones de la sucursal usando las opciones PÁLIDAS menos costosas del transporte sin afectar al funcionamiento, a la Seguridad, o a la confiabilidad. Con la solución de IWAN, el tráfico se rutea dinámicamente sobre la base del Acuerdo de nivel de servicio (SLA) de la aplicación, del tipo del punto final, y de los estados de la red para entregar la mejor experiencia de la calidad.

Con IWAN, usted puede desarrollar rápidamente las aplicaciones de ancho de banda intensivo, tales como vídeo, infraestructura del escritorio virtual (VDI), y servicios del Wi-Fi del invitado. Y no importa que transportan el modelo que usted prefiere, si Multiprotocol Label Switching (MPLS), el Internet, celulares, o un modelo híbrido del acceso a WAN.

La figura siguiente delinea los componentes de la solución de IWAN. La encaminamiento del funcionamiento es un pilar dominante de esta iniciativa:



Los cuatro componentes de Cisco WAN inteligente son:

- **Diseño seguro y flexible de la transporte-independiente**: Usando el Dynamic Multipoint VPN (DMVPN) IWAN proporciona las capacidades para el multi-homing fácil sobre cualquier servicio de portadora que ofrece, incluyendo el Multiprotocol Label Switching (MPLS), la

Banda ancha, y 3G/4G/LTE celular.
- Tecnología: Diseño del recubrimiento DMVPN/IPsec

- **Control de trayecto inteligente: Usando la encaminamiento del funcionamiento de Cisco (PfR)**, este componente mejora la salida de la aplicación y la eficacia de WAN. PfR controla dinámicamente las decisiones de reenvío del paquete de datos por la mirada Application type (Tipo de aplicación), el funcionamiento, las directivas, y el Estado del trayecto. PfR protege las aplicaciones comerciales contra el funcionamiento PÁLIDO que fluctúa mientras que inteligente tráfico del balanceo de carga sobre la trayectoria más de funcionamiento satisfactorio basada en la directiva de la aplicación. PfR monitorea el rendimiento de la red - jitter, pérdida del paquete, retardo - y toma las decisiones para remitir las aplicaciones críticas sobre la trayectoria más de funcionamiento satisfactorio basada en la directiva de la aplicación. Cisco PfR consiste en los Router del borde que conectan con el servicio de banda ancha, y una aplicación del regulador principal soportada por el software de Cisco IOS® en un router. Los Router del borde recogen el tráfico y la información de trayecto y la envían al regulador principal, que detecta y aplica las políticas de servicio para hacer juego el requerimiento de la aplicación. Cisco PfR puede seleccionar una trayectoria PÁLIDA de la salida inteligente al tráfico del balance de la carga basado en los costes del circuito, para reducir los costos totales de las comunicaciones de una compañía. El control de trayecto inteligente de IWAN es la clave a proporcionar a una clase comercial WAN sobre el transporte de Internet. Tecnología: Encaminamiento del funcionamiento (PfR). PfR se desarrolla a una nueva versión importante llamada PfRv3.

- **Optimización de la aplicación**: La visibilidad de la aplicación de Cisco y el control (AVC) y el Wide Area Application Services de Cisco (WAAS) proporcionan la visibilidad y la optimización del rendimiento de la aplicación sobre WAN. Con las aplicaciones venciendo cada vez más opaco aumentar la reutilización de los puertos conocidos tales como HTTP (puerto 80), la clasificación del puerto estático de la aplicación es no más suficiente. Cisco AVC proporciona la conciencia de la aplicación con la inspección de paquetes profunda del tráfico para identificar y para monitorear el funcionamiento de las aplicaciones. Visibilidad y control en el nivel de aplicación (la capa 7) se proporciona con las Tecnologías AVC tales como reconocimiento de la aplicación basada en la red 2 (NBAR2), Netflow, Calidad de Servicio (QoS), supervisión de rendimiento, Medianet, y más. Tecnologías: La visibilidad y el control (AVC) de la aplicación, WAAS, Akamai conectan

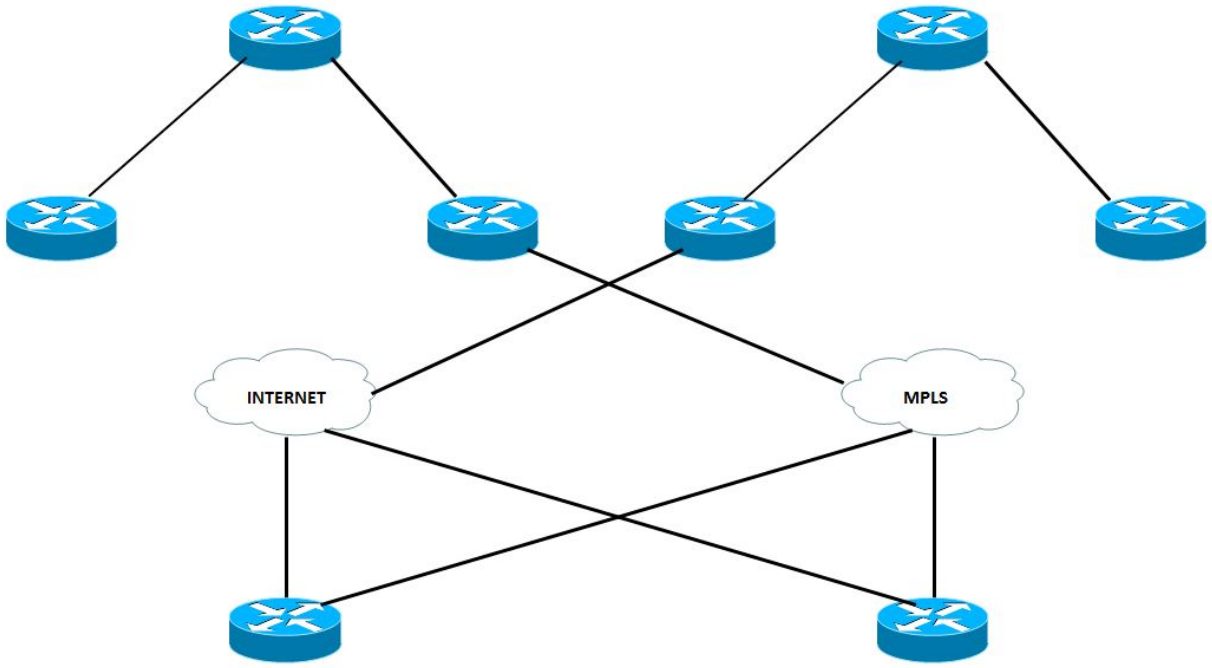
- **Conectividad segura**: Protege WAN y descarga el tráfico de usuarios directamente a Internet. La encripción de IPSec fuerte, los Firewall zona-basados, y las Listas de acceso estrictas se utilizan para proteger WAN sobre el Internet pública. Rutear a los usuarios de la bifurcación directamente a Internet mejora el rendimiento de la aplicación público de la nube mientras que reduce el tráfico sobre WAN. El servicio de la Seguridad de la red de la nube de Cisco (CWS) proporciona nube-basado Web Proxy (Proxy Web) centralmente para manejar y el tráfico del Usuario usuario seguro que accede Internet. Tecnologías: Cisco IOS Firewall/IPS, Seguridad de la red de la nube (CWS)

PORQUÉ SE ESTÁ UTILIZANDO EL DMVPN

IWAN utiliza un diseño preceptivo con un diseño independiente del transporte híbrido basado en el DMVPN. El DMVPN se despliega a través del MPLS y del transporte de Internet. Esto simplifica grandemente la encaminamiento usando un solo dominio de ruteo que abarque ambos

transportes. El Routers DMVPN utiliza las interfaces del túnel que soportan la unidifusión IP así como Multicast IP y tráfico de broadcast, incluyendo el uso de los Dynamic Routing Protocol. Después de que el túnel inicial del spoke a hub sea activo, es posible crear los túneles dinámicos del spoke al spoke cuando los flujos del tráfico IP del sitio a localizar lo requieren.

El diseño independiente del transporte se basa en una nube DMVPN por el proveedor. En esta guía dos se están utilizando los proveedores, uno que es considerado como el (MPLS) primario, y uno considerado como el secundario (Internet). Los sitios secundarios están conectados con ambas nubes DMVPN y ambos túneles están para arriba.



Tal y como se muestra en del diagrama antedicho, cada router de rama está conectado con ambos los proveedores, uno es el MPLS que es primario y otro es INTERNET que es secundario.

Dependiendo del tipo de tráfico, cada uno del proveedor se está utilizando para enviar el tráfico. Por ejemplo: los datos que está de prioridad más alta se pueden enviar con el MPLS y los datos con poca prioridad se pueden rutear sobre INTERNET, éste lo hace más rentable y los recursos disponibles libres pueden ser utilizados para objetivos comerciales más innovadores.

Resumen del diseño

El diseño proporciona las trayectorias PÁLIDAS activo-activas que aprovechan completo del DMVPN para el recubrimiento constante del IPSec. El MPLS y las conexiones de Internet se pueden terminar en un único router, o terminar en dos routeres separados para la elasticidad adicional. El mismo diseño se puede utilizar sobre el MPLS, Internet, o los transportes 3G/4G, haciendo a la independiente del transporte del diseño.

Se recomienda para utilizar un concentrador DMVPN (BR PfRv3) por el proveedor y el transporte en el concentrador. Hace la configuración de ruteo mucho más fácil.

El DMVPN requiere el uso de los intervalos de keepalive de la Versión del protocolo 2 de la

administración de claves de Internet (IKEv2) para el Dead Peer Detection (DPD), que es esencial facilitar el reconvergence rápido y para que funcione el registro del spoke correctamente en caso de que se recargue un concentrador DMVPN. Este diseño habilita habló para detectar que un peer de encripción ha fallado y que la sesión IKEv2 con ese par es añeja, que entonces permite que un nuevo sea creado. Sin el DPD, IPSec SA debe medir el tiempo hacia fuera (el valor por defecto es 60 minutos) y cuando el router no puede renegociar un nuevo SA, se inicia una nueva sesión IKEv2. El tiempo de espera máximo es aproximadamente 60 minutos.

Resumen de la fase DMVPN

El DMVPN tiene fases múltiples que se resuman abajo:

La fase 1 DMVPN se basa en las funciones del hub and spoke.

- Configuración simplificada y más pequeña en el Hubs
- El soporte dirigió dinámicamente CPEs (NAT)
- Soporte para los Routing Protocol y el Multicast.
- El spokes no necesita la tabla de ruteo completa, puede resumir en el concentrador.

La fase 2 DMVPN no tiene ningún resumen en el concentrador:

Cada spoke tiene el Next-Hop (direccionamiento del spoke) para cada prefijo de destino del spoke.

PfR tiene toda la información para aplicar la trayectoria con el PBR dinámico y la información correcta del Next-Hop

El DMVPN phase3 permite el resumen de Route:

- Cuando se realizan las operaciones de búsqueda de la ruta del padre, sólo la ruta al concentrador está disponible.
- El NHRP instala dinámicamente el túnel del acceso directo y por lo tanto puebla RIB/CEF.
- PfR tiene la información del Next-Hop del concentrador y sigue siendo actualmente inconsciente del cambio del Next-Hop.

PfRv3 soporta todas las fases DMVPN.

Para más información sobre el DMVPN, refiera por favor al link:

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