Introduction to IWAN and PfRv3

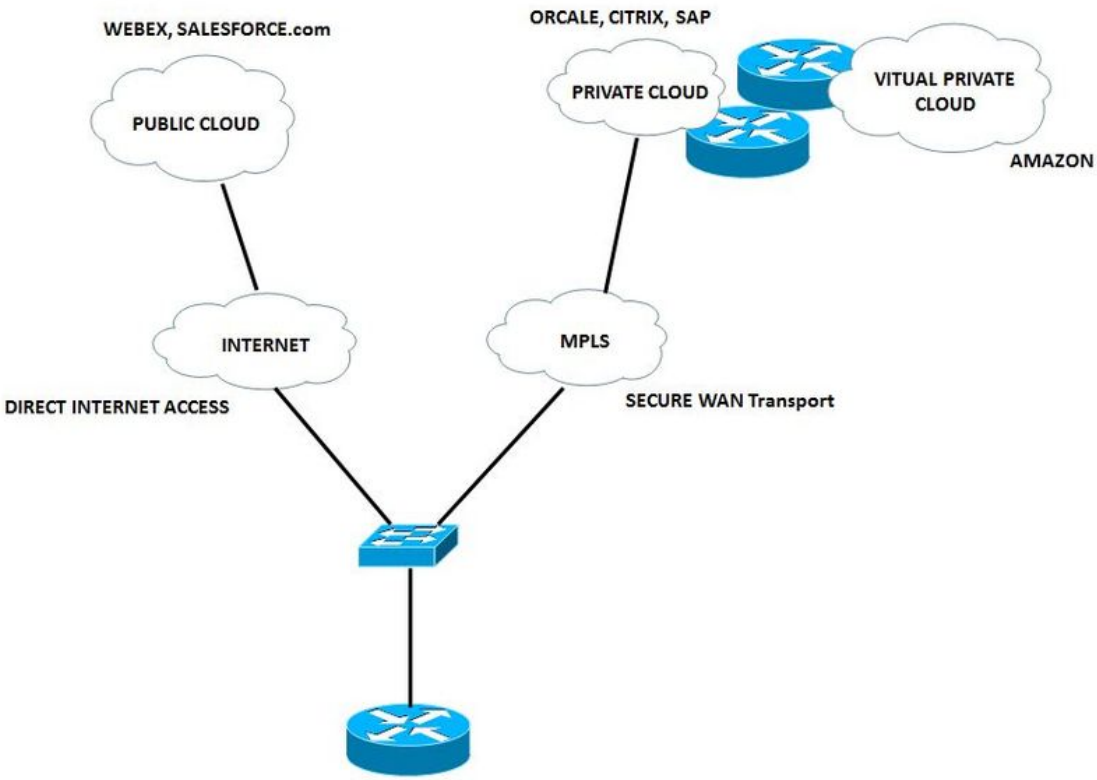
Contents

Introduction

This document describes Cisco Intelligent WAN (IWAN) and Cisco Performance Routing (PfR).

IWAN

The Cisco IWAN is a system that enhances collaboration and cloud application performance, while it also reduces the operating cost of the WAN. The IWAN solution provides design and implementation guidance for organizations that look to deploy a transport independent WAN with intelligent path control, application optimization, and secure connectivity to the Internet and branch locations while it reduces the operating cost of the WAN. IWAN takes full advantage of premium WAN and cost-effective Internet services to increase bandwidth capacity without a compromise in performance, reliability, or security of collaboration or cloud-based applications. Organizations can use IWAN in order to leverage the Internet as a WAN transport, as well as for direct access to public cloud applications.



R1 will prefer voice and video traffic to take the best path with a relatively less delay, jitter and/or loss among the two links available to it. Other traffic is load balanced in order to maximize bandwidth.

Voice and video is rerouted if the current path degrades (Multiprotocol Label Switching (MPLS)) and then the Direct Internet Access (DIA) link is chosen.

IWAN allows you to:

- Connect to a lower cost mode as INTERNET for less important data.
- Allows WAN to use application optimization, intelligent caching, and highly secure DIA.

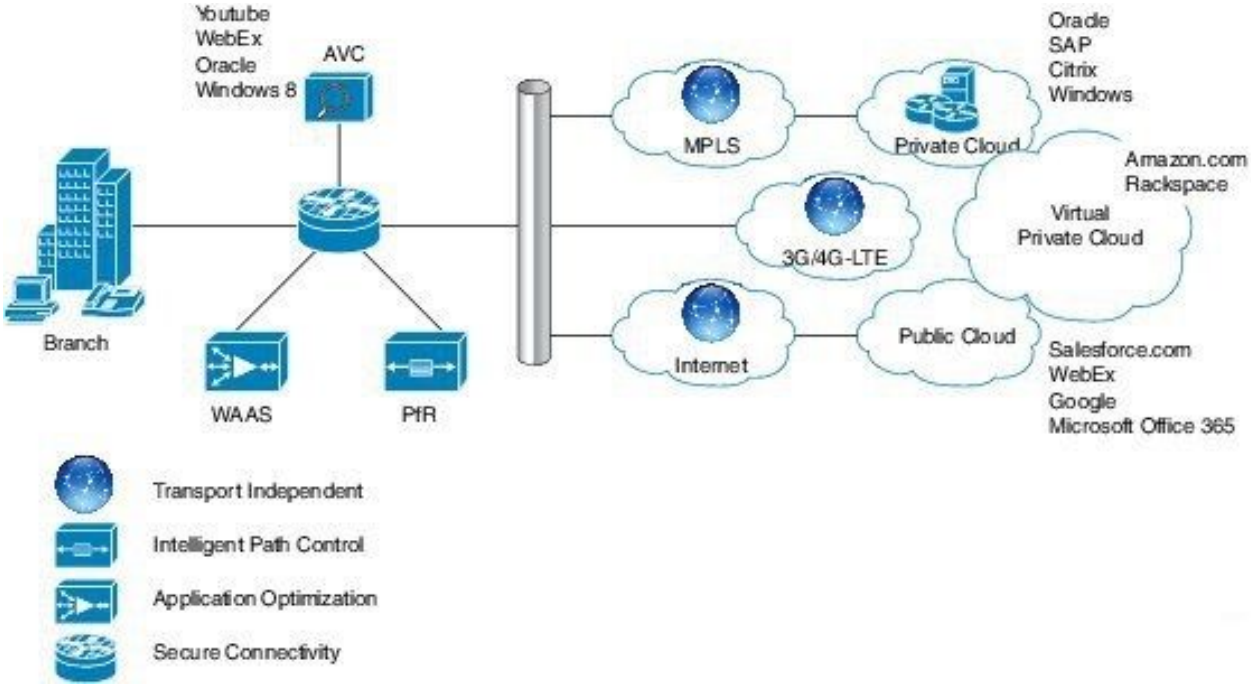
So far, the only way to get reliable connectivity with predictable performance is to take advantage of a private WAN using MPLS or a leased line service. However, carrier-based MPLS and leased line services can be expensive and are not always cost-effective for an organization to use for WAN transport to support growing bandwidth requirements for remote-site connectivity. Organizations look for ways to lower their operating budget while adequately providing the network transport for a remote site.

IWAN can enable organizations to deliver an uncompromised experience over any connection. With Cisco IWAN, IT organizations can provide more bandwidth to their branch office connections with less expensive WAN transport options without affecting performance, security, or reliability. With the IWAN solution, traffic is dynamically routed based on application service-level agreement (SLA), endpoint type, and network conditions to deliver the best quality experience.

With IWAN, you can quickly roll out bandwidth-intensive applications, such as video, virtual desktop infrastructure (VDI), and guest Wi-Fi services. And it does not matter which transport model you prefer, whether MPLS, the Internet, cellular, or a hybrid WAN access model.

This figure outlines the components of the IWAN solution. Performance Routing is a key pillar of

this initiative:



The four components of IWAN are:

- **Secure and flexible transport-independent design -** Dynamic Multipoint VPN (DMVPN) IWAN provides capabilities for easy multi-homing over any carrier service offering, which includes MPLS, broadband, and cellular 3G/4G/LTE. Technology: DMVPN/IPsec overlay design

- **Intelligent path control -** With Cisco PfR, this component improves application delivery and WAN efficiency. PfR dynamically controls data packet forwarding decisions by looking at application type, performance, policies, and path status. PfR protects business applications from fluctuating WAN performance while intelligently load-balancing traffic over the best performing path based on the application policy. PfR monitors the network performance - jitter, packet loss, delay - and makes decisions to forward critical applications over the best performing path based on the application policy. Cisco PfR consists of border routers that connect to the broadband service, and a primary controller application supported by Cisco IOS® Software on a router. The border routers collect traffic and path information and send it to the primary controller, which detects and enforces the service policies to match the application requirement. Cisco PfR can select an egress WAN path to intelligently load-balance traffic based on circuit costs in order to reduce a company's overall communications expenses. IWAN intelligent path control is the key to providing a business-class WAN over Internet transport. Technology: PfR. PfR evolves to a major new release called PfRv3.

- **Application optimization -** Cisco Application Visibility and Control (AVC) and Cisco Wide Area Application Services (WAAS) provide application performance visibility and optimization over the WAN. With applications becoming increasingly opaque due to increase reuse of well-known ports such as HTTP (port 80), static port classification of application is no longer sufficient. Cisco AVC provides application awareness with deep packet inspection of traffic to identify and monitor applications' performance. Visibility and control at the application level (layer 7) is provided through AVC technologies such as Network-Based Application Recognition 2 (NBAR2), NetFlow, quality of service (QoS), Performance Monitoring,

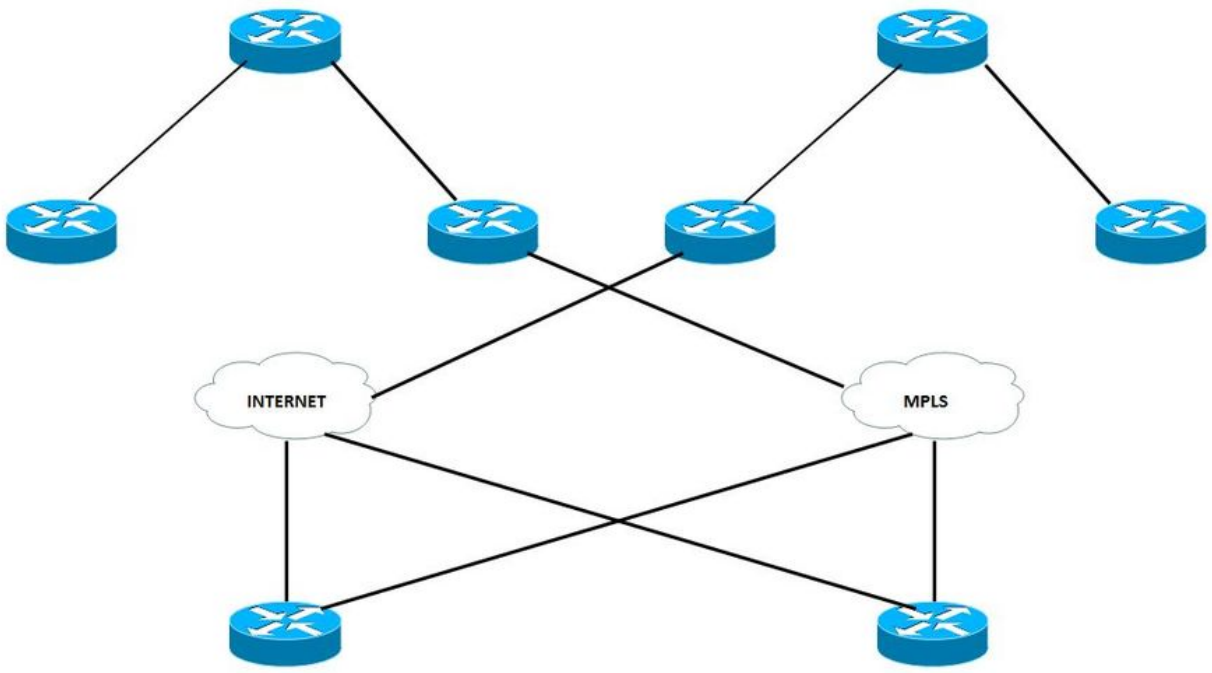
Medianet, and more. Technologies: Application Visibility and Control (AVC), WAAS, Akamai Connect

- **Secure connectivity -** It protects the WAN and offloads user traffic directly to the Internet. Strong IPsec encryption, zone-based firewalls, and strict access lists are used to protect the WAN over the public Internet. Routing branch users directly to the Internet improves public cloud application performance while reducing traffic over the WAN. Cisco Cloud Web Security (CWS) service provides a cloud-based web proxy to centrally manage and secure user traffic accessing the Internet. Technologies: Cisco IOS Firewall/IPS, Cloud Web Security (CWS)

Why DMVPN is Used

IWAN uses a prescriptive design with an Hybrid Transport Independent design based on DMVPN. DMVPN is deployed across MPLS and Internet Transport. This greatly simplifies the routing by using a single routing domain that encompasses both transports. The DMVPN routers use tunnel interfaces that support IP unicast as well as IP multicast and broadcast traffic, which includes the use of dynamic routing protocols. After the initial spoke-to-hub tunnel is active, it is possible to create dynamic spoke-to-spoke tunnels when site-to-site IP traffic flows require it.

The Transport Independent Design is based on one DMVPN cloud per provider. In this guide two providers are used, one is considered the primary (MPLS), and one is considered the secondary (Internet). Branch sites are connected to both DMVPN clouds and both tunnels are up.



As shown in the diagram, each Branch router is connected to both the providers, one is MPLS which is primary and other is INTERNET which is secondary.

Dependent on the type of traffic, each of the providers is used to send the traffic. For example, data which is of higher priority can be sent out through MPLS and data with lesser priority can be routed over INTERNET. This makes it more cost effective and frees available resources can be

utilized for more innovative business purposes.

Transport Independent Design (Dual DMVPN)

Design Summary

The design provides active-active WAN paths that take full advantage of DMVPN for consistent IPsec overlay. The MPLS and Internet connections can be terminated on a single router, or terminated on two separate routers for additional resiliency. The same design can be used over MPLS, Internet, or 3G/4G transports, which makes the design transport- independent.

It is recommended to use a DMVPN hub (PfRv3 BR) per provider and transport on the hub. It makes the routing configuration much easier.

DMVPN requires the use of Internet Key Management Protocol version 2 (IKEv2) keepalive intervals for Dead Peer Detection (DPD), which is essential to facilitate fast reconvergence and for spoke registration to function properly in case a DMVPN hub is reloaded. This design enables a spoke to detect that an encryption peer has failed and that the IKEv2 session with that peer is stale, which then allows a new one to be created. Without DPD, the IPsec SA must time out (the default is 60 minutes) and when the router cannot renegotiate a new SA, a new IKEv2 session is initiated. The maximum wait time is approximately 60 minutes.

DMVPN Phase Summary

DMVPN has multiple phases that are summarized here:

DMVPN Phase 1 is based on Hub and Spoke functionality.

- Simplified and smaller configuration on hubs
- Support dynamically addressed CPEs (NAT)
- Support for routing protocols and multicast
- Spokes do not need full routing table, can summarize on hub

DMVPN Phase 2 has no summarization on the hub.

Each spoke has the next-hop (spoke address) for each spoke destination prefix.

PfR has all the information to enforce the path with dynamic PBR and the correct next-hop information.

DMVPN phase3 allows route summarization:

- When parent route lookup is performed, only the route to the hub is available.
- NHRP dynamically installs shortcut tunnel and hence populates RIB/CEF.
- PfR still has the hub next-hop information and is currently unaware of the next-hop change.

PfRv3 supports all DMVPN phases.

For further information on DMVPN, see Cisco IOS DMVPN Overview.