Introduzione a IWAN e PfRv3

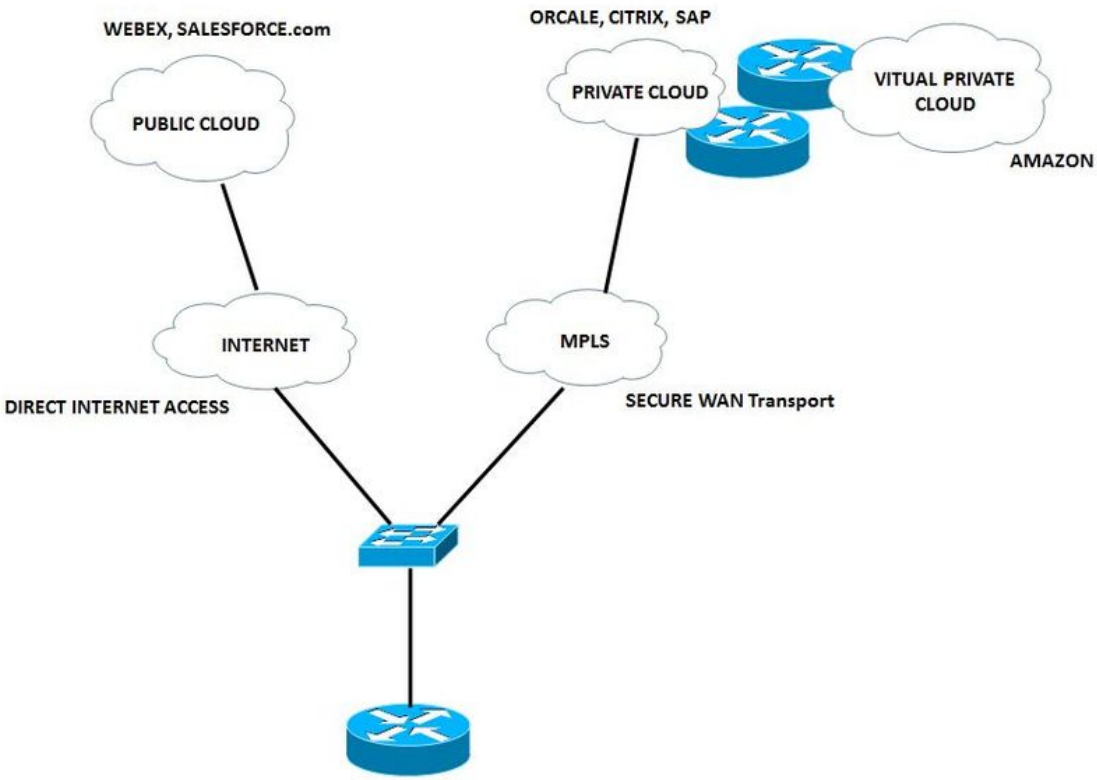
Sommario

Introduzione

Questo documento descrive Cisco Intelligent WAN (IWAN) e Cisco Performance Routing (PfR).

IWAN

Cisco IWAN è un sistema che migliora la collaborazione e le prestazioni delle applicazioni cloud, riducendo al contempo i costi operativi della WAN. La soluzione IWAN fornisce una guida alla progettazione e all'implementazione per le organizzazioni che intendono implementare una WAN indipendente dal trasporto con controllo intelligente dei percorsi, ottimizzazione delle applicazioni e connettività sicura a Internet e alle filiali, riducendo al contempo i costi operativi della WAN. La tecnologia IWAN sfrutta appieno i vantaggi della rete WAN avanzata e dei servizi Internet a costi contenuti per aumentare la capacità della larghezza di banda senza compromettere le prestazioni, l'affidabilità o la sicurezza delle applicazioni basate su cloud o di collaborazione. Le organizzazioni possono utilizzare la IWAN per sfruttare Internet come un trasporto WAN, nonché per l'accesso diretto alle applicazioni cloud pubbliche.



R1 preferirà il traffico voce e video per prendere il miglior percorso con un ritardo relativamente minore, jitter e/o perdita tra i due collegamenti disponibili. Il carico degli altri traffici è bilanciato in modo da massimizzare la larghezza di banda.

La voce e il video vengono reindirizzati se il percorso corrente si degrada (MPLS (Multiprotocol Label Switching)) e quindi viene scelto il collegamento Direct Internet Access (DIA).

La connessione IWAN consente di:

- Connessione a una modalità a basso costo come INTERNET per i dati meno importanti.
- Consente alla WAN di utilizzare l'ottimizzazione delle applicazioni, la memorizzazione intelligente nella cache e la DIA ad elevata sicurezza.

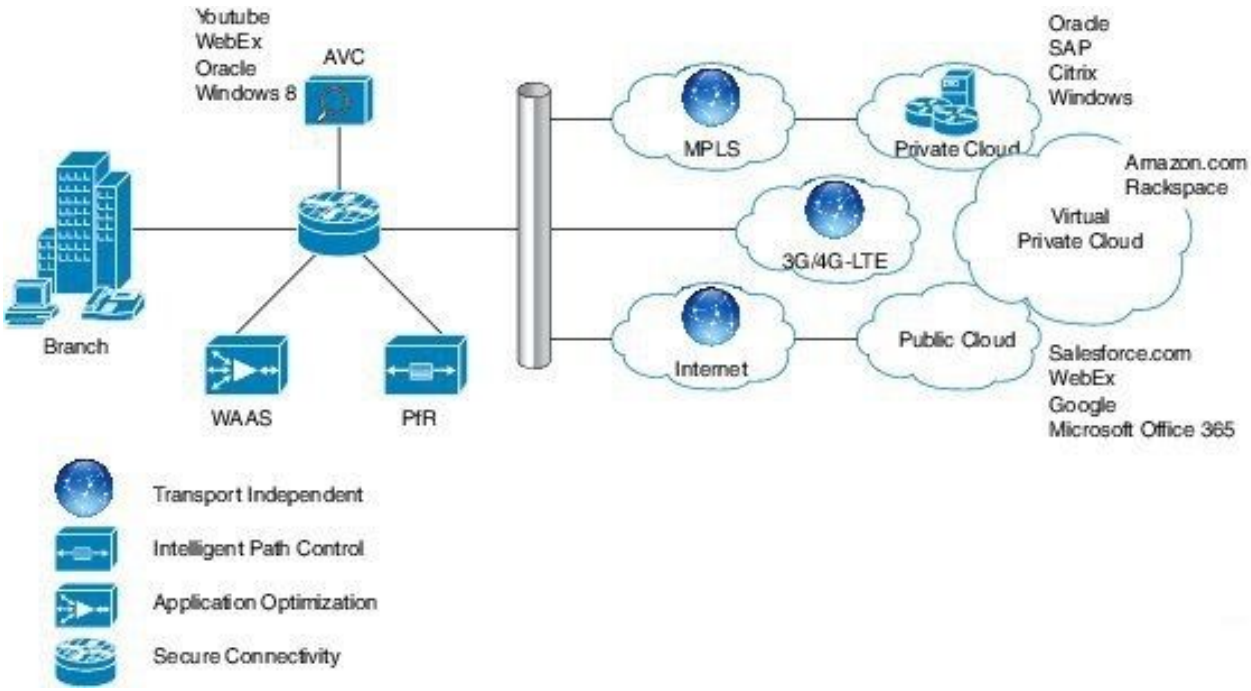
Finora, l'unico modo per ottenere una connettività affidabile con prestazioni prevedibili è sfruttare una WAN privata utilizzando MPLS o un servizio di linea in leasing. Tuttavia, i servizi MPLS basati su carrier e i servizi di linea in leasing possono essere costosi e non sempre convenienti per l'utilizzo da parte di un'organizzazione del trasporto WAN per supportare i crescenti requisiti di larghezza di banda per la connettività dei siti remoti. Le organizzazioni cercano modi per ridurre il budget operativo e al tempo stesso fornire il trasporto di rete per un sito remoto.

La tecnologia IWAN consente alle organizzazioni di offrire un'esperienza senza compromessi su qualsiasi connessione. Con Cisco IWAN, le organizzazioni IT possono fornire una maggiore larghezza di banda alle connessioni delle filiali con opzioni di trasporto WAN meno costose senza influire sulle prestazioni, sulla sicurezza o sull'affidabilità. Con la soluzione IWAN, il traffico viene instradato dinamicamente in base agli accordi sui livelli di servizio (SLA) delle applicazioni, al tipo di endpoint e alle condizioni di rete per offrire un'esperienza di qualità ottimale.

Con IWAN è possibile implementare rapidamente applicazioni a uso intensivo di larghezza di banda, quali video, VDI (Virtual Desktop Infrastructure) e servizi Wi-Fi guest. E non importa quale modello di trasporto preferisci, che sia MPLS, Internet, cellulare o un modello di accesso ibrido

alla WAN.

La figura mostra i componenti della soluzione IWAN. Performance Routing è un pilastro chiave di questa iniziativa:



I quattro componenti della IWAN sono:

- **Design indipendente dal trasporto sicuro e flessibile:** Dynamic Multipoint VPN (DMVPN) IWAN offre funzionalità per il multi-homing su qualsiasi offerta di servizi vettore, tra cui MPLS, banda larga e 3G/4G/LTE cellulare. Tecnologia: Progettazione overlay DMVPN/IPsec

- **Controllo intelligente dei percorsi:** con Cisco PfR, questo componente migliora la distribuzione delle applicazioni e l'efficienza della WAN. PfR controlla in modo dinamico le decisioni di inoltro dei pacchetti di dati analizzando il tipo di applicazione, le prestazioni, le regole e lo stato del percorso. PfR protegge le applicazioni aziendali dalle fluttuazioni delle prestazioni WAN e bilancia il carico in modo intelligente sul percorso con le migliori prestazioni in base alle regole dell'applicazione. PfR controlla le prestazioni di rete (instabilità, perdita di pacchetti, ritardo) e prende decisioni per inoltrare le applicazioni critiche sul percorso più efficiente in base alla policy dell'applicazione. Il PfR Cisco è costituito da router di confine che si connettono al servizio a banda larga e da un'applicazione controller primario supportata dal software Cisco IOS® su un router. I router di confine raccolgono le informazioni sul traffico e sul percorso e le inviano al controller primario, che rileva e applica i criteri dei servizi in base ai requisiti dell'applicazione. Cisco PfR può selezionare un percorso WAN in uscita per bilanciare in modo intelligente il carico del traffico in base ai costi del circuito e ridurre così le spese complessive di comunicazione di un'azienda. Il controllo intelligente dei percorsi IWAN è la chiave per fornire una WAN di classe aziendale su Internet. Tecnologia: PfR PfR si evolve in una nuova importante release chiamata PfRv3.

- **Ottimizzazione delle applicazioni:** Cisco Application Visibility and Control (AVC) e Cisco Wide Area Application Services (WAAS) offrono visibilità e ottimizzazione delle prestazioni delle applicazioni sulla WAN. Con le applicazioni che diventano sempre più opache a causa di un maggiore riutilizzo di porte conosciute come HTTP (porta 80), la classificazione delle porte

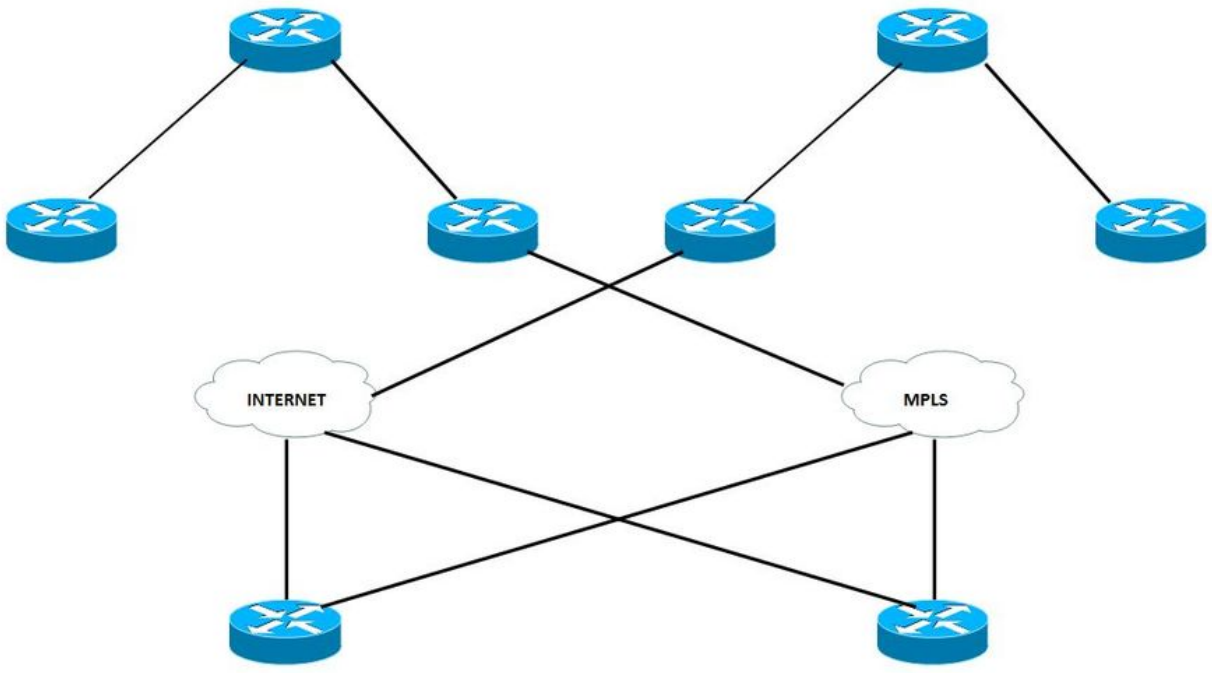
statiche dell'applicazione non è più sufficiente. Cisco AVC offre funzionalità di riconoscimento delle applicazioni con analisi approfondita del traffico dei pacchetti per identificare e monitorare le prestazioni delle applicazioni. Visibilità e controllo a livello di applicazione (livello 7) sono garantiti tramite tecnologie AVC quali NBAR2 (Network-Based Application Recognition 2), NetFlow, QoS (Quality of Service), monitoraggio delle prestazioni, Medianet e altro ancora. Tecnologie: Application Visibility and Control (AVC), WAAS, Akamai Connect

- **Connettività sicura:** protegge la WAN e scarica il traffico degli utenti direttamente su Internet. La crittografia IPsec avanzata, i firewall basati su zone e gli elenchi degli accessi rigidi vengono utilizzati per proteggere la WAN tramite Internet pubblica. Il routing diretto degli utenti delle filiali a Internet migliora le prestazioni delle applicazioni cloud pubbliche riducendo al contempo il traffico sulla WAN. Il servizio Cisco Cloud Web Security (CWS) fornisce un proxy Web basato su cloud per gestire a livello centrale e proteggere il traffico degli utenti che accedono a Internet. Tecnologie: Cisco IOS Firewall/IPS, Cloud Web Security (CWS)

Perché utilizzare DMVPN

IWAN utilizza un design prescrittivo con un design Hybrid Transport Independent basato su DMVPN. DMVPN viene implementata in MPLS e nel trasporto Internet. Ciò semplifica notevolmente il routing utilizzando un unico dominio di routing che comprende entrambi i trasporti. I router DMVPN utilizzano interfacce tunnel che supportano IP unicast, IP multicast e traffico broadcast, che includono l'uso di protocolli di routing dinamico. Dopo l'attivazione del tunnel spoke-to-hub iniziale, è possibile creare tunnel spoke dinamici quando i flussi di traffico IP da sito a sito lo richiedono.

La progettazione indipendente dal trasporto si basa su un cloud DMVPN per provider. In questa guida vengono utilizzati due provider, uno è considerato il provider primario (MPLS) e uno è considerato il provider secondario (Internet). I siti di succursale sono connessi a entrambi i cloud DMVPN ed entrambi i tunnel sono attivi.



Come mostrato nel diagramma, ogni router di succursale è connesso a entrambi i provider, uno è MPLS che è primario e l'altro è INTERNET che è secondario.

A seconda del tipo di traffico, ogni provider viene utilizzato per inviare il traffico. Ad esempio, i dati con priorità più alta possono essere inviati tramite MPLS e i dati con priorità inferiore possono essere instradati tramite INTERNET. In questo modo, la soluzione risulta più economica e le risorse disponibili possono essere utilizzate per scopi aziendali più innovativi.

Design indipendente dal trasporto (DMVPN doppia)

Riepilogo della progettazione

La progettazione fornisce percorsi WAN attivi-attivi che sfruttano al massimo DMVPN per una sovrapposizione IPsec coerente. Le connessioni MPLS e Internet possono essere terminate su un singolo router o su due router separati per una maggiore resilienza. Lo stesso design può essere utilizzato su MPLS, Internet o trasporti 3G/4G, rendendo il design indipendente dal trasporto.

Si consiglia di utilizzare un hub DMVPN (PfRv3 BR) per provider e trasporto sull'hub. Semplifica notevolmente la configurazione del routing.

DMVPN richiede l'uso degli intervalli keepalive IKEv2 (Internet Key Management Protocol versione 2) per Dead Peer Detection (DPD), che è essenziale per facilitare una rapida riconvergenza e per il corretto funzionamento della registrazione spoke in caso di ricaricamento di un hub DMVPN. Questa progettazione consente a uno spoke di rilevare che un peer di crittografia ha avuto esito negativo e che la sessione IKEv2 con tale peer è obsoleta, consentendo quindi la creazione di un nuovo peer. Senza DPD, l'associazione di protezione IPsec deve scadere (l'impostazione predefinita è 60 minuti) e quando il router non può rinegoziare una nuova associazione di protezione, viene avviata una nuova sessione IKEv2. Il tempo di attesa massimo è di circa 60 minuti.

Riepilogo fasi DMVPN

DMVPN dispone di più fasi che vengono riepilogate di seguito:

DMVPN Fase 1 si basa sulla funzionalità Hub e Spoke.

- Configurazione semplificata e ridotta sugli hub
- Supporto di CPE con indirizzo dinamico (NAT)
- Supporto per protocolli di routing e multicast
- I spoke non richiedono una tabella di routing completa, possono essere riepilogati sull'hub

DMVPN fase 2 non dispone di un riepilogo sull'hub.

Ogni spoke ha il prefisso di destinazione next-hop (indirizzo spoke).

PfR dispone di tutte le informazioni necessarie per applicare il percorso con PBR dinamico e le informazioni corrette dell'hop successivo.

DMVPN fase 3 consente il riepilogo delle route:

- Quando viene eseguita la ricerca della route padre, è disponibile solo la route verso l'hub.

- NHRP installa in modo dinamico il tunnel di collegamento e quindi popola RIB/CEF.
- PfR dispone ancora delle informazioni dell'hop successivo dell'hub e al momento non è a conoscenza della modifica dell'hop successivo.

PfRv3 supporta tutte le fasi DMVPN.

Per ulteriori informazioni su DMVPN, vedere Panoramica di Cisco IOS DMVPN.