Einführung in IWAN und PfRv3

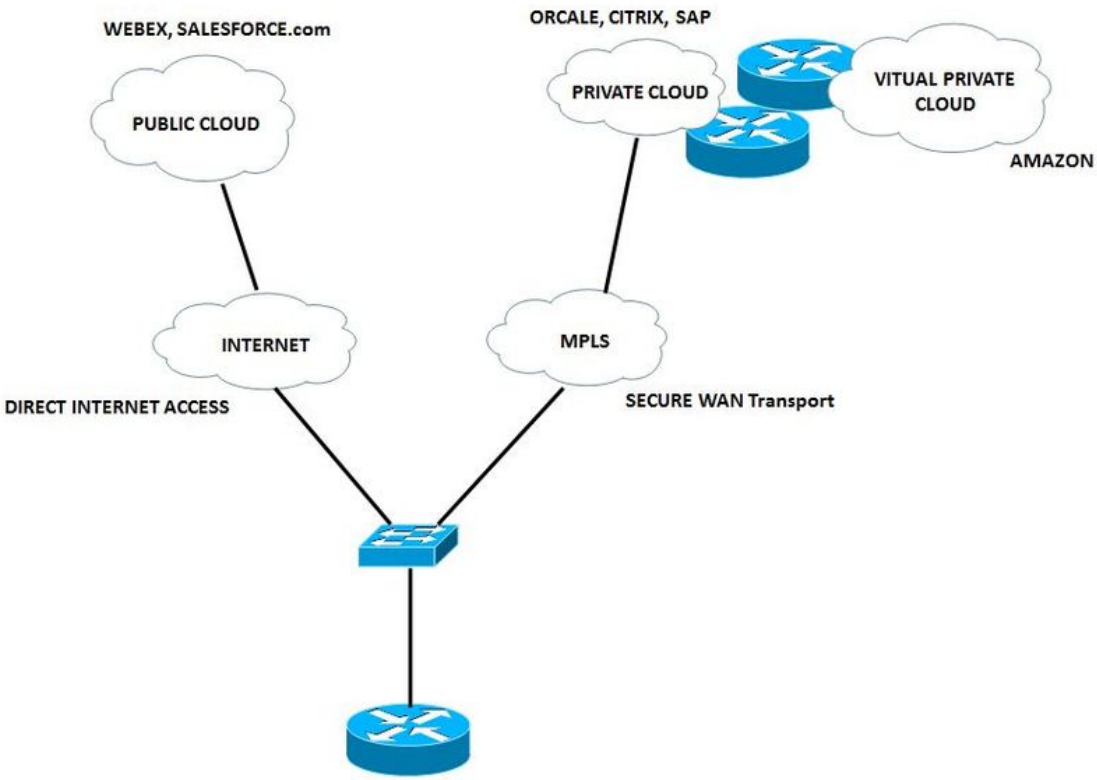
Inhalt

Einführung

Dieses Dokument beschreibt Cisco Intelligent WAN (IWAN) und Cisco Performance Routing (PfR).

IWAN

Das Cisco IWAN ist ein System, das die Leistung von Collaboration- und Cloud-Anwendungen verbessert und gleichzeitig die Betriebskosten des WAN senkt. Die IWAN-Lösung bietet Unternehmen, die ein transportunabhängiges WAN mit intelligenter Pfadkontrolle, Anwendungsoptimierung und sicherer Konnektivität zum Internet und zu Zweigstellen bereitstellen möchten, Design- und Implementierungsanleitungen und senkt gleichzeitig die Betriebskosten des WAN. Das IWAN nutzt Premium-WAN und kosteneffiziente Internetservices, um die Bandbreitenkapazität ohne Beeinträchtigung der Leistung, Zuverlässigkeit oder Sicherheit von Collaboration- oder Cloud-basierten Anwendungen zu erhöhen. Organisationen können IWAN verwenden, um das Internet als WAN-Transportnetz sowie den direkten Zugriff auf Public Cloud-Anwendungen zu nutzen.



R1 bevorzugt Sprach- und Videodatenverkehr, um den besten Pfad mit einer relativ geringeren Verzögerung, Jitter und/oder Verlust zwischen den beiden verfügbaren Verbindungen zu verwenden. Für den anderen Datenverkehr wird ein Load Balancing durchgeführt, um die Bandbreite zu maximieren.

Sprache und Video werden umgeleitet, wenn der aktuelle Pfad abfällt (Multiprotocol Label Switching (MPLS)) und dann die Direktverbindung für den Internetzugang (DIA) ausgewählt wird.

IWAN bietet Ihnen folgende Vorteile:

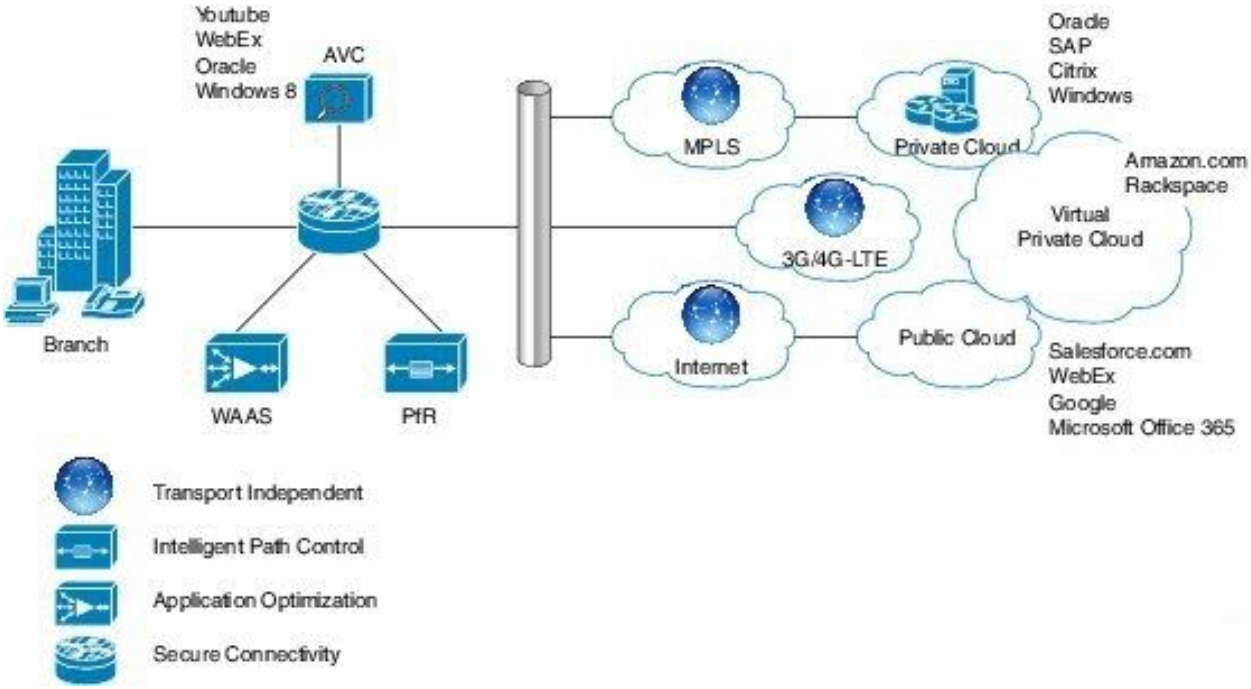
- Stellen Sie für weniger wichtige Daten eine Verbindung zu einem kostengünstigeren Internet-Modus her.
- Ermöglicht WAN die Verwendung von Anwendungsoptimierung, intelligentem Caching und hochsicherem DIA.

Bisher ist die einzige Möglichkeit, zuverlässige Verbindungen mit vorhersehbarer Leistung zu erhalten, die Nutzung eines privaten WAN über MPLS oder einen Mietleitungsdienst. Carrier-basierte MPLS- und Mietleitungsdienste können jedoch teuer sein und sind für Unternehmen nicht immer kosteneffizient, wenn sie für den WAN-Transport eingesetzt werden, um die wachsenden Bandbreitenanforderungen für die Anbindung von Remote-Standorten zu unterstützen. Unternehmen suchen nach Möglichkeiten, ihr Betriebsbudget zu senken und gleichzeitig den Netzwerktransport für Remote-Standorte angemessen bereitzustellen.

Mit IWAN können Organisationen über jede Verbindung ein uneingeschränktes Anwendererlebnis gewährleisten. Mit dem Cisco IWAN können IT-Abteilungen ihren Zweigstellenverbindungen mehr Bandbreite mit kostengünstigeren WAN-Transportoptionen bereitstellen, ohne die Leistung, Sicherheit oder Zuverlässigkeit zu beeinträchtigen. Die IWAN-Lösung ermöglicht eine dynamische Weiterleitung des Datenverkehrs auf der Grundlage von Application Service Level Agreement (SLA), Endgerätetyp und Netzwerkbedingungen, um ein optimales Anwendererlebnis zu gewährleisten.

Mit IWAN können Sie schnell bandbreitenintensive Anwendungen wie Video, Virtual Desktop Infrastructure (VDI) und Gast-Wi-Fi-Services bereitstellen. Dabei spielt es keine Rolle, welches Transportmodell Sie bevorzugen, ob MPLS, das Internet, Mobilfunk oder ein Hybrid-WAN-Zugriffsmodell.

In dieser Abbildung sind die Komponenten der IWAN-Lösung dargestellt. Performance Routing ist eine der wichtigsten Säulen dieser Initiative:



Die vier Komponenten von IWAN sind:

- **Sicheres und flexibles transportunabhängiges Design - Das** Dynamic Multipoint VPN (DMVPN) IWAN bietet Funktionen für einfaches Multihoming über alle Carrier-Services, einschließlich MPLS, Breitband und mobiles 3G/4G/LTE. Technologie: DMVPN/IPsec-Overlay-Design

- **Intelligente Pfadkontrolle -** Mit Cisco PfR verbessert diese Komponente die Anwendungsbereitstellung und WAN-Effizienz. Der PfR steuert dynamisch Entscheidungen zur Weiterleitung von Datenpaketen, indem er Anwendungstyp, Leistung, Richtlinien und Pfadstatus berücksichtigt. PfR schützt Geschäftsanwendungen vor Schwankungen der WAN-Leistung und sorgt für einen intelligenten Lastenausgleich des Datenverkehrs über den leistungsstärksten Pfad, der auf der Anwendungsrichtlinie basiert. Der PfR überwacht die Netzwerkleistung - Jitter, Paketverlust, Verzögerung - und trifft auf der Grundlage der Anwendungsrichtlinie Entscheidungen zur Weiterleitung kritischer Anwendungen über den leistungsstärksten Pfad. Cisco PfR besteht aus Border Routern, die mit dem Breitbanddienst verbunden sind, und einer primären Controller-Anwendung, die von der Cisco IOS®-Software auf einem Router unterstützt wird. Die Grenzrouter erfassen Verkehrs- und Pfadinformationen und senden diese an den primären Controller, der die Service-Richtlinien entsprechend der Anwendungsanforderungen erkennt und durchsetzt. Cisco PfR kann einen WAN-Ausgangspfad für einen intelligenten Lastenausgleich des Datenverkehrs basierend auf Schaltungskosten auswählen, um die Kommunikationskosten des Unternehmens insgesamt zu senken. Die intelligente Pfadkontrolle über das IWAN ist der Schlüssel zur Bereitstellung eines WAN-over-Internet-Transports der Business-Klasse. Technologie: PfR PfR entwickelt

sich zu einer neuen Hauptversion namens PfRv3.

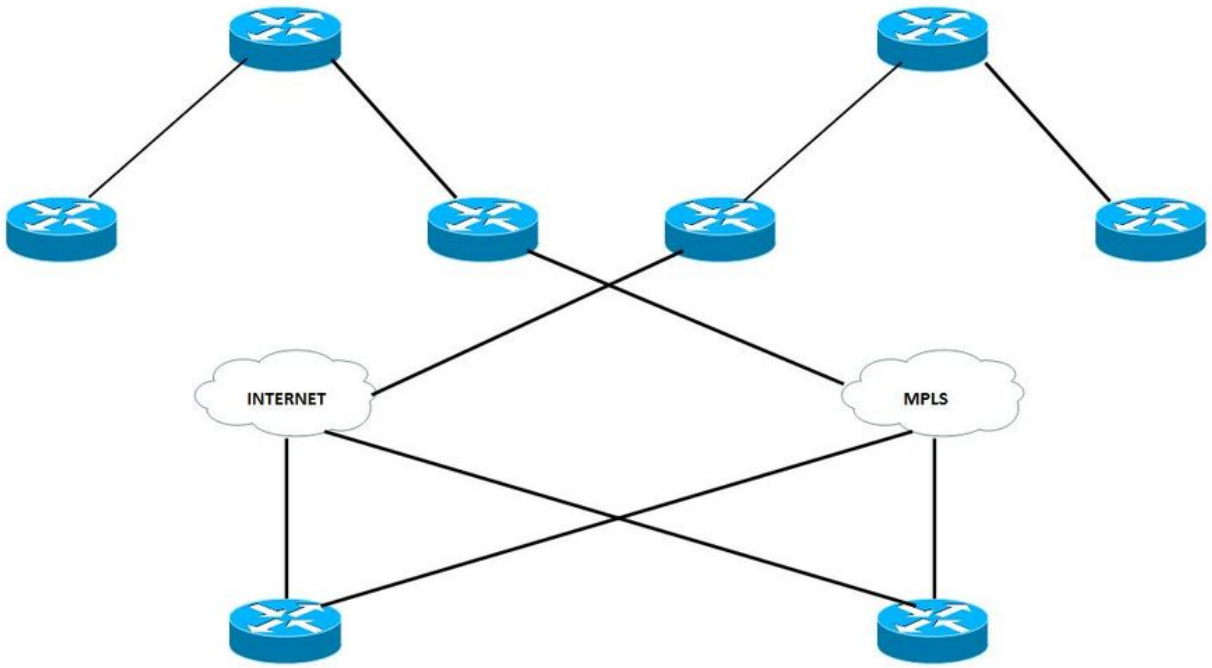
- **Anwendungsoptimierung -** Cisco Application Visibility and Control (AVC) und Cisco Wide Area Application Services (WAAS) bieten Anwendungstransparenz und -optimierung über das WAN. Da Anwendungen aufgrund der zunehmenden Wiederverwendung bekannter Ports wie HTTP (Port 80) zunehmend undurchsichtig werden, reicht eine statische Port-Klassifizierung der Anwendung nicht mehr aus. Cisco AVC bietet Anwendungserkennung durch Deep Packet Inspection des Datenverkehrs, um die Anwendungsleistung zu identifizieren und zu überwachen. Transparenz und Kontrolle auf Anwendungsebene (Layer 7) wird durch AVC-Technologien wie Network-Based Application Recognition 2 (NBAR2), NetFlow, Quality of Service (QoS), Performance Monitoring, Medianet usw. gewährleistet. Technologien: Application Visibility and Control (AVC), WAAS, Akamai Connect

- **Sichere Konnektivität -** Sie schützt das WAN und lagert Benutzerdatenverkehr direkt in das Internet aus. Starke IPsec-Verschlüsselung, zonenbasierte Firewalls und strenge Zugriffslisten dienen dem Schutz des WAN über das öffentliche Internet. Durch das direkte Routing von Zweigstellenbenutzern zum Internet wird die Leistung von Public-Cloud-Anwendungen verbessert und der Datenverkehr über das WAN reduziert. Der Cisco Cloud Web Security (CWS)-Service bietet einen Cloud-basierten Webproxy zur zentralen Verwaltung und Sicherung des Benutzerdatenverkehrs, der auf das Internet zugreift. Technologien: Cisco IOS Firewall/IPS, Cloud Web Security (CWS)

Gründe für die Verwendung von DMVPN

Das IWAN basiert auf einem vorgegebenen Design mit einem Hybrid Transport Independent Design, das auf DMVPN basiert. DMVPN wird über MPLS und Internet-Transport bereitgestellt. Dies vereinfacht das Routing erheblich, indem eine einzige Routing-Domäne verwendet wird, die beide Transportnetze umfasst. Die DMVPN-Router verwenden Tunnelschnittstellen, die sowohl IP-Unicast- als auch IP-Multicast- und Broadcast-Datenverkehr unterstützen, einschließlich der Verwendung dynamischer Routing-Protokolle. Wenn der ursprüngliche Spoke-to-Hub-Tunnel aktiv ist, können dynamische Spoke-to-Spoke-Tunnel erstellt werden, wenn der standortübergreifende IP-Datenverkehr dies erfordert.

Das Transport Independent Design basiert auf einer DMVPN-Cloud pro Anbieter. In diesem Leitfaden werden zwei Anbieter verwendet: einer wird als primärer (MPLS) und einer als sekundärer (Internet) Anbieter. Zweigstellen sind mit beiden DMVPN-Clouds verbunden, und beide Tunnel sind in Betrieb.



Wie im Diagramm gezeigt, ist jeder Zweigstellen-Router mit beiden Anbietern verbunden, einer ist MPLS, der primär ist, und der andere ist INTERNET, das sekundär ist.

Je nach Art des Datenverkehrs wird der Datenverkehr von jedem Anbieter gesendet. So können beispielsweise Daten mit höherer Priorität über MPLS gesendet und Daten mit geringerer Priorität über das INTERNET weitergeleitet werden. Dadurch wird die Kosteneffizienz erhöht, und die verfügbaren Ressourcen können für innovativere Geschäftszwecke genutzt werden.

Transportunabhängiges Design (Dual DMVPN)

Zusammenfassung des Designs

Das Design bietet Aktiv-Aktiv-WAN-Pfade, die die Vorteile von DMVPN für konsistentes IPsec-Overlay voll ausschöpfen. Die MPLS- und Internetverbindungen können aus Gründen der Ausfallsicherheit auf einem einzelnen Router oder auf zwei separaten Routern terminiert werden. Das gleiche Design kann über MPLS-, Internet- oder 3G/4G-Transportnetze verwendet werden, wodurch das Design transportunabhängig ist.

Es wird empfohlen, einen DMVPN-Hub (PfRv3 BR) pro Anbieter und Transport auf dem Hub zu verwenden. Dies erleichtert die Routing-Konfiguration erheblich.

DMVPN erfordert die Verwendung von IKEv2 (Internet Key Management Protocol Version 2)-Keepalive-Intervallen für die Dead Peer Detection (DPD), was für eine schnelle Rekonvergenz und für die ordnungsgemäße Funktion der Spoke-Registrierung beim erneuten Laden eines DMVPN-Hubs unerlässlich ist. Mit diesem Design kann ein Spoke erkennen, dass ein Verschlüsselungs-Peer ausgefallen ist und dass die IKEv2-Sitzung mit diesem Peer veraltet ist. Dadurch kann eine neue Sitzung erstellt werden. Ohne DPD muss die IPsec-SA eine Zeitüberschreitung verursachen (der Standardwert beträgt 60 Minuten). Wenn der Router keine neue SA verhandeln kann, wird eine neue IKEv2-Sitzung initiiert. Die maximale Wartezeit beträgt ca. 60 Minuten.

DMVPN-Phase - Zusammenfassung

DMVPN umfasst mehrere Phasen, die hier zusammengefasst werden:

DMVPN Phase 1 basiert auf Hub-and-Spoke-Funktionen.

- Vereinfachte und kleinere Konfiguration an Hubs
- Unterstützung dynamisch adressierter CPEs (NAT)
- Unterstützung für Routing-Protokolle und Multicast
- Spokes benötigen keine vollständige Routing-Tabelle, können auf dem Hub zusammenfassen

DMVPN Phase 2 verfügt über keine Zusammenfassung auf dem Hub.

Jeder Spoke hat den Next-Hop (Spoke-Adresse) für jedes Spoke-Zielpräfix.

PfR verfügt über alle Informationen, um den Pfad mit dynamischem PBR und den richtigen Next-Hop-Informationen durchzusetzen.

DMVPN Phase3 ermöglicht die Routenzusammenfassung:

- Bei der Durchführung einer übergeordneten Routensuche ist nur die Route zum Hub verfügbar.
- NHRP installiert Shortcut-Tunnel dynamisch und füllt daher RIB/CEF aus.
- PfR verfügt weiterhin über die Hub-Next-Hop-Informationen und ist sich derzeit noch nicht über die Next-Hop-Änderung bewusst.

PfRv3 unterstützt alle DMVPN-Phasen.

Weitere Informationen zu DMVPN finden Sie unter Cisco IOS DMVPN Overview.