POLITECNICO DI TORINO

Corso di Laurea
in Ingegneria Informatica

Tesi di Laurea Magistrale

Connettività multi-cloud su piattaforma SD-WAN

Relatore

prof. Fulvio Risso

Tutor aziendale Reply

ing. Enrico Maria Giraudo

Candidato

Gennaro Gaglione

Anno Accademico 2021-2022

“Noi siamo come nani sulle spalle di giganti,
così che possiamo vedere più cose di loro e più lontane,
non certo per l'acume della vista o l'altezza del nostro corpo,
ma perché siamo sollevati e portati in alto dalla statura dei giganti.”

Bernard de Chartres

Abstract

In seguito alla diffusione massiva di tecnologie di virtualizzazione e *cloud computing,* negli ultimi anni sempre più aziende scelgono di adottare soluzioni basate sul Cloud per le risorse e le infrastrutture IT di cui hanno bisogno. In tale contesto, le risorse IT aziendali vengono ospitate e gestite dai cloud service provider e fornite alle aziende tramite una connessione di rete, la quale diventa un elemento essenziale per collegare le risorse on premise con quelle sul cloud e assicurare la loro coesistenza grazie a un modello di "rete ibrida", da progettare secondo specifici requisiti, quali sicurezza, affidabilità, prestazioni, costo, scalabilità, flessibilità e time to market.

In letteratura si trovano diversi modelli di connettività al cloud e la scelta di uno di questi da parte di un'azienda dipende da un insieme di requisiti, di tipo sia economico sia ingegneristico, che vanno attentamente valutati al fine di trovare la soluzione migliore per ogni caso specifico. Tali modelli di connettività possono essere basati su rete Internet, su connessioni dedicate, oppure sfruttare un *Cloud Exchange*, cioè un'azienda che fornisce una connessione "as a service" verso più cloud service provider, garantendo grande flessibilità nella connessione verso differenti cloud provider o servizi SaaS da parte di un'azienda. Di fatto una soluzione basata sul Cloud Exchange fornisce sia sicurezza ed elevate prestazioni, tipiche di una connessione dedicata, sia flessibilità e scalabilità, come una soluzione basata su Internet.

Un'altra tecnologia recente che viene sempre più adottata è la Software Defined WAN (SD-WAN), una piattaforma per gestire l'infrastruttura WAN di una rete aziendale applicando i principi delle Software Defined Network (SDN). Con l'SD-WAN è possibile interconnettere diverse location quali sedi aziendali, datacenter privato, Cloud provider, delineando dunque un ulteriore modello di connettività oltre quelli già elencati, che offre notevoli vantaggi rispetto ad una rete WAN tradizionale, quali la gestione centralizzata della rete, la creazione di una rete *overlay* indipendente dalla rete di trasporto utilizzata, funzionalità di *path selection*. Inoltre, così come l'SD-WAN permette di costruire un'unica rete WAN virtuale, astraendo le diverse tecnologie di trasporto sottostanti (Internet, MPLS, 4G, etc.), allo stesso modo essa può creare una rete "virtuale" di interconnessione con i vari Cloud Service Provider in maniera del tutto trasparente.

L'obiettivo principale del lavoro di tesi è quello di realizzare un'architettura di rete SD-WAN che garantisca alta affidabilità, *fault tolerance* e prestazioni elevate a costi inferiori rispetto a una soluzione che si serva di un Cloud Exchange. In particolare, tale architettura dovrà garantire il supporto al multi-cloud, ovvero la possibilità di configurare l'SD-WAN su cloud provider diversi e ottenere quindi un ambiente multi-cloud di reti interconnesse tra di loro e gestibili tramite un'unica piattaforma.

A tale scopo si è deciso di utilizzare *flexiWAN,* uno dei prodotti SD-WAN presenti sul mercato, che si distingue per la sua natura open-source e la possibilità di integrare software di terze parti. L'installazione e il deployment dell'SD-WAN è stato realizzato sia su cloud AWS, sia poi su un altro cloud provider compatibile con flexiWAN (Alibaba Cloud) secondo le best practice di riferimento.

Relativamente al cloud provider Amazon AWS, dopo aver realizzato un deployment ad alta affidabilità dell'SD-WAN sul cloud AWS, ci siamo proposti di progettare un'automazione che, sfruttando i principali servizi AWS, permetta di ottenere un'architettura ad high availability, in cui il tempo di failover risulti inferiore ad un target prefissato.

Ci si aspetta, come punto di arrivo, che la soluzione basata su SD-WAN risulti effettivamente meno costosa rispetto ad utilizzare un Cloud Exchange, sia di facile installazione da parte di un'azienda che vuole adottarla, garantisca ridondanza e alta affidabilità, e infine abbia prestazioni (in termini di latenza e throughput) paragonabili a quelle del Cloud Exchange.

Indice

1 Introduzione

Negli ultimi anni sempre più aziende scelgono di adottare soluzioni basate sul Cloud per le risorse e le infrastrutture IT di cui hanno bisogno. Mentre nel passato era diffuso "ospitare" queste risorse all'interno di datacenter privati *on premise*, oggi invece, in seguito alla diffusione massiva di tecnologie di virtualizzazione e *cloud computing*, le risorse IT aziendali vengono ospitate e gestite dai cloud service provider e fornite alle aziende tramite una connessione di rete. La migrazione delle risorse IT verso il cloud può essere totale oppure solo parziale; nel secondo caso si parla di *hybrid cloud*, un ambiente in cui coesistono cloud privato (il datacenter aziendale) e Cloud pubblico. In entrambi i casi però, c'è bisogno di una connessione di rete per collegare le risorse on premise e quelle sul cloud, e assicurare quindi la loro coesistenza grazie a un modello di "rete ibrida" da progettare secondo specifici requisiti. Esistono infatti diversi modelli di connettività al cloud e la scelta dipende da un insieme di requisiti, di tipo sia economico sia ingegneristico, che vanno attentamente valutati al fine di trovare la soluzione migliore per ogni caso specifico. Questi requisiti posso essere raggruppati in varie categorie, a seconda che siano relativi a: vincoli temporali, sicurezza, affidabilità, prestazioni, costo, scalabilità, flessibilità, etc. Pertanto, dopo aver collezionato e analizzato i requisiti e conoscendo vantaggi e svantaggi dei vari modelli di connettività, un ingegnere di rete dovrà essere in grado di scegliere il modello migliore (o i modelli migliori, giacché potrebbe non esserci un unico modello ottimale). Nello specifico, i modelli di connettività possono essere basati su Internet, su connessioni dedicate, oppure sfruttare un Cloud Exchange; quest'ultima soluzione è certamente quella che offre più benefici, a patto però di dover affidarci ad un ulteriore provider (i.e. quello che fornisce l'infrastruttura del Cloud Exchange) oltre al comune Internet provider.

Raggiungere i diversi provider con la connessione a Internet già fornita dal proprio ISP è sicuramente possibile, ma con tutti i limiti che la Internet comporta in termini di sicurezza, prestazioni e affidabilità; a fronte di una grande flessibilità, che permette di collegarsi immediatamente ai vari cloud provider tramite Internet e quindi anche di trasferire facilmente i propri workload da un provider all'altro, utilizzare Internet come rete di trasporto fornisce un servizio "best effort" che raramente risponde ai requisiti di un'azienda che vuole disporre di applicazioni critiche da eseguire sul Cloud.

L'utilizzo di una *VPN over Internet* risolve il problema della sicurezza, grazie alla creazione di tunnel sicuri IPSec tra la rete on premise e le reti private sul Cloud, ma non gli altri due. La connessione VPN verso il Cloud può essere creata o tramite servizio gestito dal cloud provider (tutti i provider offrono un servizio di questo tipo, ad es. AWS Site-to-Site VPN), oppure tramite un router "virtuale" del *servizio cloud* che fa da terminatore del tunnel e può essere configurato e gestito liberamente.

Per ottenere il massimo dell'affidabilità e delle prestazioni è necessario ricorrere a collegamenti diretti (anche detti privati o *Private WAN)* verso uno specifico cloud provider. Questi possono essere sia di tipo hosted, e quindi condivisi con altri clienti, sia dedicati, e tipicamente forniscono una velocità molto elevata. Tuttavia questa soluzione comporta di solito un dispendio di tempo per l'installazione fisica iniziale, non è scalabile e diventa assai costosa nel caso in cui abbiamo bisogno di collegamenti dedicati con due o più cloud service provider diversi.

Una terza possibilità è rappresentata dall'utilizzo di un InterCloud Exchange, una soluzione che riesce a prendere "il meglio dei due mondi", poiché fornisce sicurezza ed elevate prestazioni, tipiche di una connessione dedicata, e allo stesso tempo è flessibile e scalabile, come una soluzione basata su Internet. Un InterCloud Exchange è un'azienda che fornisce una connessione diretta "as a service" verso più cloud service provider, garantendo grande flessibilità nella connessione verso differenti cloud provider o servizi SaaS da parte di un'azienda.

Un'altra tecnologia recente che viene sempre più adottata è la Software Defined WAN (SD-WAN), una piattaforma per gestire l'infrastruttura WAN di una rete aziendale applicando i principi delle Software Defined Network (SDN). Sebbene essa sia nata con l'obiettivo di interconnettere le diverse sedi aziendali tra di loro e/o con il datacenter privato, è possibile estendere la piattaforma SD-WAN per includere anche le risorse sul Cloud, quindi delineando un ulteriore modello di connettività, oltre quelli già presentati, che offre innumerevoli vantaggi rispetto ad una rete WAN tradizionale. I principali benefici di una piattaforma SD-WAN sono infatti la gestione centralizzata della rete on premise e del cloud, la creazione di una rete *overlay* indipendente dalla rete di trasporto utilizzata (Internet, MPLS, …), l'ottimizzazione della user experience grazie alla tecnica di *path selection* basata sulle policy e sul monitoraggio real-time dei collegamenti WAN, e le funzionalità avanzate di sicurezza.

Lo scopo principale di questa tesi è quello di realizzare una *proof of* concept ("prova di fattibilità") della tecnologia SD-WAN, concentrandosi in particolare su come estendere le funzionalità dell'SD-WAN non solo per permettere ad un'azienda di collegare il proprio datacenter on premise con le varie sedi e con il cloud (*hybrid cloud*), ma anche di usufruire dei servizi di più cloud service provider contemporaneamente (*multi-cloud environment*). Infatti, sempre più aziende hanno bisogno di utilizzare servizi offerti da cloud service provider diversi (es. AWS, Google Cloud Platform o Microsoft Azure), sia per poter usufruire di servizi specifici di un dato provider (approccio "best of breed"), sia per questioni economiche. I tre modelli di connettività prima accennati rappresentano lo "stato dell'arte" nell'ambito delle tecniche di interconnessione con il Cloud, con il modello dell'InterCloud Exchange che rappresenta senza dubbio quello con più benefici. Ciò che vogliamo dimostrare in questa tesi è la possibilità di adottare una quarta soluzione basata su una piattaforma SD-WAN che presenti all'incirca gli stessi vantaggi del Cloud Exchange, ma allo stesso tempo non obblighi a fare affidamento su un ulteriore provider per usufruire dei servizi Cloud (es. Equinix) e in più permetta di sfruttare tutti i vantaggi dell'SD-WAN anche nel collegamento con il Cloud: in sostanza ci proponiamo di mostrare che, così come l'SD-WAN permette di costruire un'unica rete WAN virtuale, astraendo le diverse tecnologie di trasporto sottostanti (Internet, MPLS, 4G, etc.), allo stesso modo essa può creare una rete "virtuale" di interconnessione con i vari Cloud Service Provider in maniera del tutto trasparente.

2 Connettività verso il Cloud con SD-WAN

La tesi si concentra sugli aspetti architetturali inerenti il deployment di una soluzione SD-WAN presente sul mercato e si propone di realizzare un'architettura di interconnessione SD-WAN che garantisca alta affidabilità, *fault tolerance* e buone prestazioni a costi inferiori rispetto a una soluzione che si serva di un Cloud Exchange.

In particolare, l'obiettivo della tesi è duplice. Per prima cosa, si vuole realizzare il deployment di una soluzione SD-WAN presente sul mercato, con particolare riferimento all'integrazione con il Cloud, sia con un singolo cloud provider sia multi-cloud; in quest'ultimo caso, l'obiettivo è quello di progettare una soluzione per interconnettere una singola organizzazione a diversi cloud provider (analogamente a ciò che accade affidandosi ad un servizio Cloud Exchange), basandosi sulla tecnologia SD-WAN. A tale scopo si è deciso di utilizzare *flexiWAN*, uno dei prodotti SD-WAN presenti sul mercato, che si distingue per la sua natura open-source e la possibilità di integrare software di terze parti.

L'installazione e il deployment dell'SD-WAN è stato realizzato sia su cloud AWS, sia poi su un altro cloud provider compatibile con flexiWAN (Alibaba Cloud) secondo le best practice di riferimento. Inoltre, relativamente al cloud provider Amazon AWS, dopo aver realizzato un deployment ad alta affidabilità dell'SD-WAN sul cloud AWS, ci proponiamo di progettare un'automazione che, sfruttando i servizi del Cloud (eventi, funzioni lambda, etc.), permetta di raggiungere un *failover time* inferiore a un certo target (es. un minuto).

3 Stato dell'arte

In questo capitolo andremo a trattare quello che si può definire lo "stato dell'arte" per le soluzioni di connettività verso il Cloud, cioè i modelli di connessione principali che sono stati usati fino ad ora. In particolare, vedremo come viene progettata la Wide Area Network di una rete enterprise per rendere possibile il collegamento tra le reti on premise di un'azienda (sedi aziendali e datacenter privato) e i vari cloud service provider. Ci limiteremo a considerare soltanto il cloud cosiddetto "pubblico", poiché il collegamento con il cloud "privato" (i.e., il datacenter on premise) non influenza la WAN in maniera sostanziale.

3.1 Accesso al Cloud tramite Internet

Utilizzare la Internet per accedere ai propri workload nel Cloud è certamente la soluzione più facile e meno costosa per un'azienda. Il primo vantaggio è rappresentato dall'**agilità**, giacché qualunque azienda è già connessa a Internet tramite un certo ISP, così come lo sono i vari Cloud Service Provider (CSP), quindi diventa davvero semplice cominciare a usare immediatamente i servizi del cloud.

Connesso all'agilità, un altro vantaggio è rappresentato dalla possibilità per un'azienda di spostare facilmente le proprie risorse da un cloud provider all'altro senza dover richiedere una connessione dedicata. Agilità e **facilità di migrazione** rendono questa soluzione altamente flessibile e dinamica, e permettono anche il **supporto al multi-cloud**, che è una caratteristica sempre più richiesta dalle aziende negli ultimi anni.

Tuttavia, usare l'infrastruttura Internet come rete di trasporto presenta sempre molti svantaggi. Innanzitutto, ricordiamo che la Internet fornice un servizio "*best effort*", quindi non viene fornito nessun meccanismo di *Quality of Service*, e ciò può condurre a una pessima *user experience*, a causa di una banda ridotta, un'elevata latenza e/o jitter, perdita di pacchetti, etc. Inoltre, utilizzare la Internet senza alcun tipo di cifratura del traffico a livello rete/applicazione, è la maniera meno sicura per accedere ai nostri workload nel cloud, giacché il traffico potrebbe essere intercettato e quindi letto/modificato/filtrato da eventuali attaccanti. Un altro aspetto importante da considerare, è l'enorme quantità di traffico che dovrà passare sul singolo collegamento Internet della rete enterprise, che potrebbe ben presto rivelarsi un collo di bottiglia per le prestazioni dell'intera rete. Infine si consideri pure che spesso un'azienda potrebbe aver bisogno di un *Service Level Agreement* per avere determinate garanzie sulle prestazioni e sull'affidabilità del collegamento con il Cloud (anche in caso di guasti), specialmente per i workload considerati critici, e un Internet provider tipicamente non lo fornisce, a differenza della maggior parte dei cloud provider (es. il servizio "AWS Direct Connect" oppure la piattaforma "Equinix").

3.2 Internet VPN

Volendo sempre usare Internet come rete di trasporto, una soluzione indubbiamente migliore, soprattutto dal punto di vista della sicurezza, è quella di collegarsi al Cloud con una VPN. Per esempio è possibile creare un tunnel IPSec tra la rete aziendale e il cloud provider, affinché tutto il traffico da/verso il Cloud sia cifrato e autenticato in transito. Configurare una VPN è assai veloce e supportato da praticamente tutti i router impiegati a livello enterprise, inoltre molti cloud provider già consentono di collegarsi alle proprie risorse sul cloud tramite VPN, sia come servizio gestito dal provider, sia facendo partire un proprio router, sotto forma di Virtual

Machine nella rete del provider, che faccia da terminatore del tunnel, che quindi può essere gestito e configurato dall'azienda, talvolta risparmiando sui costi.

3.2.1 Managed service vs. customer-managed VPN

Come abbiamo detto, quindi, ci sono due modalità di connettersi tramite una VPN alle proprie risorse sul Cloud. Nel caso di VPN gestita dal cloud provider, sarà il provider stesso a farsi carico di configurare la VPN lato cloud, mentre l'azienda dovrà configurare soltanto il proprio router. Nel caso invece di *customer-managed VPN*, l'azienda avrà un router "virtuale" lato cloud che potrà configurare come VPN gateway e gestire direttamente. Il secondo approccio sfrutta il concetto di Virtual Network Function, cioè quello di creare un'istanza "virtuale" di un dispositivo di rete reale (switch, router, …) o funzione di rete (es. NAT, firewall, load balancer) che viene eseguita come macchina virtuale all'interno della rete privata del customer nel Cloud (es. Amazon VPC); ciò permette non solo di risparmiare (rispetto a utilizzare il servizio gestito) ma anche di controllare e configurare liberamente il proprio dispositivo, a fronte però di un certo costo di gestione e manutenzione dei dispositivi di rete.

3.3 Private WAN (MPLS e Ethernet WAN)

Se si desidera una connessione al Cloud dedicata, privata, con alte prestazioni in termini di banda, throughput e latenza, allora si può ricorrere a una *Private WAN*. Le soluzioni tecnologiche principali appartenenti a questo gruppo sono rappresentate dalle *VPN over MPLS* e dalle *Ethernet WAN* (vedi appendice su **MetroEthernet**).

Il principale vantaggio di questa soluzione rispetto alle VPN è rappresentato dalla possibilità di applicare tecniche di *Quality of Service (QoS)* sulla Private WAN e di richiedere un *service-level agreement* (*SLA*) al cloud provider, quindi di ottenere una certa garanzia sulle prestazioni. Per quanto concerne la sicurezza, usare una Private WAN è considerato abbastanza sicuro e solitamente si accetta l'eventualità di non cifrare il traffico; tuttavia, se si vuole una maggiore sicurezza si può decidere di cifrare e autenticare comunque il traffico, instaurando una *VPN over Private WAN*, aggiungendo però un certo *overhead* dovuto alla cifratura e al tunneling.

Tra gli svantaggi, invece, c'è sicuramente il tempo di deployment più elevato (fino ad alcuni mesi nel caso di collegamenti dedicati, più breve per i collegamenti hosted), che potrebbe notevolmente ritardare i tempi richiesti ad un'azienda per migrare i suoi workload sul Cloud. Si consideri infine anche il caso in cui si voglia passare a un altro cloud provider, in cui si dovrà dismettere il collegamento corrente ed instaurarne un altro col nuovo provider, attendendo di nuovo tempi lunghi per l'installazione (a differenza delle soluzioni basate su Internet).

3.3.1 Esempio: il servizio AWS Direct Connect

AWS Direct Connect (abbreviato in **AWS DX**) è un servizio offerto da AWS che fornisce una connessione privata e dedicata dalle reti aziendali on-premise (e.g. branch office, datacenter aziendale, co-location environment, etc.) verso una regione AWS, bypassando l'internet service provider. In particolare, esso permette di collegare l'on premise ad una AWS DX Location in una regione specifica attraverso un normale cavo Ethernet in fibra ad alta velocità (da 1Gbps fino ad arrivare a 10/100Gbps in alcune DX Location).

Tale servizio rappresenta a tutti gli effetti un esempio di connettività al Cloud di tipo Private WAN che abbiamo definito prima, quindi per esso saranno valide tutte le considerazioni fatte circa i relativi benefici e svantaggi, che comunque andremo a riprendere e analizzare in questo

caso specifico. Infatti, AWS Direct Connect viene utilizzato principalmente in presenza di workload che a) sono considerati critici, b) hanno bisogno di banda elevata, o c) sono sensibili a latenza e jitter, e più in generale quando si ha bisogno di una connessione di rete più stabile, affidabile e sicura rispetto a quella di Internet, grazie alla caratteristica di DX di essere un collegamento dedicato.

3.3.1.1 Principali vantaggi

Quando si utilizzano collegamenti verso il Cloud basati su Internet, non si ha alcuna garanzia sulla effettiva banda fornita né sulla latenza, poiché per inoltrare il traffico da/verso i propri workload su AWS possono essere usati percorsi diversi in momenti diversi; con Direct Connect, invece, si può decidere quale traffico far passare sulla connessione dedicata e quest'ultimo sarà inoltrato verso la Regione AWS in cui si trova la destinazione nel minor tempo possibile.

Direct Connect fornisce originariamente una banda di 1 o 10 Gbps per una singola connessione (arrivando fino a 100 Gbps in alcune DX Location), ma è possibile creare un *Link Aggregation Group (LAG)* allo scopo di "aggregare" due o più connessioni fisiche in una sola connessione logica (quindi gestita singolarmente) per aumentare la banda disponibile. Notiamo che il servizio "AWS Managed VPN" può supportare fino a 1.25 Gbps per ogni VPN tunnel, pertanto esso dovrebbe essere evitato se si necessita di una velocità maggiore per accedere ai propri workload, perfino quando la VPN è utilizzata come connessione di backup per il collegamento DX principale.

Il metodo di *Link Aggregation* (secondo lo standard IEEE 802.3ad) permette di aggregare diversi link fisici in un singolo "channel", sia per aumentare la capacità del link in maniera incrementale, sia per migliorarne la resilienza in caso di guasto. Se ci sono più collegamenti dedicati dal router aziendale (*customer gateway)* verso una specifica DX Location per questioni di ridondanza, tutti con la stessa banda, allora è possibile creare un LAG per tali collegamenti e considerarli come se fossero un solo collegamento (logico), così da semplificarne la configurazione e la gestione.

Se un'azienda dispone di applicazioni sul Cloud che consumano molta banda sul collegamento Internet, allora Direct Connect può aiutare a ridurre i costi, giacché il traffico in ingresso e in uscita viene trasferito da/verso la rete AWS direttamente, senza dunque dover transitare per il proprio Internet provider (la qual cosa spesso costringe a dover richiedere un CIR più alto al proprio ISP e/o a pagare costi maggiori per la quantità di dati trasferiti).

Inoltre, Direct Connect è compatibile con tutti gli altri servizi di AWS, sia quelli privati (e.g. Amazon EC2, VPC, etc.) sia quelli pubblici (e.g. Amazon S3); in particolare, sfruttando opportunamente le *virtual interface (VIF) e le VLAN*, esso permette di accedere direttamente a più VPC distinte all'interno di una regione (utilizzando le VIF private), oppure ai servizi pubblici di AWS (tramite le VIF pubbliche). Pertanto, non solo Direct Connect offre una connessione stabile, a elevata banda e a ridotta latenza, ma fornisce anche un collegamento sicuro verso diverse VPC sul Cloud, assicurando *network segmentation* e *isolation* nell'accesso alle varie VPC.

3.3.1.2 Ottenere elevata resilienza per i workload critici

Ottenere elevata resilienza nella connettività di rete verso il Cloud è fondamentale per avere un'architettura di interconnessione al Cloud ben progettata; di seguito riportiamo alcune *best practice* da seguire per ottenere questo obiettivo.

Per prima cosa, è consigliato avere più reti on premise, fisicamente separate, che sono collegate ad AWS attraverso altrettante DX Location separate tra loro, così da garantire un buon grado di resilienza non solo in seguito a guasti sui singoli device, ma anche a guasti che compromettano l'intera DX Location.

In secondo luogo, si suggerisce di avere dispositivi di rete e *telco provider* ridondanti, ad es. customer gateway diversi connessi ad altrettanti DX router all'interno di ciascuna DX Location (vedi Figura 3-1). Inoltre, è importante utilizzare il routing dinamico (il protocollo eBGP in questo caso) per ottenere un comportamento di *load balancing/failover* tra le varie connessioni ridondanti.

Infine, bisognerebbe evitare di utilizzare una "AWS managed VPN" come collegamento di backup di una connessione DX principale con una banda maggiore di 1Gbps, e più in generale bisognerebbe fornire banda di rete sufficiente a garantire che un guasto su un collegamento di rete principale non "stressi" eccessivamente i collegamenti ridondanti.

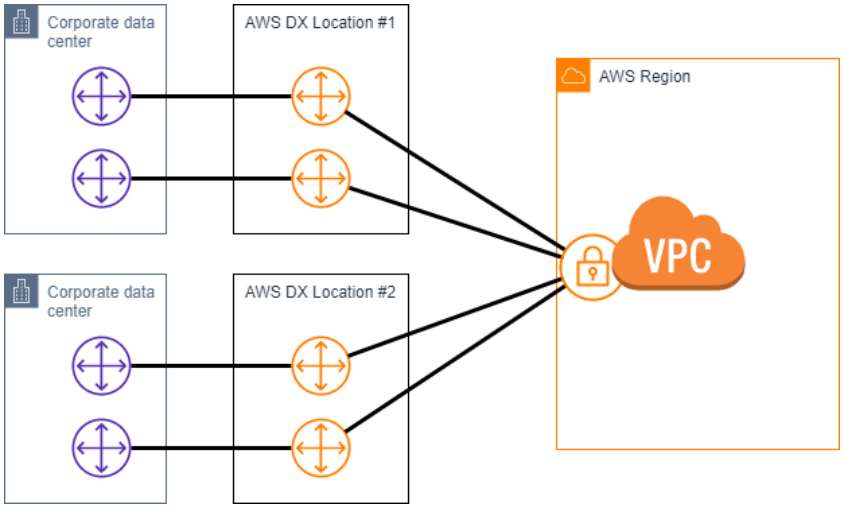


Figura 3-1 Configurazione High Resilience per workload critici.

3.4 Inter-Cloud Exchange

Una soluzione che garantisce tutti i vantaggi di una Private WAN, ma allo stesso tempo rende estremamente semplice la migrazione verso un altro cloud provider, è rappresentata dal *Cloud Exchange*, che in sostanza è un'altra azienda (distinta dall'ISP e dal cloud provider) che fornisce un servizio di connettività privata *as a service*, con tutta la flessibilità che ne consegue.

L'infrastruttura di rete di un Cloud Exchange è connessa da un lato ai maggiori cloud provider (Amazon AWS, Microsoft Azure, etc.) e dall'altro è collegata ai suoi customer, che desiderano usufruire di una connessione privata verso il Cloud pubblico in maniera flessibile. Una volta che un'azienda si è collegata al Cloud Exchange (tipicamente collegando direttamente il proprio router con quello del Cloud Exchange all'interno di uno dei *Point of Presence* di quest'ultimo), può decidere dinamicamente di farsi connettere a un cloud provider piuttosto che ad un altro, tramite la richiesta di creazione di circuiti virtuali (vedi *MetroEthernet*); se in futuro l'azienda vorrà cambiare provider di servizi cloud, il collegamento verso l'Exchange non andrà modificato in alcun modo, ma si dovrà solamente chiedere all'Exchange la creazione di un nuovo circuito virtuale verso il cloud provider desiderato.

Per concludere, con un Cloud Exchange si hanno tutti i vantaggi delle Private WAN ma con in più un altro grado di flessibilità (come con le soluzioni che usano Internet). L'unico svantaggio è quello di doversi affidare ad un altro provider per l'Exchange, oltre a i già citati ISP e cloud provider, il che introduce dei costi ulteriori per le aziende.

3.5 Piattaforma SD-WAN integrata con il Cloud

Dal momento che la connettività a Internet è ormai diventata "commodity" per le aziende e la banda disponibile è sempre più elevata, queste spesso decidono, invece di mettere in piedi e mantenere una rete WAN separata, di costruire una rete WAN virtuale "al di sopra" della Internet, chiamata *Software-Defined WAN* (SD-WAN). Una piattaforma SD-WAN permette alle aziende di costruirsi in maniera flessibile la rete WAN e di gestirla in modo centralizzato, attraverso meccanismi software assai intelligenti. In pratica l'SD-WAN rappresenta una estensione delle customer-managed VPN e quindi varranno per essa tutte le considerazioni fatte in precedenza.

La tecnologia SD-WAN è nata inizialmente con lo scopo di interconnettere le sedi secondarie di una azienda con la sede principale e con il datacenter on premise, ma è possibile estenderla naturalmente per includere le risorse e le reti sul Cloud pubblico.

I vantaggi derivanti dall'utilizzo di una piattaforma SD-WAN sono notevoli e, se questa viene opportunamente integrata con il Cloud, tali vantaggi varranno anche per l'accesso ai servizi del cloud provider. Tra le funzionalità più importanti vi sono:

- meccanismi di automazione della configurazione dei dispositivi, che rendono più facile l'installazione iniziale e il monitoraggio;
- controllo centralizzato della WAN e del Cloud attraverso un singolo management pane;
- meccanismi automatici di *failover* del percorso in caso di guasto;
- *application-based routing*;
- funzionalità avanzate di sicurezza.

Gli svantaggi invece consistono nell'overhead dovuto al tunneling e alla cifratura, e nel fatto che l'affidabilità di questa soluzione dipende strettamente dalla rete di trasporto sottostante, che nel caso di Internet non dà alcuna garanzia; per ovviare a questo problema, si potrebbe utilizzare l'SD-WAN al di sopra di una Private WAN. In effetti la caratteristica dell'SD-WAN cui si fa affidamento in questi casi è la possibilità di utilizzare più reti di trasporto sottostanti come fossero un'unica rete WAN virtuale, scegliendo quale tipo di traffico far passare sulla Internet e quale invece far viaggiare sulla rete di trasporto più affidabile (es. MPLS per i workload critici che richiedono prestazioni garantite e/o affidabilità).

3.6 Scelta del modello di connettività al Cloud

In questo paragrafo andremo ad approfondire il processo decisionale che, date le specifiche su 1) tempo di deployment, 2) prestazioni, 3) SLA, 4) costo e 5) sicurezza, permette di scegliere la soluzione migliore per un'azienda che richiede la connettività al Cloud. Dopo aver definito i vari parametri da tenere in considerazione nella nostra analisi, e aver evidenziato il relativo peso sulle scelte progettuali, discuteremo le diverse soluzioni tecniche disponibili in base ai requisiti specifici dell'azienda.

3.6.1 Tempo di deployment

Il primo parametro di cui tener conto nel processo di scelta è sicuramente quello temporale. È importante definire *sia* qual è il tempo massimo entro cui la connessione deve essere stabilita (*provisioning time) sia* per quanto tempo la connessione sarà utilizzata (es. alcune settimane nel caso di un ambiente di testing/development, oppure diversi mesi/anni in un ambiente di produzione).

In base al provisioning time si potrà decidere se utilizzare dei collegamenti già esistenti (tramite connessioni dette *hosted,* cioè messe a disposizione da un WAN provider e condivise da più customer contemporaneamente) oppure richiedere delle connessioni dedicate al cloud provider (oppure al Cloud Exchange) che soddisfino i requisiti specifici dell'azienda. A seconda invece che la connettività richiesta sia temporanea oppure no, si potrà decidere di utilizzare la connessione già esistente verso Internet (con una "Site-to-Site VPN") oppure di ricorrere a connessioni private (sia hosted sia dedicate).

Concentriamoci adesso sul provisioning time e andiamo ad analizzare le varie soluzioni tecniche disponibili a seconda del valore stimato di questo parametro. Se il tempo a disposizione per mettere in piedi il collegamento consiste in alcune ore o giorni, allora si deciderà probabilmente di utilizzare il link verso Internet già esistente, su cui si instaurerà una connessione VPN verso il Cloud. Se invece abbiamo a disposizione poche settimane, possiamo pensare di affidarci ad un Cloud Exchange per usufruire di una hosted connection, che tipicamente viene fornita molto più velocemente di una connessione dedicata; questo perché il Cloud Exchange sfrutta la sua infrastruttura fisica già esistente verso il cloud provider considerato, e fornirà a ciascuna azienda una connessione *hosted* attraverso un link fisico verso il cloud provider che è condiviso tra i vari customer (utilizzando la tecnologia delle VLAN).

Se il requisito sul provisioning time è di diverse settimane o mesi, allora conviene stabilire una connessione dedicata direttamente con il cloud provider. Ciò richiede di connettere il proprio router con quello del cloud provider, o nella propria rete on premise oppure, più di frequente, in delle "location" di connettività dedicata (es. AWS Direct Connect Location). Esiste anche un caso particolare di quest'ultimo, quello cioè in cui si hanno già i propri router all'interno di una *colocation facility* che ospita anche una Location di connettività dedicata del cloud provider cui ci si vuole collegare; in questo caso, è possibile collegare il proprio router a quello del provider ed usufruire di una connessione dedicata in pochi giorni.

3.6.2 Prestazioni

Un secondo parametro importante è certamente quello delle prestazioni che, nel nostro caso, si riferisce alle prestazioni della connessione di rete che permette il transito del traffico tra la rete on premise e il Cloud. Tipicamente, i parametri che caratterizzano la bontà di una connessione di rete sono la larghezza di banda (*bandwidth)*, il *throughput*, il numero di flussi di traffico e la latenza.

La **larghezza di banda** indica la massima velocità di trasferimento dei dati di una connessione, ed è indipendente dall'applicazione che genera il traffico. Il **throughput** invece, è un parametro strettamente connesso all'applicazione, e indica il tasso di trasmissione che un'applicazione riesce effettivamente a raggiungere; di solito, infatti, un'applicazione non può sfruttare tutta la banda che ha a disposizione, per esempio perché ci sono degli overhead dovuti al tunneling e/o alla cifratura del traffico. Un **flusso di traffico** rappresenta una singola connessione tra due

endpoint ed è anche detta *5-tuple* perché viene univocamente definita dalla quintupla **(IP_src, IP_dst, port_src, port_dst, protocol)**. Infine la **latenza** indica il tempo impiegato da un pacchetto per raggiungere la destinazione e tornare indietro al mittente (anche detto *Round Trip Time, RTT)*.

Nell'andare a definire i requisiti richiesti da un'azienda per collegare la rete on premise al Cloud e utilizzare al meglio le proprie applicazioni, un ingegnere di rete dovrà porsi una serie di domande ben specifiche e comprendere a fondo i requisiti dell'azienda. Innanzitutto, dovrà capire quali sono i parametri critici (tra quelli appena elencati) richiesti dalle applicazioni "fruite" attraverso il Cloud.

Se le applicazioni richiedono prestazioni deterministiche sulla latenza o sullo jitter (es. applicazioni VoIP) per garantire una adeguata *user experience*, allora bisogna optare per una connessione diretta (dedicata oppure hosted). Dopodiché si passa ad analizzare il requisito sul throughput, da cui segue necessariamente la larghezza di banda. Se è richiesta un'elevata banda (maggiore di 1 Gbps), allora si deve ricorrere ad una connessione dedicata col cloud provider; per una banda ancora più alta si può ricorre a tecnologie come la Link Aggregation (per "aggregare" due o più link fisici in un solo collegamento logico) oppure *l'Equal Cost Multipath Routing* (per inviare il traffico su più connessioni contemporaneamente).

Un'alternativa potrebbe essere utilizzare una Site-to-Site VPN, considerando che sempre più aziende dispongono di connessioni a banda larga verso Internet. Si ricordi però che Internet fornisce sempre un servizio "best effort" e che quindi è soggetta ad eventi aleatori, congestione e periodi di elevata latenza. Per mitigare questi effetti alcuni cloud provider forniscono un servizio di connettività VPN detto *accelerated,* che in sostanza fa sì che il traffico passi sul backbone del provider il prima possibile e quindi riduce il numero di eventi aleatori a cui è soggetto il traffico rispetto a quando esso viaggia interamente sulla Internet pubblica.

3.6.3 Service Level Agreement (SLA)

Quando un'azienda (customer) usufruisce di un certo servizio fornito da un provider, tipicamente le due parti stabiliscono un accordo (detto *Service Level Agreement, SLA*) che specifica entro quali termini il servizio verrà fornito e reso operativo, spesso attraverso parametri definiti e misurabili come l'*uptime target* e la *availability*; nel caso in cui tali termini siano violati, il service provider dovrà provvedere a fornire un compenso economico all'azienda (*service credits)*, anch'esso già stabilito nell'accordo.

Il requisito sull'SLA può rivelarsi spesso quello dirimente, cioè quello che porta necessariamente a scegliere una soluzione piuttosto che un'altra. Infatti se un'azienda ha l'esigenza di accedere in qualunque momento a determinate risorse sul Cloud, e la connettività non fosse disponibile per un certo periodo di tempo, ciò rappresenterebbe un problema (con possibili impatti economici) e quindi si dovrebbe optare per soluzioni con un SLA specifico sulla availability (cioè il grado di resilienza garantito dall'interconnessione di rete). Tipicamente non tutte le risorse sul Cloud richiedono un SLA: per esempio, le risorse per applicazioni in fase di testing o sviluppo non lo richiedono per ovvi motivi, laddove quelle relative ad applicazioni in produzione lo richiederanno con alta probabilità; in casi come questo, si possono utilizzare due o più soluzioni di collegamento al Cloud contemporaneamente, di cui una viene utilizzata come connessione principale e l'altra come collegamento di backup in caso di guasti.

Se si utilizza una connessione tramite Internet, allora non potrà essere fornito alcun SLA dal cloud provider, perché quest'ultimo non avrà alcun controllo sul percorso del traffico una volta che questo "esce" dalla sua rete. Se invece si utilizza una connessione dedicata (oppure hosted) verso il cloud, oppure si passa per un Cloud Exchange, allora potrà essere stipulato un SLA tra l'azienda e il cloud provider. Si noti tuttavia che, se si fa affidamento ad un Cloud Exchange, la connettività sarà soggetta eventualmente ad un SLA con quest'ultimo, e non col cloud provider finale.

Tutti i cloud provider forniscono dei servizi di connettività dedicata con SLA (es. "AWS Direct Connect" di Amazon o "Azure ExpressRoute" di Microsoft). Tuttavia, a seconda per esempio dell'uptime richiesto (99.99%, 99.9%, etc.) il cloud provider specifica i requisiti minimi che il customer deve soddisfare per far valere l'SLA (in termini di ridondanza dei router, dei collegamenti e delle location), e per ottenere una connettività al cloud con diversi gradi di resilienza a seconda delle sue esigenze.

3.6.4 Costo

Il costo di un'infrastruttura di rete per la connettività al Cloud consta principalmente di due componenti: il costo delle risorse fornite dal cloud provider, che si misura in unità temporali (i.e. costo all'ora), e il costo di utilizzo di tali risorse, che si misura in base alla quantità di dati trasferiti (in Gigabyte). Un altro costo da considerare è quello per collegare il proprio router aziendale al *Point of Presence (PoP)* del cloud provider: questo costo sarà ridotto nel caso in cui il proprio router e quello del cloud provider si trovino già nella stessa *colocation facility*, mentre potrebbe essere più alto se bisogna passare per la rete di un altro service provider (i.e. un Partner del CSP oppure un Cloud Exchange).

Chi progetta la connessione al Cloud tipicamente cerca di soddisfare tutti i requisiti dell'azienda minimizzando i costi; se ciò può andar bene inizialmente, quando poi i requisiti cambiano e diventano più stringenti, allora potrebbe risultare molto difficile e costoso far scalare la soluzione che si era scelto di adottare in un primo momento. Infatti, quando ci sono richieste di prestazioni molto elevate (per es. in termini di banda), utilizzare connessioni dirette può risultare addirittura più economico che utilizzare soluzioni Internet-based. Supponendo di avere dei workload che richiedono una banda elevata, che vogliamo eseguire sul Cloud, utilizzare una connessione diretta può risultare più economico: infatti, passare direttamente per il CSP permette di lasciare invariata la banda precedentemente concordata con l'internet provider (detta *committed information rate, CIR)*; inoltre, il costo per i dati trasferiti direttamente al cloud provider è solitamente inferiore di quello richiesto dall'ISP.

Notiamo infine che la maggior parte dei cloud provider applica un costo soltanto al traffico *in uscita* dalla sua rete, non a quello in ingresso; pertanto, uno sviluppatore cloud dovrebbe progettare le applicazioni in modo tale che la maggior parte dell'elaborazione avvenga all'interno del Cloud, quindi minimizzando il trasferimento di dati dalla rete del cloud verso l'on premise.

Se si ha bisogno di una connessione permanente oppure il volume di dati da trasferire è molto elevato, allora conviene affidarsi ad una connessione diretta. In particolare, ci si può collegare direttamente al cloud provider con una connessione dedicata, il che permette di avere una banda fissa di 1 Gbps o superiore, oppure si può usare una connessione hosted se si desidera maggiore granularità di banda (es. 50 o 100 Mbps invece di 1 Gbps) e risparmiare sui costi. Se invece la connettività al cloud di cui si necessita è solo temporanea, e le caratteristiche di una connessione

Internet sono adeguate ai requisiti richiesti, allora si può utilizzare una Site-to-Site VPN su Internet. Un altro approccio consiste nel combinare le due soluzioni di connettività, utilizzando la connessione diretta come collegamento principale e la VPN su Internet come collegamento di backup in caso di guasto.

Infine, un'altra soluzione è quella di utilizzare una VPN customer-managed oppure una piattaforma SD-WAN terminate su una o più macchine virtuali nel Cloud controllate direttamente dal customer (l'azienda in questione); quest'approccio può essere più economico rispetto ad una VPN gestita dal provider (soprattutto se si ha bisogno di tanti tunnel con una banda ridotta), tuttavia esso richiede i costi di gestione delle *virtual appliance* e il costo delle risorse (i.e. macchine virtuali) utilizzate sul Cloud.

3.6.5 Sicurezza

Il requisito di sicurezza prende in considerazione due aspetti: il tipo di trasporto utilizzato per accedere al Cloud (Internet vs. connessione diretta) e la cifratura del traffico *in-transit*, che può essere fornita sia a livello di rete (con le VPN) sia a livello applicativo (con TLS).

Se si decide di usare Internet come trasporto, allora una Site-to-Site VPN permette di creare dei tunnel cifrati (con IPSec) tra la rete on premise e le reti private sul Cloud, fornendo quindi la cifratura del traffico in-transit al livello di rete. Le stesse considerazioni valgono anche per le VPN customer-managed e per la SD-WAN.

Se invece c'è la necessità di usare una connessione diretta (ad es. perché si vogliono valori deterministici per latenza e jitter oppure una banda elevata) allora si può optare per una connessione dedicata oppure hosted che, benché ritenute di per sé moderatamente sicure, potrebbero comunque essere soggette a numerosi attacchi, poiché il traffico viaggia comunque in chiaro su un'infrastruttura che potrebbe essere condivisa (come nel caso di hosted connection). Se si vuole anche cifrare il traffico in transito, allora è possibile implementare una Site-to-Site VPN che viaggia su una connessione diretta, soluzione che fornisce la massima sicurezza e prestazioni garantite.

3.6.6 Riepilogo

Dunque si è visto che nella scelta della soluzione di connettività al Cloud migliore, per un dato insieme di requisiti, esistono diversi *driver* che vanno considerati e bilanciati per arrivare a un trade-off e selezionare la soluzione migliore.

Un ingegnere di rete o del Cloud dovrà dapprima chiedersi se è accettabile mettere in piedi una connessione che viaggi su Internet; in caso negativo, si dovrà subito virare verso le soluzioni di connettività diretta: una connessione hosted se il tempo di deployment a disposizione è limitato (alcune settimane), oppure una connessione dedicata se c'è bisogno di una banda elevata (> 1 Gbps).

Se, al contrario, usare Internet come rete di trasporto è ritenuto accettabile (es. il link verso Internet ha una capacità elevata e le applicazioni cui si accede sul Cloud non richiedono prestazioni garantite), si passa ad analizzare il requisito sull'SLA; infatti, se ad esempio è richiesto un SLA sulla *availability* (nel caso di workload critici per l'azienda), allora la scelta dovrà ricadere di nuovo sulle soluzioni di connettività diretta e varranno ancora le considerazioni fatte prima.

Laddove non vi sia il requisito sull'SLA, allora si passa a valutare se vi è necessità di avere prestazioni garantite (i.e. deterministiche) su latenza, jitter, packet loss, …, e in caso positivo si ricadrà ancora una volta sulle soluzioni di connessione diretta col cloud provider, perché sono le uniche a poter garantire SLA e performance deterministiche, mentre la Internet pubblica fornisce come al solito un servizio "best effort".

Quando vengono meno i requisiti su SLA e performance deterministiche e si ha un tempo di deployment molto limitato (alcuni giorni), allora si può virare verso le soluzioni basate su Internet (Site-to-Site VPN o customer-managed VPN), che però garantiscono una banda di 1 Gbps al massimo per ogni connessione; per velocità più elevate conviene ricorrere ancora una volta alle connessioni dirette, soprattutto quelle dedicate.

In Figura 3-2 è riportata una tabella comparativa che mette a confronto i modelli di connettività al Cloud descritti in questo capitolo, rispetto ai principali driver e funzionalità da considerare nella scelta della soluzione migliore per una certa azienda.

	Internet	Internet VPN	Private WAN (MPLS VPN, Ethernet WAN)	Intercloud Exchange	SD-WAN
Security in-transit	No	Yes if using secure VPN protocols (i.e. IPSec or TLS)	Traffic is not encrypted	Traffic is not encrypted	Yes, with IPsec
Advanced security services	No	Partial (if using L7 fw)	No	No	Yes
QoS (packet loss, delay, jitter)	No (best effort)	No (traffic traverses the Internet)	Yes (leased line)	Yes	Yes
Agility (in migrating to another CSP)	Yes	Yes	No	Yes	Yes
Time to deploy	Nearly zero	Low	High	High	Low to medium
Cost	Very low	Medium	High	Medium	Medium
Bandwidth	Variable	Limited	High	High	High
Availability	Depends on ISP	Depends on ISP	Only if a backup connection exist	High	High
Multipath routing	No	No	No	Only a few providers (Equinix)	Yes
Traffic segmentation	No	No	Yes with VRF and 802.1Q VLANs	Yes with VRF and 802.1Q VLANs	Yes, with VPNs

Figura 3-2 Tabella comparativa dei modelli di connettività al Cloud

4 Confronto di soluzioni SD-WAN

In questo capitolo andremo a presentare le funzionalità di alcuni dei più importanti *vendor* SD-WAN presenti sul mercato, con particolare riferimento all'integrazione con il Cloud; ciascun prodotto SD-WAN sarà analizzato secondo un quadro ben preciso di requisiti (es. supporto alla configurazione multi-AZ, high availability, performance, etc.) e sarà fornita un'architettura di riferimento.

Questa stessa metodologia di benchmark sarà utilizzata poi nel capitolo successivo per progettare e realizzare un deployment di **flexiWAN**, una soluzione SD-WAN presente sul mercato che si differenzia dalle altre per l'utilizzo di software open source e per la possibilità di integrare prodotti di terze parti, laddove la maggior parte delle SD-WAN propongono soluzioni *all-in-one* fortemente limitate ai prodotti dello specifico vendor.

4.1 Requisiti di una soluzione SD-WAN

I requisiti che si vogliono analizzare consistono principalmente in quelli di tipo prestazionale (es. throughput dell'SDWAN) e quelli di *availability* (tempi di convergenza e di failover tra le istanze SDWAN). In particolare considereremo:

- La **facilità di installazione** della soluzione SDWAN e di creazione delle VPN. Ciò è importante, infatti, per ridurre il tempo necessario ad un'azienda per migrare ad una soluzione SDWAN.
- Il **supporto a più Availability Zone (AZ)**, infatti nel Cloud è una best practice avere più AZs separate.
- La soluzione deve supportare una **configurazione ad "high availability"**. Bisogna misurare i **tempi di convergenza** e **failover**, sia per il traffico tra le reti on premise e il Cloud, sia per il traffico tra le istanze SDWAN all'interno del Cloud, sia infine per quello tra due istanze poste in due cloud provider diversi (supporto al multi-cloud). Infatti l'availability è un requisito di importanza critica per il business e per le sfide aziendali, soprattutto negli ambienti IT moderni con risorse fortemente distribuite.
- Le prestazioni in termini di **latenza** e **throughput**. Avere reti performanti è fondamentale per le aziende moderne, dove ogni aspetto è fortemente influenzato dalla bontà dell'infrastruttura di rete, soprattutto in un contesto dove gli utenti accedono alle applicazioni da luoghi diversi e con dispositivi differenti.
- Le caratteristiche di **management** e **monitoring** del sistema SDWAN. Questo aspetto è molto importante giacché gli ambienti IT odierni richiedono la capacità di monitorare e gestire efficacemente le risorse e i servizi in risposta alle richieste del business. Per tale motivo, le aziende hanno bisogno di strumenti flessibili e facili da usare per monitorare e gestire agilmente sia le risorse on premise sia quelle in Cloud.

4.2 Aviatrix Cloud Interconnect

Aviatrix Cloud Interconnect è una soluzione SDWAN pensata per interconnettere tutte le sedi di una azienda, sia i singoli branch on premise, sia il datacenter, sia le reti sul Cloud (es. Amazon VPCs). Infatti la soluzione permette di collegare fra di loro tutte le reti attraverso dei tunnel IPSec cifrati, utilizzando una topologia *mesh* oppure *hub-and-spoke*, in modo semplice e centralizzato.

I due componenti principali di questa soluzione sono **l'Aviatrix Cloud Controller (ACC)** e **l'Aviatrix Gateway (AGW)**, come si vede dalla Figura 4-1, in cui in particolare viene mostrata l'integrazione di Aviatrix con uno dei principali cloud service provider (Amazon AWS). Una volta fatto il deployment del controller all'interno di una VPC pubblica (i.e. abilitata al traffico in uscita verso Internet), l'utente dell'SDWAN può predisporre i vari AGWs tramite il controller stesso, andando a posizionarli nelle reti on premise e nelle VPC private che intente collegare. Non appena i vari gateway saranno visibili dal controller, l'utente potrà, tramite una dashboard, selezionare le *location* che vuole connettere con dei tunnel IPSec. Per garantire l'high availability verso il Cloud, l'utente può creare una coppia di tunnel ridondati dall'AGW di ciascun sito on premise verso i due AGWs impiegati sul Cloud, in una tipica configurazione multi-AZ (come mostrato in figura).

Infine questa soluzione prevede anche la possibilità di connettere utenti remoti al Cloud passando solamente per il controller: a tale scopo, il gestore dell'SDWAN dovrà aggiungere i loro profili su un AGW nel Cloud e i singoli utenti dovranno avere installato un applicativo client VPN; dopo che i profili saranno verificati tramite certificato, gli utenti verranno connessi all'AGW tramite il controller e potranno quindi accedere al Cloud. Pertanto, il meccanismo centralizzato di instaurazione di VPN (in modo molto semplice, tramite una dashboard) vale non solo per collegare branch diversi ma anche per far connettere singoli utenti al Cloud in modo sicuro.

Infine Aviatrix è ben integrato con AWS e capace di utilizzare le sue APIs: infatti dalla dashboard del Controller è possibile gestire le proprie VPC, le subnet, collezionare statistiche sui flussi di traffico, etc.

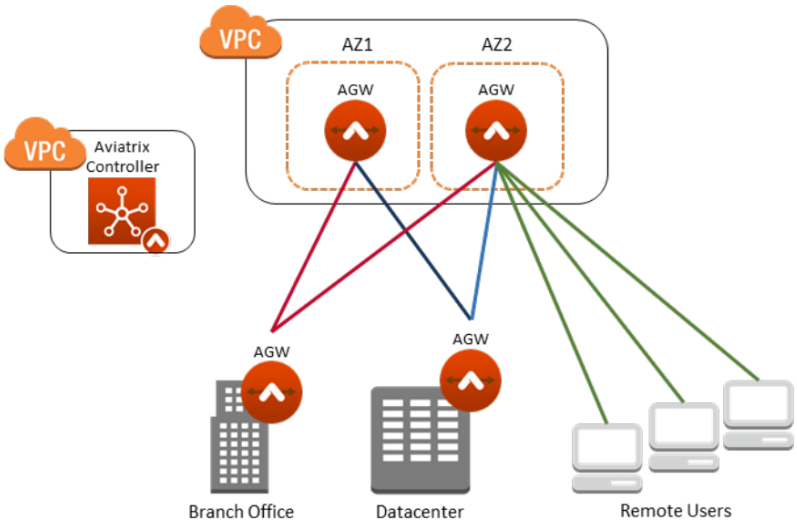


Figura 4-1 Aviatrix Cloud Interconnect: componenti principali e integrazione con AWS

4.3 Cisco SD-WAN

La soluzione SD-WAN di Cisco consiste di tre componenti principali:

- **vEdge Router**, ovvero il router vero e proprio, che può essere sia un dispositivo hardware dedicato (*appliance*) sia una macchina virtuale. L'insieme dei router costituisce il *data plane* della soluzione.
- **vSmart Controller**, che è responsabile del *control plane.*

- **vManage Network Management System**, responsabile del *management plane.*

Un'azienda che vuole adottare questa soluzione disporrà i vEdge Router sui vari branch, sedi remote e datacenter. Tali router permetteranno di connettere i vari branch con le "application VPC" (ovvero le VPC in cui risiedono le applicazioni che si intende raggiungere, vedi Figura 4-2) attraverso una "gateway VPC", cioè una VPC privata in cui sono posti due vEdge ridondanti come macchine virtuali; quest'ultima VPC permette all'amministratore dell'SD-WAN di scalare facilmente rispetto al numero di application VPC che si possono raggiungere, dato che quest'approccio permette di ridurre il numero di tunnel diretti tra le reti on premise e le application VPC.

In questo modo è possibile mappare diverse application VPC alla stessa Gateway VPC e poi sfruttare quest'ultima per creare i tunnel dai branch on premise verso le application VPC (anche dette "host VPC"). Grazie alle "Gateway VPC" è quindi possibile non solo fare *scale up/scale down* del numero delle "Host VPC", a seconda delle richieste, ma anche di assicurare isolamento ai vari workload; ciò permette una più semplice gestione della rete, il monitoraggio delle applicazioni e una maggior sicurezza.

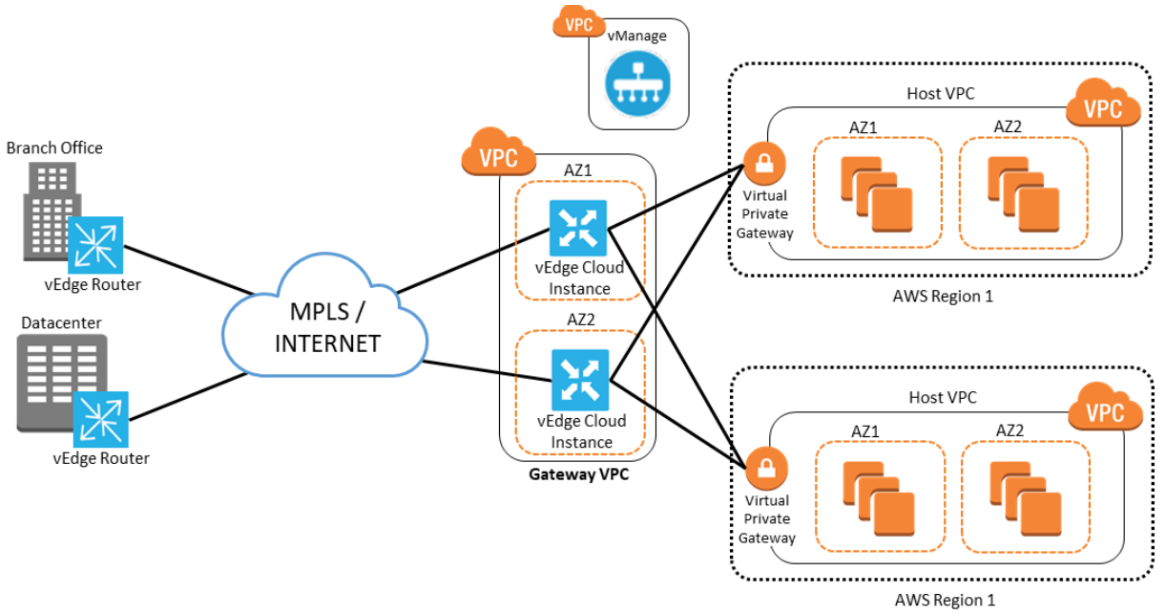


Figura 4-2 Cisco SD-WAN: componenti principali e integrazione con AWS

4.4 Citrix NetScaler SD-WAN

La soluzione SD-WAN di Citrix mira a massimizzare le prestazioni e l'availability delle applicazioni che devono comunicare dalla rete WAN aziendale verso il datacenter privato o il Cloud. A tale scopo Citrix si serve di due funzionalità:

- *Intelligent path selection,* che permette all'SD-WAN di scegliere in tempo reale il percorso migliore dove inoltrare i pacchetti. A differenza di altre SD-WAN, dai branch si possono utilizzare tutti i tipi di trasporto (e.g., MPLS, internet, 4G, etc.); poiché NetScaler monitora lo stato dei collegamenti (in entrambe le direzioni), essa in grado in ogni istante di utilizzare uno qualsiasi dei collegamenti per inviare i pacchetti generati dall'applicazione.

- *QoS policies,* cioè delle policy per garantire QoS definibili in maniera granulare e per specifiche applicazioni, utilizzando un database con priorità predefinite e classi di applicazioni.

Avere delle prestazioni garantite per le proprie applicazioni è un aspetto fondamentale per quelle aziende che dispongono di applicazioni che sono distribuite in diversi punti della rete WAN aziendale, o che si servono pesantemente dei servizi Cloud per la loro infrastruttura IT. In Figura 4-3 sono rappresentati i componenti principali della soluzione e l'integrazione con AWS.

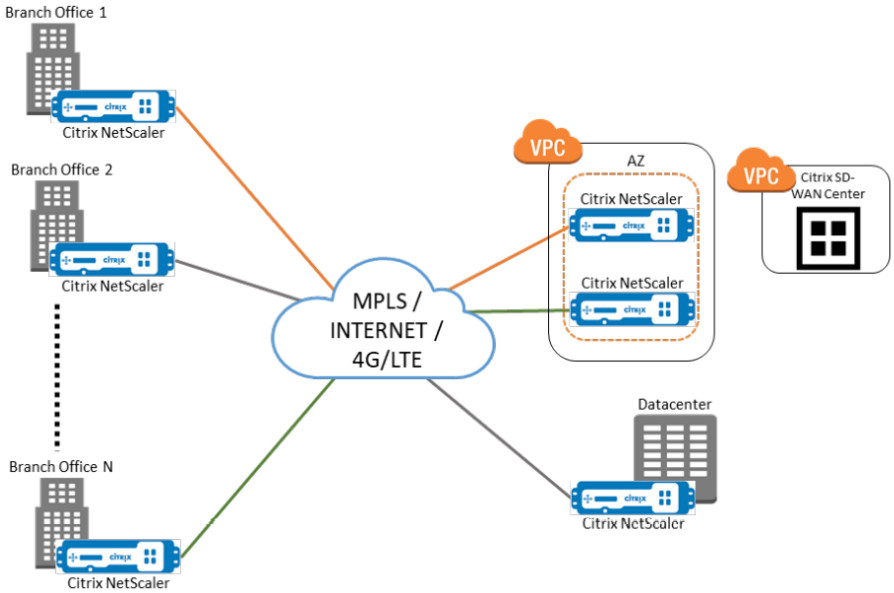


Figura 4-3 Citrix NetScaler SD-WAN: componenti principali e integrazione col Cloud

4.5 CloudGenix Instant-On Network (ION)

CloudGenix Instant-On Network (ION) è un'altra soluzione SD-WAN per interconnettere branch e sedi remote con il datacenter e i cloud provider. Questa soluzione è incentrata *sull'application-centric forwarding*, a differenza di altre soluzioni che invece utilizzato la *deep packet inspection* (DPI) per inoltrare i pacchetti applicativi non cifrati individualmente ad ogni nodo della rete. Al contrario, ION crea delle "sessioni" di traffico cifrato tra i due endpoint dell'applicazione basandosi su delle "*business rules"* oppure dei *service level agreement* (SLA) definiti dal customer stesso.

Dal momento che le aziende utilizzano sempre più applicazioni sia on-premise, sia basate sul cloud e/o di tipo SaaS, permettere una delivery affidabile delle applicazioni stesse diventa una questione cruciale. Pertanto, non ha più senso affidarsi ai soli protocolli di routing per inoltrare il traffico guardando il singolo pacchetto; invece, guardando i pacchetti applicativi come un flusso di traffico end-to-end, è possibile inoltrare il traffico applicativo utilizzando delle "*business rules"* e delle *policy*, che tengono conto di quelle che sono le priorità dell'azienda in un dato momento.

La soluzione consiste di un Controller e dei router ION. Il Controller rappresenta il centro di controllo e management dei router ION, i quali vengono disposti sia presso i vari branch e datacenter on premise, sia pure nel Cloud (come macchine virtuali). Tutti i router ION vanno a

formare la cosiddetta *ION Fabric*, ovvero una rete overlay che astrae i collegamenti fisici WAN sottostanti. Nella Figura 4-4 vengono mostrati i componenti di ION e l'integrazione della soluzione SD-WAN con il Cloud.

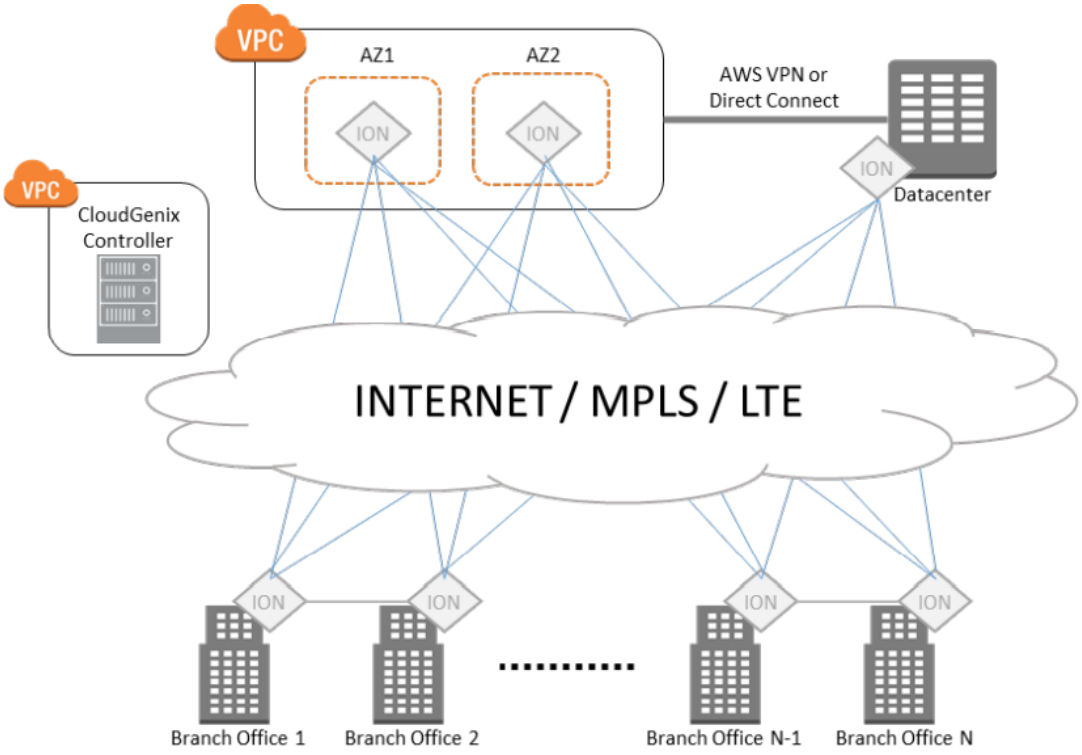


Figura 4-4 CloudGenix Instant-On Network SD-WAN: componenti principali e integrazione col Cloud

4.6 Riverbed SteelConnect

La soluzione SD-WAN sviluppata da Riverbed mira ad aiutare le aziende a realizzare un networking di tipo *application-aware*. Oltre alle varie funzionalità proprie dell'SD-WAN, Riverbed ha integrato in SteelConnect le funzionalità di altri suoi prodotti, in particolare la *WAN optimization* e *l'application performance monitoring*. Inoltre questa soluzione può aiutare le aziende con diverse sedi da collegare che hanno bisogno di ottimizzare la delivery e le prestazioni delle applicazioni.

I componenti principale di questa soluzione sono lo SteelConnect Manager ed i Gateway; lo SteelConnect Manager fa da centro di provisioning, deployment, monitoring e controllo dell'infrastruttura WAN "ibrida" (cioè composta da reti on premise e VPC sul Cloud) e lavora con il Gateway per fornire la connettività tra le reti.

Il deployment dei vari Gateway sul Cloud è molto semplice grazie al cosiddetto "SteelConnect Stack": l'amministratore dell'SD-WAN dovrà inserire delle informazioni sui branch office e le VPC da collegare, dopodiché il Manager si occuperà di trovare una rete libera in un'availability zone di una VPC in cui fare il deployment del Gateway, e ne ricaverà due subnet separate, una *uplink subnet* verso le reti on premise e una *downlink subnet* verso la VPC (vedi Figura 4-5): le due subnet insieme al gateway costituiscono lo SteelConnect Stack. Il Manager lavorerà insieme ai vari Stack (es. Stack1 in AZ1 e Stack2 in AZ2, nella stessa VPC, in un tipico

deployment ad high availability) per rendere possibile l'inoltro del traffico in maniera dinamica tra le reti on premise e le VPC, ovvero utilizzando delle policy a livello di applicazione e delle regole di path selection.

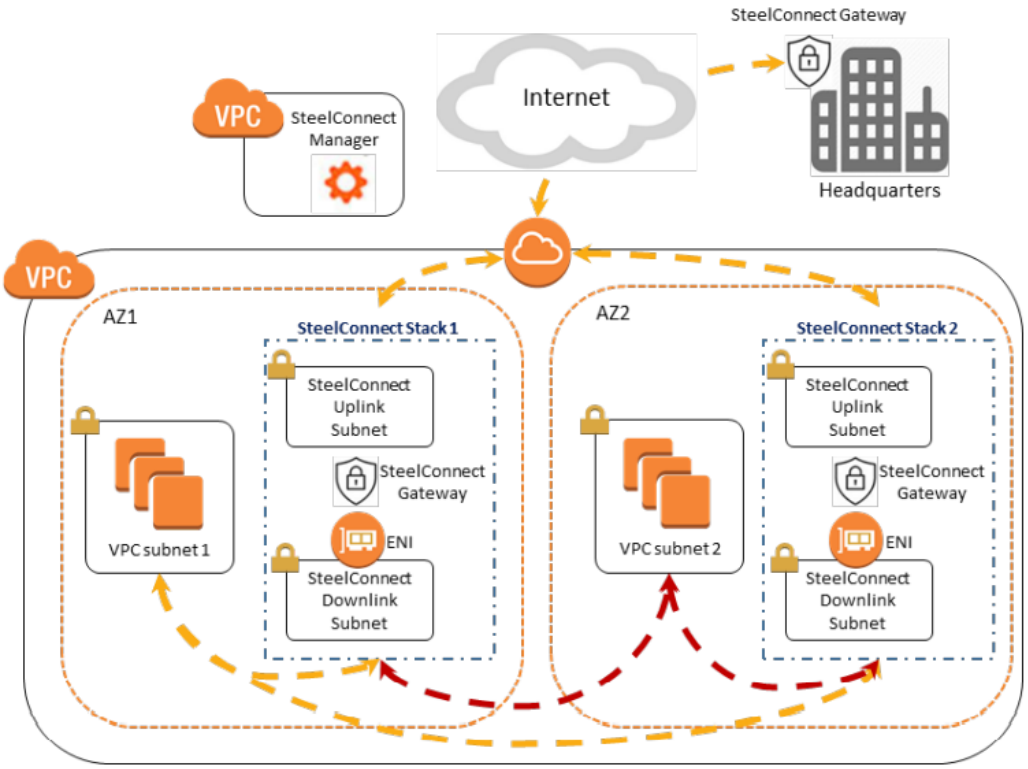


Figura 4-5 Riverbed SteelConnect: componenti principali e integrazione col Cloud

4.7 flexiWAN

4.7.1 Overview

Lo schema architetturale ad alto livello di **flexiWAN** è rappresentato in Figura 4-6 e consta di due componenti principali: un software-based WAN edge router, chiamato **flexiEdge**, e un sistema di management centralizzato, detto appunto **flexiManage**. Ciascun dispositivo flexiEdge comunica direttamente col flexiManage tramite delle API sicure (usando connessioni TLS). In particolare:

- **flexiEdge** consiste nel WAN edge router vero e proprio (virtuale, cioè implementato via software), e svolge la funzione di "data plane" dell'SD-WAN per il singolo branch (on premise o sul Cloud); a sua volta il router flexiEdge è composto di:
  - **infrastruttura di routing**, che consiste in una versione modificata di **VPP** (Vector Packet Processing, un framework che permette il processamento di più pacchetti contemporaneamente, diminuendo il ritardo di processamento dei router)
  - **routing control plane**, che viene implementato tramite la suite di protocolli di routing **FRR**
  - **flexiWAN agent**, la componente software che connette flexiEdge col flexiManage Agent Brocker tramite API protette

- **flexiManage** è il sistema di management centralizzato della piattaforma SD-WAN (che rappresenta il control plane e il management plane). È responsabile della configurazione dei vari router flexiEdge e della raccolta di dati e statistiche sulla rete. Vi si accede tramite un web server scalabile e permette all'amministratore di rete di gestire tutti i router flexiEdge presenti nelle varie sedi. L'**Agent Brocker** si occupa di far comunicare i vari router flexiEdge e fa da "canale" di comunicazione tra il web server e i vari router. Infine c'è l'**analytics system** che colleziona dati e statistiche dai router flexiEdge, li analizza e fornisce dei report all'amministratore.

4.7.2 Scelte di Deployment

Mentre il deployment del componente flexiEdge avviene tipicamente su hardware dedicato oppure in ambienti virtualizzati (sia su datacenter privati sia soprattutto sui vari cloud provider), il deployment di flexiManage invece può essere di tre tipologie:

- **Modello SaaS in ambiente condiviso:** in questo modello flexiManage viene ospitato sul cloud Amazon AWS dagli ingegneri di flexiWAN (l'azienda sviluppatrice dell'omonimo software SD-WAN). I server sono quindi gestiti da flexiWAN e vi sono numerosi account di vari customer sugli stessi server, in una configurazione multi-tenancy; pertanto, questo modello va bene per realizzare delle PoCs o test di laboratorio o per delle aziende molto piccole. Questo è il modello che è stato utilizzato per costruire l'architettura di interconnessione e condurre i test nella presente tesi.
- **Ambiente dedicato:** un ambiente dedicato e "white-label" su misura per il customer, il quale disporrà di server dedicati, potrà usare il proprio nome di dominio per l'accesso a flexiManage, ma non dovrà preoccuparsi dell'installazione e manutenzione dei server. Questa rappresenta la soluzione migliore per aziende medio-grandi e risulta particolarmente utile per gli MSPs che si occupano di gestire l'SD-WAN per conto dei loro customer.
- **Self-hosting:** questo modello prevede l'installazione e manutenzione di tutto il sistema SD-WAN a carico del customer, nel suo cloud privato (i.e. datacenter), il che richiede il dispiegamento di ingenti risorse umane (DevOps). È raccomandabile optare per questo modello soltanto nel caso di grandi deployment (i.e. nel caso di migliaia di sedi da interconnettere).

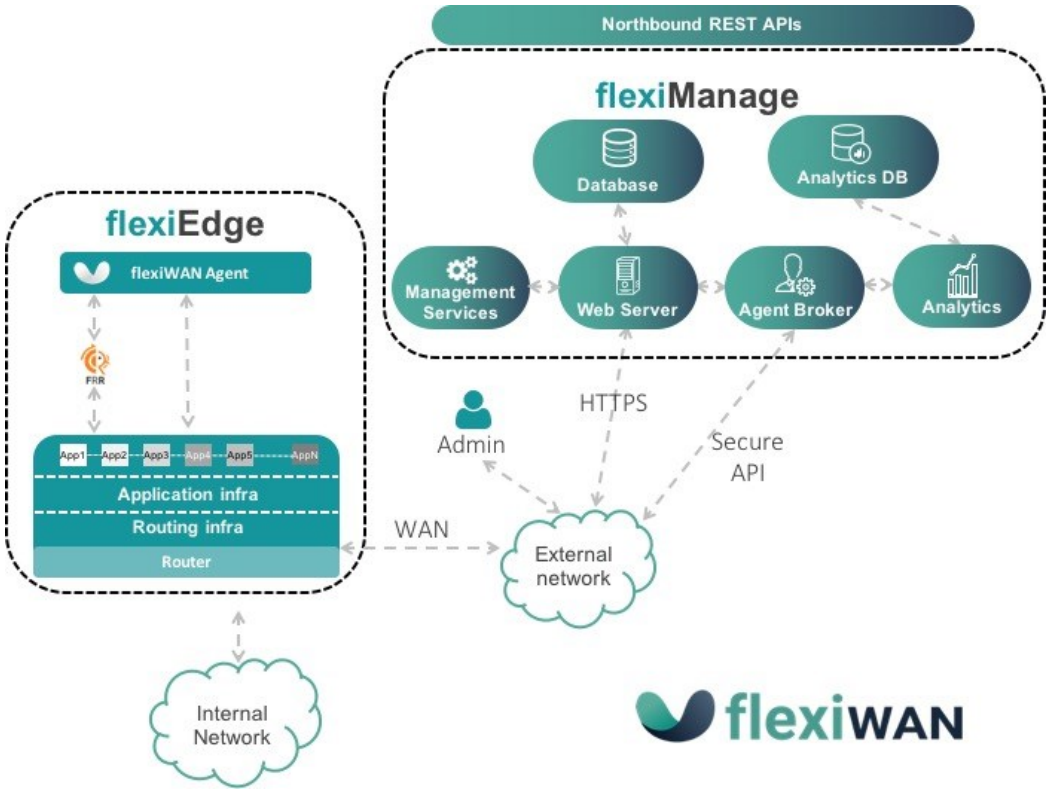


Figura 4-6: Architettura ad alto livello di flexiWAN

4.7.3 Path labels

Le *path labels* rappresentano uno strumento molto potente per poter differenziare le reti di trasporto e i relativi VPN tunnel e quindi influenzare il routing del traffico fra le varie sedi dell'SD-WAN. In sostanza a ogni interfaccia di rete WAN può essere assegnata una o più label, che sta a indicare una specifica rete di trasporto (es. MPLS) oppure uno specifico ISP o qualunque altra "rete logica" che si vuole definire; in questo modo le operazioni di creazione di tunnel o definizione di policy vengono fatte in base alle label, e non in base alla particolare interfaccia del device.

Inoltre esistono due tipi di path label, a seconda che si riferiscono a VPN tunnel tra due device ("Tunnel" label) oppure a interfacce direttamente collegate a Internet ("Direct Internet Access" label). Come esempio di consideri la topologia in Figura 4-7, in cui vi sono due flexiEdge router, ciascuno con due interfacce WAN etichettate con le label Blue e Green, collegati tramite due tunnel, uno per ogni label; l'uso di label diverse in questo caso potrebbe indicare la presenza di due reti di trasporto differenti (es. Fibra vs. 4G, oppure ISP1 vs. ISP2, etc.) e permette di avere un controllo granulare sulla creazione dei tunnel e sui percorsi del traffico di rete tra le due sedi, tramite la definizione di policy che, ancora una volta, si basano sulle label (es. failover/load balancing del traffico sui due tunnel verso le destinazioni interne).

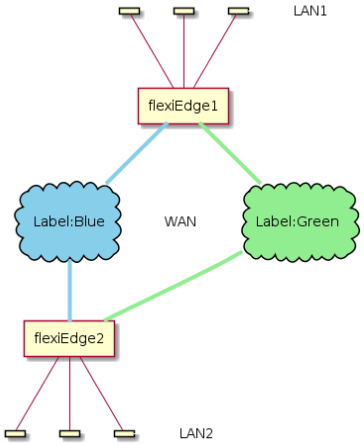


Figura 4-7: Topologia di esempio sulla definizione di path labels

4.7.4 Path selection e definizione delle policy

La funzione di Path Selection, tramite la definizione di policy, permette al sistema SD-WAN di realizzare il cosiddetto *application-aware routing*, ovvero decidere dinamicamente su quale interfaccia inoltrare un certo tipo di traffico (es. traffico voce), così da ottenere un comportamento di load balancing, failover, oppure di differenziazione del traffico.

Tale funzionalità di flexiWAN si serve di tre meccanismi fondamentali dell'approccio SD-WAN: l'identificazione e classificazione del traffico a livello applicativo, il concetto di path labels e le policy, che scelgono dove inoltrare il traffico in base alle path labels assegnate alle interfacce dei dispositivi.

La classificazione del traffico avviene grazie a un database di applicazioni predefinite che possono essere selezionate a seconda del nome (sia in base alla porta, es. BitTorrent, sia in base al range di indirizzi, es. Dropbox), della categoria (es. file sharing, management, autenticazione, …), della service class (es. real-time), o dell'importanza (che può essere definita dal customer in base alle sue esigenze per dare priorità ad alcune applicazioni rispetto ad altre).

Consideriamo adesso come la funzione di path selection riesce a influenzare quella di routing e come queste due convivono insieme. Anzitutto, affinché il traffico sia sempre inoltrato su un percorso realmente disponibile, il routing ha sempre priorita sul path selection; quindi, per una certa destinazione D vengono prima calcolati i percorsi migliori (secondo il protocollo di routing utilizzato), poi a parità di costo, la policy installata sui dispositivi permette all'SD-WAN di decidere quale percorso utilizzare (e come) tra quelli disponibili. Per esempio un tipico deployment è quello in cui ci sono più tunnel verso una certa destinazione (es. tunnel1=fiber e tunnel2=4G) e quindi più percorsi con lo stesso costo, in cui l'SD-WAN deciderà quale percorso utilizzare proprio in base alla policy definita.

5 Progettazione dell'architettura SD-WAN

5.1 High Level Design

L'high level design dell'interconnessione da *on-premises* verso diversi cloud provider, gestista con SD-WAN, comprende:

- un nodo on premise con accesso ad internet su due reti di trasporto eterogenee (es. wideband Internet e 4G);
- una rete cloud complessa realizzata su cloud AWS con deployment multi-AZ, con diverse zone di rete a perimetro di sicurezza differente;
- un'ulteriore rete cloud complessa realizzata su un altro cloud provider, *Alibaba Cloud*, secondo le best-practices di riferimento (vedi Paragrafo 5.4).

Il deployment di tutta l'architettura è realizzato sul cloud AWS, secondo il modello IaaS, e consiste in una prima VPC (**Branch-1**) che rappresenta la rete on-premise, una seconda VPC (**Hub-Cloud**) che rappresenta la rete di "front-end" per l'accesso alle risorse sul Cloud, e infine un'altra VPC (**Cloud-services**) che ospita i server veri e propri (e.g. un server della rete 172.18.0.0/16, vedi Figura 5-1); quest'ultima VPC è collegata ad Hub-Cloud tramite un Transit Gateway, un servizio di AWS che permette di collegare due o più VPC fra di loro.

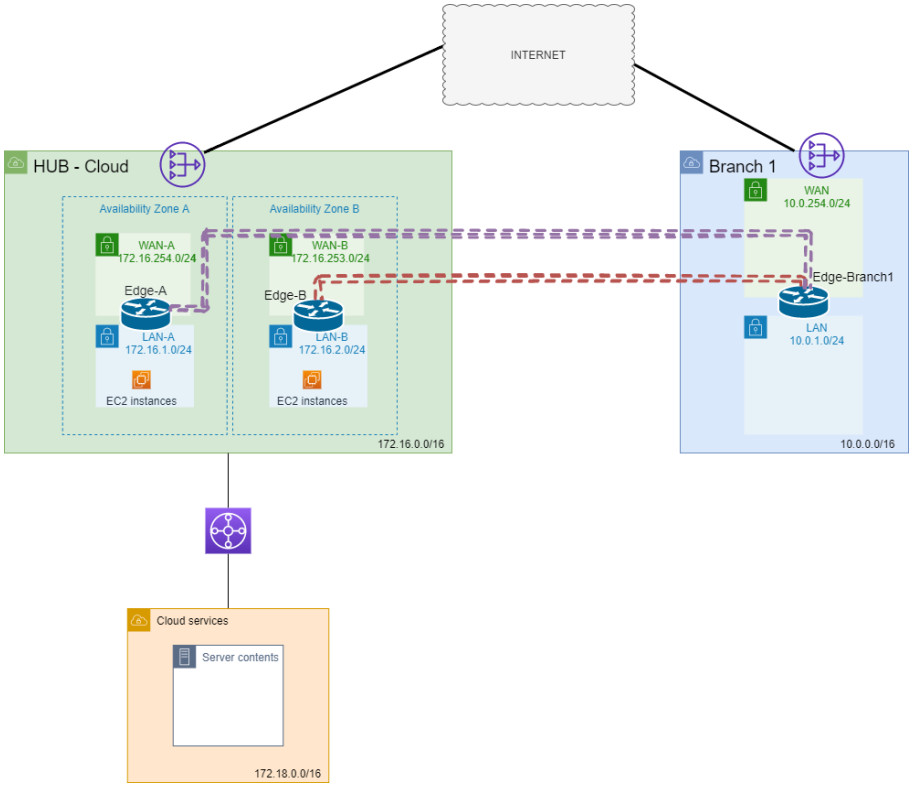


Figura 5-1: Architettura di principio High Availability

In questo contesto il servizio **AWS Transit Gateway** offre la funzionalità di router di livello 3, perché permette di collegare due o più VPC fra di loro, come mostrato nella Figura 5-2.

Ogni VPC ha la sua *route table* contenente due entry:

- la prima entry rappresenta la default route per tutte le destinazioni all'interno della VPC; tale entry permette alle macchine virtuali (*EC2 instance*) della VPC di comunicare fra di loro.
- La seconda entry serve a inoltrare tutto il traffico destinato al di fuori della VPC verso il *transit gateway*.

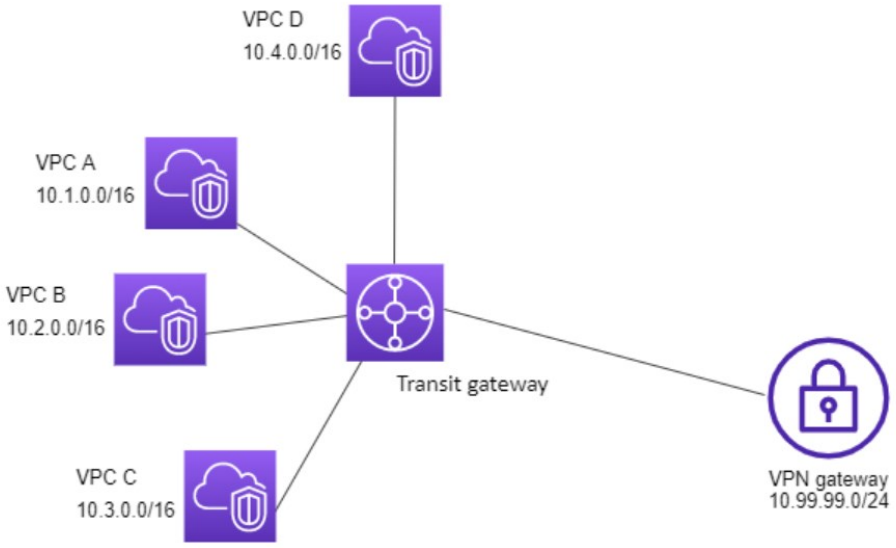


Figura 5-2 Uso del transit gateway per collegare le VPC

Inoltre, la route table del transit gateway, per la topologia descritta in figura, sarà la seguente:

Destination	Target	Route type
10.1.0.0/16	`Attachment for VPC A`	propagated
10.2.0.0/16	`Attachment for VPC B`	propagated
10.3.0.0/16	`Attachment for VPC C`	propagated

Cioè avrà tante entry quante sono le VPC da collegare, ognuna con il campo destinazione pari al blocco CIDR della VPC e con target l'attachment (i.e. il collegamento) verso la VPC stessa. La configurazione descritta abilita la VPC sia al traffico *intra-VPC*, sia a quello *inter-VPC* grazie all'utilizzo del transit gateway.

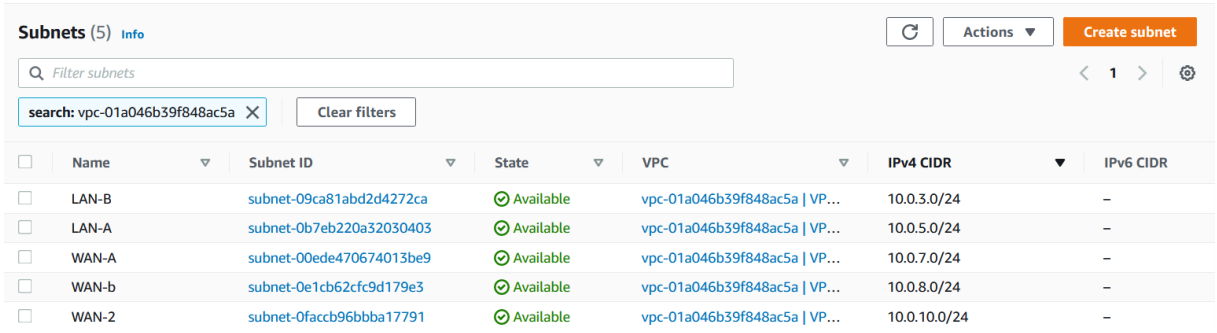
5.2 Deployment di flexiWAN sul cloud AWS

In questo paragrafo si illustra l'installazione e il deployment di flexiWAN sul cloud AWS, passando in rassegna tutti i passi necessari a creare la macchina virtuale su AWS, secondo i requisiti di flexiWAN, per poi configurarla come istanza SD-WAN.

5.2.1 Creazione delle subnet

Ciascuna istanza flexiWAN (detta flexiEdge) dovrà disporre di un'interfaccia LAN e di una (o più) interfaccia WAN. In AWS ogni *network interface* appartiene a una subnet, che a sua volta fa parte di una VPC; pertanto andremo a creare due subnet distinte (LAN e WAN rispettivamente), nella stessa VPC, in cui saranno poste le interfacce del flexiEdge.

A tale scopo, dalla console AWS navighiamo nel servizio VPC e andiamo creare le rispettive subnet, LAN-A e WAN-A, che sono mostrate di seguito:



5.2.2 Esecuzione della macchina virtuale

Dopo aver creato le subnet in cui "vivrà" il router flexiWAN, è possibile lanciare l'esecuzione di una nuova macchina virtuale. Per prima cosa è necessario scegliere l'AMI da cui far partire la macchina virtuale. In AWS un'AMI rappresenta una sorta di template che contiene già tutta la configurazione software necessaria a far partire la macchina (sistema operativo, applicazioni, etc.); nel nostro caso, flexiWAN supporta il sistema operativo "Ubuntu 18.04 LTS x86/64", di cui è già fornita un'AMI da AWS. Dopodiché andremo a scegliere l'*instance type*, che determina le risorse computazionali che saranno assegnate alla macchina (es. numero di virtual CPU, quantità di memoria fisica, etc.). Per i requisiti specifici di flexiWAN, è consigliato utilizzare l'instance type "m5.large", che permette di disporre di:

- 2 vCPU
- 8 GiB di memoria RAM
- Fino a 10Gbps di banda di rete per ogni interfaccia (vedi Figura 5-3)

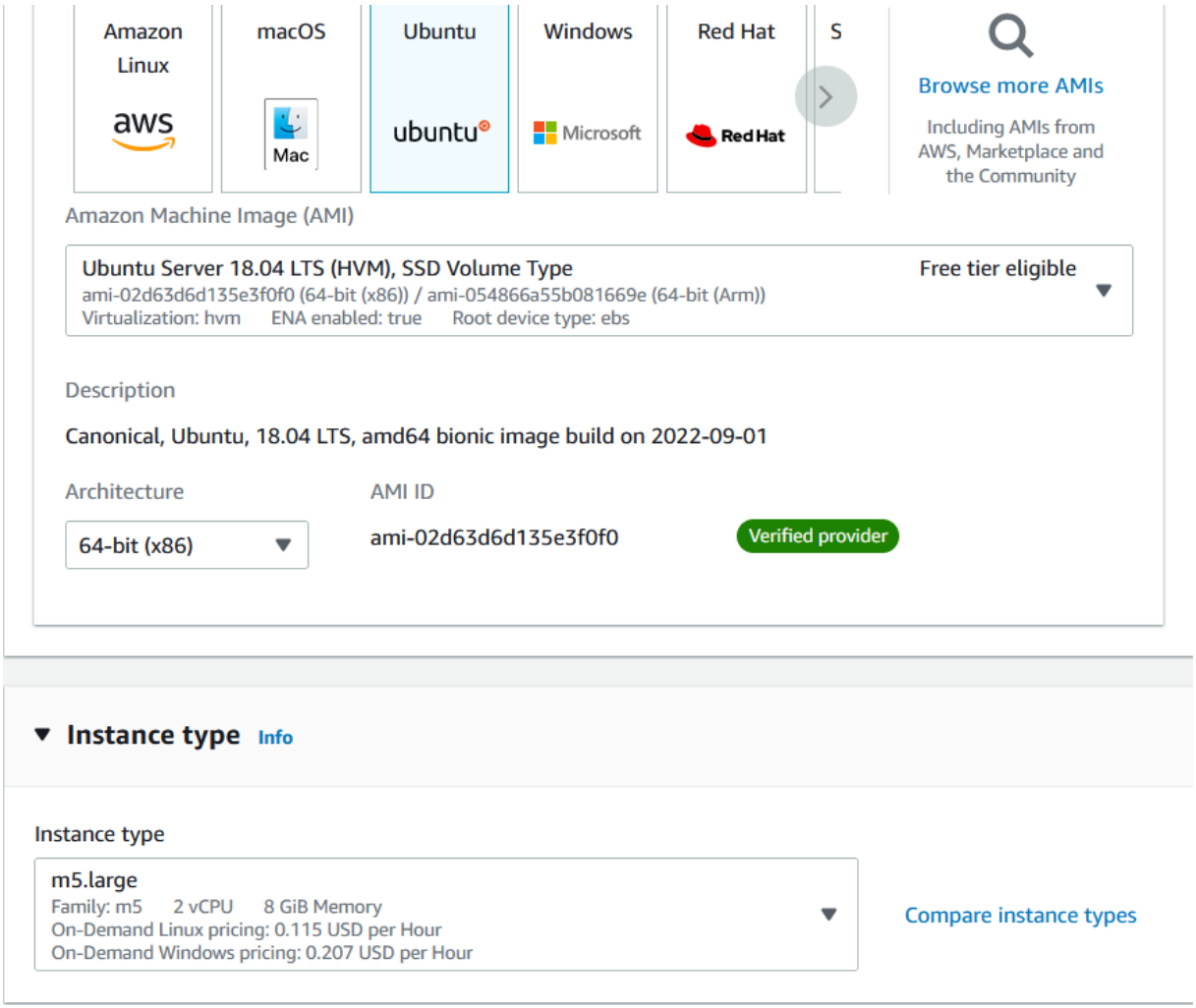
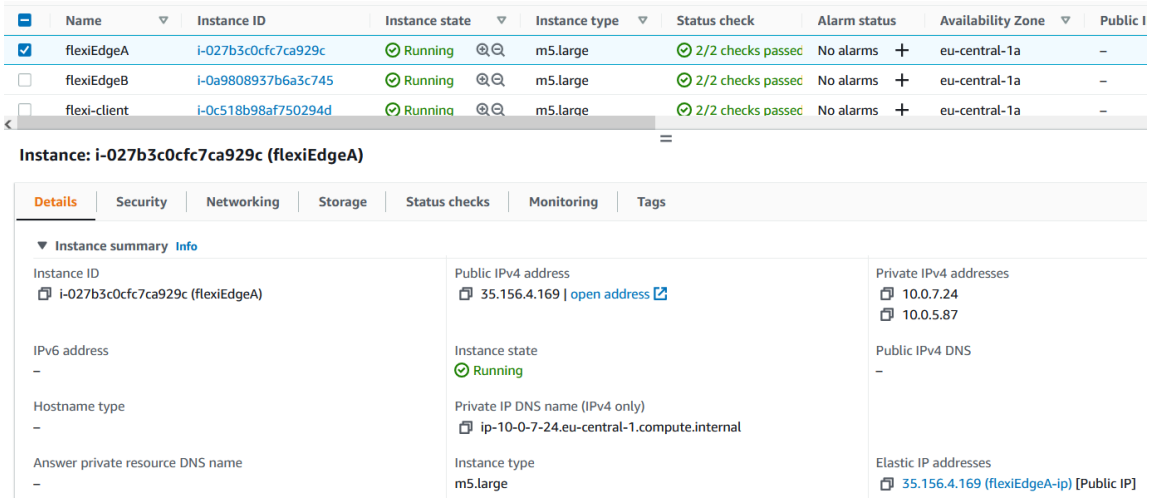


Figura 5-3 Configurazione per l'avvio di una macchina virtuale dalla console AWS

Quindi, di procede nella configurazione delle impostazioni di rete della macchina che, come detto, dovrà avere un'interfaccia nella subnet LAN-A e una in WAN-A; inoltre all'interfaccia WAN dovrà essere associato un indirizzo IP pubblico statico, così che la macchina conservi lo stesso indirizzo pubblico anche dopo un eventuale riavvio della stessa, e risulti quindi sempre raggiungibile da flexiManage, il centro di controllo dell'SD-WAN da cui imporre le configurazioni desiderate alla rete.

Dopodiché è possibile procedere al *launching* della macchina virtuale, che dopo qualche secondo apparirà nello stato di *running* sulla console, con tutti i dettagli appena configurati:



5.2.3 Installazione di flexiWAN

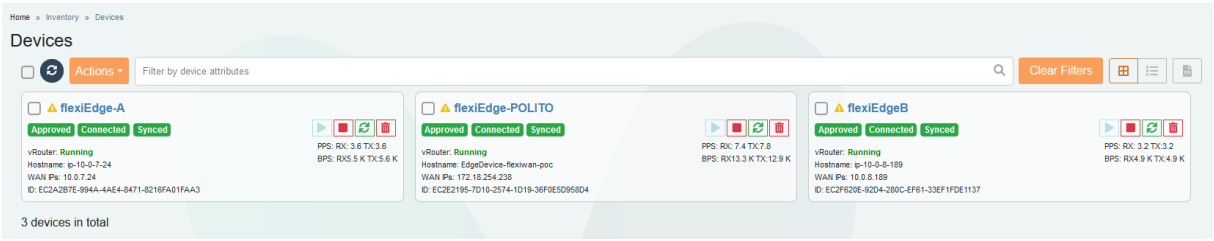
Dopo che la macchina virtuale è stata creata, è possibile connettersi ad essa in SSH utilizzando la chiave privata che è stata configurata durante l'avvio dalla console. Per permettere la connessione in SSH, abbiamo dovuto abilitare esplicitamente le connessioni in ingresso sulla porta 22 nel *security group* della macchina.

Una volta connessi alla macchina, è possibile installare flexiWAN come pacchetto APT (Advanced Packaging Tool); in particolare bisogna eseguire i seguenti comandi come utente root:

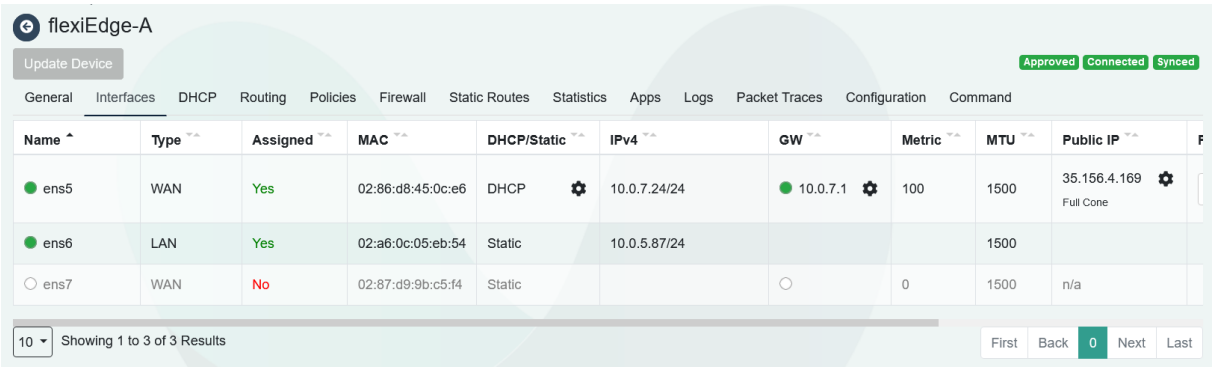
1. `sudo curl -sL https://deb.flexiwan.com/setup | sudo bash -`
2. `sudo apt-get install -y flexiwan-router`

Il primo comando permette di aggiungere la chiave associata a flexiWAN al database locale delle apt-key e la repository corrispondente alla lista delle repository di apt-get. Il secondo comando provvede a installare il software (pacchetto) flexiWAN, che renderà la macchina virtuale un router flexiEdge configurabile all'interno di un sistema SD-WAN.

Infine, dopo qualche secondo il dispositivo risulterà visibile dal pannello di flexiManage (insieme agli altri dispositivi eventualmente configurati):



A questo punto, si procede ad abilitare le interfacce del dispositivo, che avranno assegnati automaticamente gli indirizzi IP delle corrispondenti *network interface* su AWS precedentemente definite (compreso l'indirizzo IP pubblico):



5.3 Configurazione dei percorsi multipli

La valutazione dell'affidabilità e della resilienza dell'architettura proposta si basa, oltre che sulla ridondanza degli edge router, anche sulla ridondanza dei collegamenti WAN e quindi sulla possibilità di avere percorsi multipli verso i cloud provider.

In particolare si è scelto di misurare il *tempo di failover*, ovvero il tempo necessario al link "secondario" per prendere il posto del link principale, dopo il verificarsi un guasto su quest'ultimo.

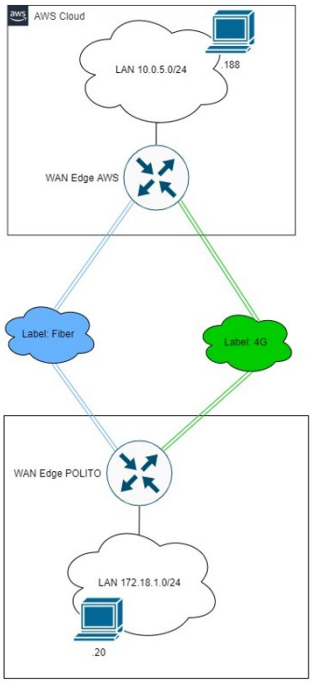


Figura 5-4: architettura SD-WAN con due reti di trasporto

La topologia utilizzata per le misurazioni è quella riportata in Figura 5-4, dove sono state impiegati due flexiEdge router per collegare altrettante reti tra loro (una rete on-premise 172.18.1.0/24 col router **Edge-Polito** e una rete su AWS 10.0.5.0/24 con il router **Edge-Cloud**). Il router Edge-Polito ha due interfacce di rete WAN che sono connesse a Internet attraverso due reti di trasporto differenti (rete in fibra e rete wireless 4G). Per permettere al sistema SD-WAN di riconoscere la diversa natura dei collegamenti WAN, e quindi di applicare correttamente le policy, sono state assegnate delle *label* alle interfacce, chiamate appunto "**Fiber**" e "**4G**":

Name	Type	Assigned	MAC	DHCP/Static	IPv4	GW	Metric	MTU	Public IP	Path Labels
eno1	WAN	Yes	40:a8:f0:46:0c:0b	Static	192.168.0.121/23	192.168.0.254	100	1500	130.192.225.251 Full Cone	Fiber
enp1s0f0	WAN	Yes	00:e0:ed:22:ee:dc	Static	192.168.3.3/24	192.168.3.1	200	1500	5.90.16.95 Full Cone	4G ISP
enp1s0f1	LAN	Yes	00:e0:ed:22:ee:dd	Static	172.18.1.1/24			1500		

Figura 5-5 Configurazione delle interfacce di Edge-Polito in flexiManage

Per il router Edge-Cloud si è scelto di configurare le interfacce allo stesso modo, con le medesime label, anche se in realtà in questo caso è presente una singola rete di trasporto (la rete di AWS); ciò è stato fatto in modo da creare due percorsi ben separati per il traffico che passa su rete via cavo e quello che viaggia col 4G:

Name	Type	Assigned	MAC	DHCP/Static	IPv4	GW	Metric	MTU	Public IP	Path Labels
ens5	WAN	Yes	02:86:d8:45:0c:e6	DHCP	10.0.7.24/24	10.0.7.1	100	1500	35.156.4.169 Full Cone	Fiber
ens6	LAN	Yes	02:a6:0c:05:eb:54	Static	10.0.5.87/24			1500		
ens7	WAN	Yes	02:87:d9:9b:c5:f4	DHCP	10.0.10.116/24	10.0.10.1	110	1500	35.156.251.156 Full Cone	4G ISP

Figura 5-6 Configurazione delle interfacce di Edge-Cloud in flexiManage

Dopo aver configurato le interfacce con le label opportune, si procede con la creazione dei tunnel tra le due istanze flexiEdge, un tunnel per la label “Fiber” e un altro per quella “4G ISP”; lo stato “connected” indica che il tunnel sta funzionando correttamente e vengono anche forniti i valori in tempo reale su latenza e perdita di pacchetti.

ID	Device A	Interface A	Device B	Interface B	Path Label	AVG Latency	Drop Rate	Encrypt	Status	Actions
1	flexiEdgeA	ens7 (loopback:10.100.0.4)	node-polito	enp1s0f0 (loopback:10.100.0.5)	4G ISP	83.22 ms	0.00 %	IKEv2	Connected	
2	flexiEdgeA	ens5 (loopback:10.100.0.6)	node-polito	eno1 (loopback:10.100.0.7)	Fiber	12.68 ms	0.00 %	IKEv2	Connected	

Figura 5-7 Configurazione dei tunnel in flexiManage

Il comportamento di failover tra i due link si ottiene semplicemente creando una policy che vada a usare il tunnel Fiber quando questo è in stato di running, oppure il tunnel 4G se il primo non è più disponibile:

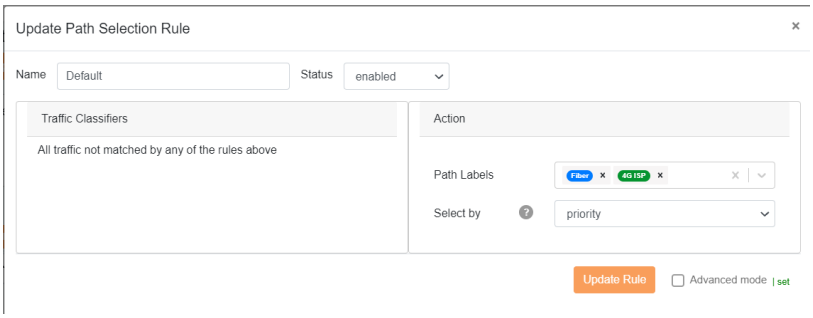


Figura 5-8 Configurazione di una policy di path selection in flexiManage

Il **tempo di failover** è dato dalla somma di due contributi:

- *Time to detection*: il tempo impiegato dal router per rilevare che c'è stato un guasto sul link
- *Time to convergence*: il tempo necessario affinché il traffico sia inoltrato su un altro percorso, una volta che il guasto è stato rilevato.

Poiché il tempo di failover sarà sicuramente dell'ordine dei secondi (si tratta in sostanza del tempo di convergenza di un protocollo di routing), l'approccio più immediato è quello di utilizzare il comando **ping**. Tale comando invia una ICMP Echo Request verso una macchina target, la quale risponde con un ICMP Echo Reply entro un secondo; se il messaggio di Echo Reply non viene ricevuto dopo un secondo, allora la macchina sorgente invia un altro Echo Request. Pertanto, per misurare il tempo di failover si può semplicemente contare il numero di pacchetti Echo Reply che sono andati persi, i quali rappresentano proprio una stima del tempo di failover. Nel caso dello Spanning Tree (IEEE 802.D) per esempio, dove il tempo di failover oscilla tra i 30 e i 90 secondi, quest'approccio risulta molto efficace. Oltre che allo Spanning Tree, questo semplice approccio si può applicare alla maggior parte delle misurazioni a livello di rete (livello 3 ISO/OSI), come ad esempio RIP, OSPF, VRRP e BFD.

Nel caso specifico, i test sono stati condotti lanciando il comando ping quando i due tunnel sono entrambi disponibili e quindi andando a cancellare una rotta statica (sul router di AWS) che fa cadere immediatamente il tunnel primario (Fiber), costringendo l'SD-WAN a far virare il traffico sul tunnel secondario (4G). Il numero di pacchetti Echo Reply persi da quando il tunnel principale cade fino a che il tunnel secondario non prende il suo posto, rappresenta proprio la misura del failover time:

```
64 bytes from 10.0.5.188: icmp_seq=14 ttl=62 time=12.7 ms
64 bytes from 10.0.5.188: icmp_seq=15 ttl=62 time=12.6 ms
64 bytes from 10.0.5.188: icmp_seq=48 ttl=62 time=48.9 ms
64 bytes from 10.0.5.188: icmp_seq=49 ttl=62 time=37.5 ms
64 bytes from 10.0.5.188: icmp_seq=50 ttl=62 time=82.4 ms
```

Figura 5-9 Ping test per misurare il tempo di failover

Su una serie di cinque misurazioni successive, la media aritmetica del failover time è risultata essere:

$$(32 + 26 + 30 + 32 + 33) / 5 = 30{,}6 \text{ sec.}$$

Dall'output del comando ping riportato si può notare come il Round Trip Time (RTT) aumenti significativamente passando dal tunnel primario (Fiber) a quello secondario (4G), testimoniando il fatto che si sta passando a una rete di trasporto più lenta.

5.4 Scenario multi-cloud

L'ultimo scenario che andremo a presentare è quello multi-cloud, ovvero un'architettura SD-WAN in cui sono presenti, oltre all'istanza SD-WAN on premise, due o più istanze poste in reti cloud complesse appartenenti a cloud provider diversi (nel nostro caso, AWS e *Alibaba Cloud* rispettivamente). Anche in questo scenario abbiamo scelto di avere dei collegamenti WAN ridondati dall'on premise verso ciascun cloud provider e di utilizzare il tempo di failover come metrica per misurare l'affidabilità e la resilienza della soluzione.

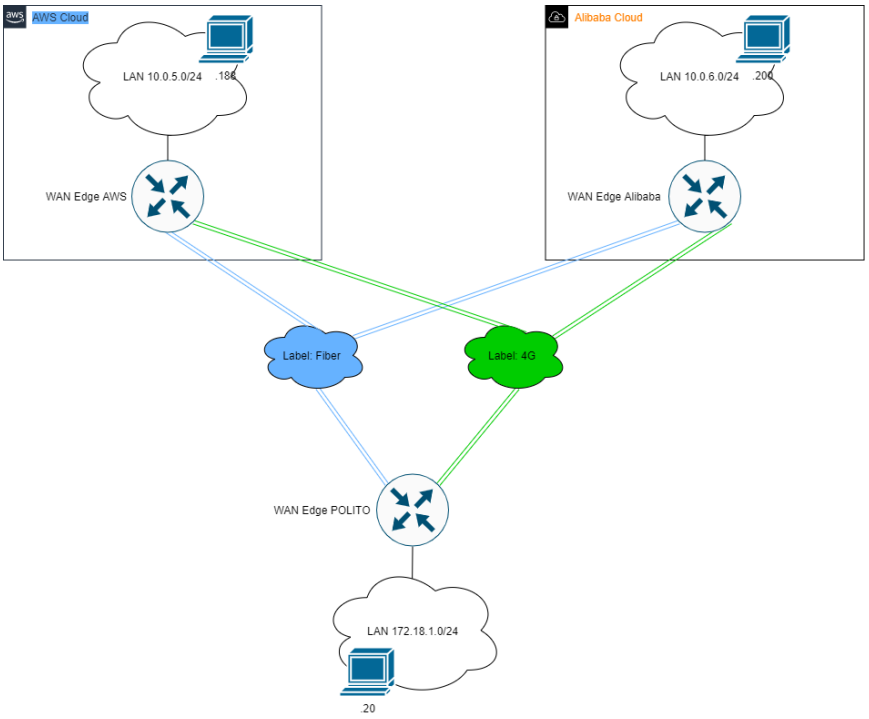
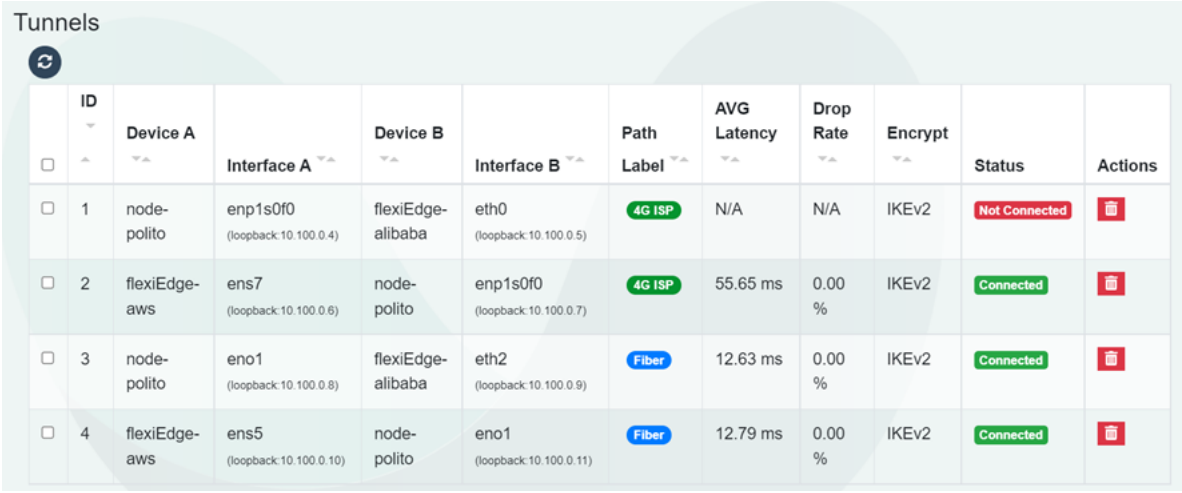


Figura 5-10 Architettura SD-WAN con due cloud provider

La topologia utilizzata è stata riportata in Figura 5-10 e consiste in tre istanze flexiEdge:

- **Edge-Polito:** è il punto di ingresso alla rete on premise 172.18.1.0/24 e ha due interfacce di rete WAN collegate a due reti di trasporto distinte (Fibra e 4G rispettivamente). Come fatto in precedenza, per permettere a flexiWAN di riconoscere la rete di trasporto del collegamento WAN, per poi inoltrare il traffico sul percorso scelto in base all'applicazione delle policy, sono state assegnate opportunamente delle *label* alle interfacce ("Fiber" e "4G").
- **Edge-AWS:** è l'istanza presente in rete cloud AWS (blocco CIDR 10.0.5.0/24) e ha le interfacce WAN configurate con le medesime label, pur essendo presente una sola rete di trasporto (quella del cloud provider); ciò è stato pensato in modo da creare due percorsi ben distinti per i due flussi di traffico, quello che viaggia su rete in fibra e quello che viaggia su rete 4G.
- **Edge-Alibaba:** è l'istanza presente in rete cloud Alibaba (blocco CIDR 10.0.6.0/24) e ha le interfacce WAN configurate analogamente a quanto fatto per l'istanza su AWS.

Per quanto riguarda il collegamento tra i nodi dell'SD-WAN, dal pannello di flexiManage abbiamo creato due tunnel IPsec (uno tra le interfacce "Fiber" e un altro tra quelle "4G ISP") tra Edge-Polito e ciascuno dei due nodi sul Cloud, per un totale di quattro tunnel creati, come mostrato di seguito:



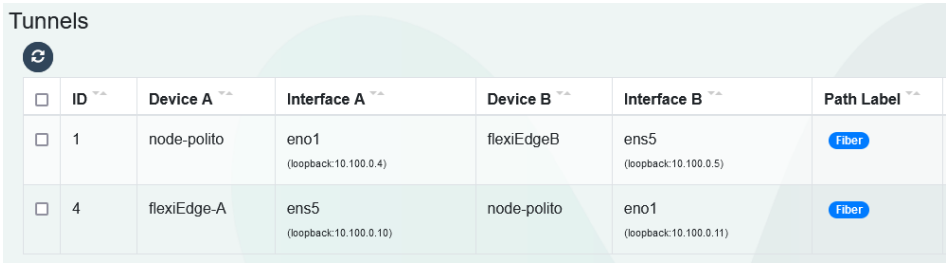
ID	Device A	Interface A	Device B	Interface B	Path Label	AVG Latency	Drop Rate	Encrypt	Status	Actions
1	node-polito	enp1s0f0 (loopback:10.100.0.4)	flexiEdge-alibaba	eth0 (loopback:10.100.0.5)	4G ISP	N/A	N/A	IKEv2	Not Connected	
2	flexiEdge-aws	ens7 (loopback:10.100.0.6)	node-polito	enp1s0f0 (loopback:10.100.0.7)	4G ISP	55.65 ms	0.00 %	IKEv2	Connected	
3	node-polito	eno1 (loopback:10.100.0.8)	flexiEdge-alibaba	eth2 (loopback:10.100.0.9)	Fiber	12.63 ms	0.00 %	IKEv2	Connected	
4	flexiEdge-aws	ens5 (loopback:10.100.0.10)	node-polito	eno1 (loopback:10.100.0.11)	Fiber	12.79 ms	0.00 %	IKEv2	Connected	

Figura 5-11 Configurazione dei tunnel in flexiManage per lo scenario multi-cloud

Come si vede dalla figura, il tunnel dal nodo on premise verso quello su cloud Alibaba non è passato nello stato "connected". Ciò è dovuto probabilmente all'infrastruttura di rete del datacenter di Alibaba, che utilizza il protocollo VXLAN con UDP (un protocollo di tunneling che permette di incapsulare frame Ethernet all'interno di pacchetti UDP), ovvero lo stesso protocollo utilizzato da flexiWAN per il tunneling dei pacchetti; questo provoca talvolta l'impossibilità di instaurare un tunnel con l'istanza SD-WAN sul cloud Alibaba.

5.5 Ridondanza dell'Edge-router

Ciascun WAN-Edge router (**Edge-A** e **Edge-B** in Figura 5-1) è eseguito come macchina virtuale, i.e. istanza EC2 per AWS, in una AZ separata ed ha un'interfaccia WAN assegnata ad una subnet pubblica (**WAN-A** e **WAN-B** rispettivamente). Queste subnet avranno associate una tabella di routing con una *default route* che punta verso l'Internet gateway. Ogni WAN-Edge router ha inoltre già stabilito un tunnel VPN (attraverso Internet, quindi sull'interfaccia WAN) che termina verso il router on-premise **Edge-Polito**. La creazione e gestione dei tunnel è effettuata direttamente dal sistema SD-WAN tramite il management pane, quindi senza richiedere la configurazione dei singoli dispositivi:



ID	Device A	Interface A	Device B	Interface B	Path Label
1	node-polito	eno1 (loopback:10.100.0.4)	flexiEdgeB	ens5 (loopback:10.100.0.5)	Fiber
4	flexiEdge-A	ens5 (loopback:10.100.0.10)	node-polito	eno1 (loopback:10.100.0.11)	Fiber

Le istanze EC2 che si trovato nelle subnet **LAN-A** e **LAN-B** hanno invece un'altra tabella di routing, in cui la *default route* punta all'interfaccia LAN di uno dei due router.

Inoltre ciascun router annuncerà sia la sua LAN sia quella dell'altro router: per es. il router Edge-B annuncerà non solo la sua LAN 10.0.3.0/24, ma anche LAN-A (10.0.5.0/24), che sarà inserita come *static route* e poi redistribuita in OSPF:

Destination	Gateway	Interface	Metric	Redistribute via OSPF
10.0.5.0/24	10.0.8.1		100	Enabled

Dal momento che la route table di AWS permette di avere solamente un "active target" alla volta, ci sarà sempre un solo router "active" per il traffico in uscita dalla subnet.

Se si verifica un guasto su Edge-A, l'obiettivo è quello di far virare il traffico in ingresso e in uscita alla rete Cloud verso Edge-B. Analizziamo separatamente i due casi di traffico in ingresso nella VPC oppure in uscita verso Internet:

- Per il traffico **incoming (o ingress)**, l'endpoind remoto del tunnel VPN (Edge-polito) dovrà rilevare che il tunnel non è più attivo tramite i protocolli di routing;
- per il traffico **outgoing (o egress)** c'è bisogno invece di un meccanismo esterno che permetta di rilevare il guasto di Edge-A e modificare, tramite una chiamata API, la routing table per redirigere il traffico verso Edge-B (0.0.0.0 -> Edge-B).

A causa dell'impossibilità di gestire la connettività layer 2 in ambiente AWS, che rende impossibile utilizzare i tipici meccanismi di failover dei router (es. quelli già implementati nei router Cisco usati per il Cloud), abbiamo deciso di progettare e implementare una soluzione specifica per il cloud provider che sfrutta solamente i servizi AWS, che verrà presentata alla fine del capitolo.

5.6 Automatismo per il failover automatico dell'edge router

Prima di descrivere l'automazione nei particolari, è utile approfondire i servizi AWS principali che sono stati utilizzati per realizzarla, ovvero **AWS Lambda, AWS CloudWatch (EventBridge)** ed **SNS.**

5.6.1 AWS Lambda

È un servizio di computing in cui è possibile caricare del codice (es. Python, Node.js, etc.) e creare una funzione Lambda. Il servizio si occuperà di fare il provisioning e di gestire i server (virtuali) su cui il codice andrà effettivamente eseguito. In questo modo lo sviluppatore non deve preoccuparsi dell'ambiente di sviluppo, del sistema operativo, di applicare le patch, dello scaling, etc. All'interno della Lambda, il codice viene compresso in un "code deployment package" e contiene un event handler.

AWS Lambda viene utilizzato principalmente in due modi:

- Per processare eventi in un contesto di architettura event-driven: la Lambda esegue il codice in risposta a determinati eventi, che possono consistere in cambiamenti ai dati di un bucket S3, di una tabella DynamoDb, o ancora di una route table all'interno di una VPC (come nell'automazione che andremo a creare).
- Oppure per eseguire del codice in risposta a richieste http utilizzando il servizio API Gateway.

A differenza dei server tradizionali, le funzioni Lambda non vengono eseguite costantemente. Quando una funzione viene "innescata" da un evento, si dice che è avvenuta un'invocazione. Le funzioni Lambda sono appositamente limitate a una durata di 15 minuti, tuttavia la

maggior parte delle invocazioni dura in media meno di un secondo: infatti, sebbene in alcune operazioni ad elevato carico computazionale ci possono volere diversi minuti per elaborare un singolo evento, nella maggioranza dei casi la durata è assai breve.

Ci sono numerosi tipi di eventi che possono innescare una Lambda, come ad esempio una richiesta http tramite API Gateway, una regola programmata di EventBridge, oppure una notifica di S3.

5.6.2 AWS CloudWatch (EventBridge)

AWS EventBridge è un servizio che gestisce bus di eventi tramite cui è possibile connettere servizi AWS differenti in un contesto event-driven. È possibile utilizzare EventBridge per implementare meccanismi di automazione e risposndere automaticamente a eventi di sistema, ad esempio problemi di raggiungibilità di un'applicazione oppure cambi di stato di una risorsa. Gli eventi generati dai servizi AWS vengono consegnati a EventBridge in maniera "near real time". È possibile creare regole per indicare gli eventi a cui si è interessati e le azioni da eseguire quando l'evento si verifica. Le azioni che possono essere automaticamente scatenate sono ad esempio l'invocazione di una funzione Lambda, l'invocazione di un Run Command su EC2, la notifica di un topic SNS, la notifica verso una coda SQS, etc.

5.6.3 AWS SNS

Amazon **Simple Notification Service** (Amazon **SNS**) è un web service che permette di configurare, gestire e inviare messaggi di notifica dal Cloud. Esso fornisce agli sviluppatori la possibilità di pubblicare messaggi da un'applicazione, per poi consegnarli immediatamente ai "subscriber" oppure ad altre applicazioni, garantendo al tempo stesso elevata scalabilità, flessibilità e costi contenuti.

Oltre a poter configurare notifiche push dal Cloud verso dispositivi mobili, un altro uso tipico di SNS è quelli di inviare notifiche tramite SMS oppure email verso delle code SQS (vedi Amazon Simple Queue Service).

5.6.4 Implementazione dell'automatismo

L'automatismo è stato implementato sfruttando alcuni dei servizi offerti da AWS e una libreria di Python molto utilizzata in ambiente AWS (**Boto3**). La topologia di partenza consiste di due edge router, **flexiEdge-A** e **flexiEdge-B**, configurati nella stessa VPC ma all'interno di subnet poste in due Availability Zone (AZ) separate (vedi Figura 5-12). In particolare, flexiEdge-A ha le sue interfacce di rete nelle subnet LAN-A e WAN-A dell'**AZ-A**, mentre flexiEdge-B ha le sue interfacce nelle subnet analoghe poste nell'**AZ-B**.

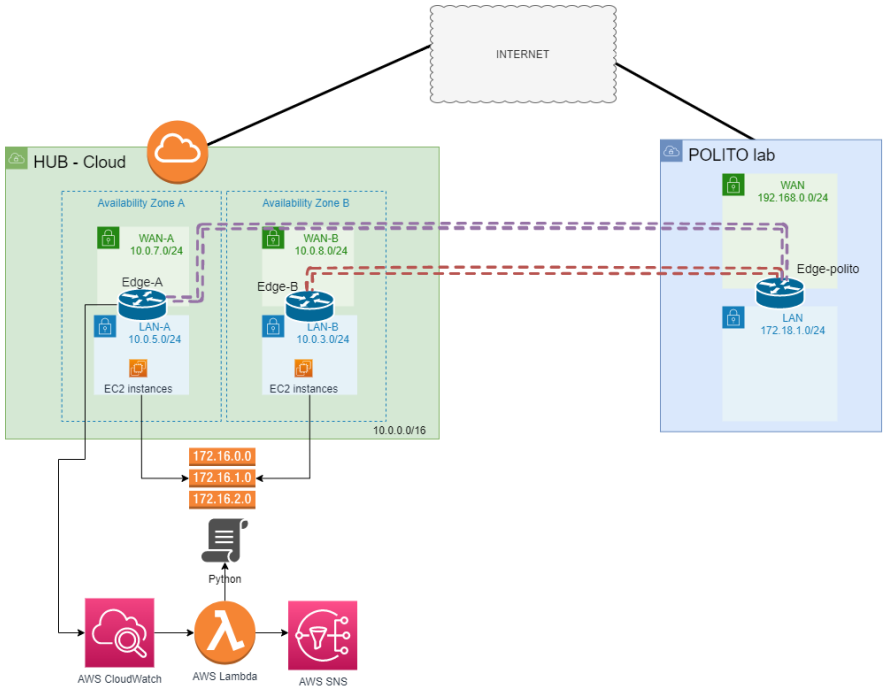


Figura 5-12: deployment multi-AZ con automatismo per la ridondanza dell'edge router

È importante sottolineare che le configurazioni dei due edge router (in termini di interfacce di rete, NAT, tunnel verso la rete on premise, etc.) devono essere esattamente le stesse, affinché quando il router di backup subentrerà a quello correntemente *active*, tutto il traffico continuerà a essere inoltrato come prima.

Anzitutto bisogna andare nel servizio **AWS Lambda** e creare una nuova funzione, selezionando una opportuna *runtime* (es. Python 3.9). Una volta creata la funzione, andiamo in **Function overview->Add trigger** per aggiungere un nuovo trigger, che sarà un evento CloudWatch.

Per creare l'evento andiamo in **AWS CloudWatch -> event rules** e creiamo una nuova regola per monitorare l'istanza EC2 del router active e far partire la funzione Lambda quando cambia lo stato dell'istanza. Per semplicità, creiamo una regola che si attiva ogniqualvolta lo stato dell'istanza è diverso da "running". Pertanto il meccanismo di failover si attiverà ogniqualvolta la funzione viene "innescata" dall'evento CloudWatch di "instance state change", ovvero quando flexiEdge-A passa dallo stato "running" a un qualunque altro stato (i.e. stopping, stopped, pending, …):

Figura 5-13 Creazione regola Cloudwatch per monitorare il router active

Una volta creato l'evento, sarà possibile aggiungerlo come trigger della funzione Lambda:

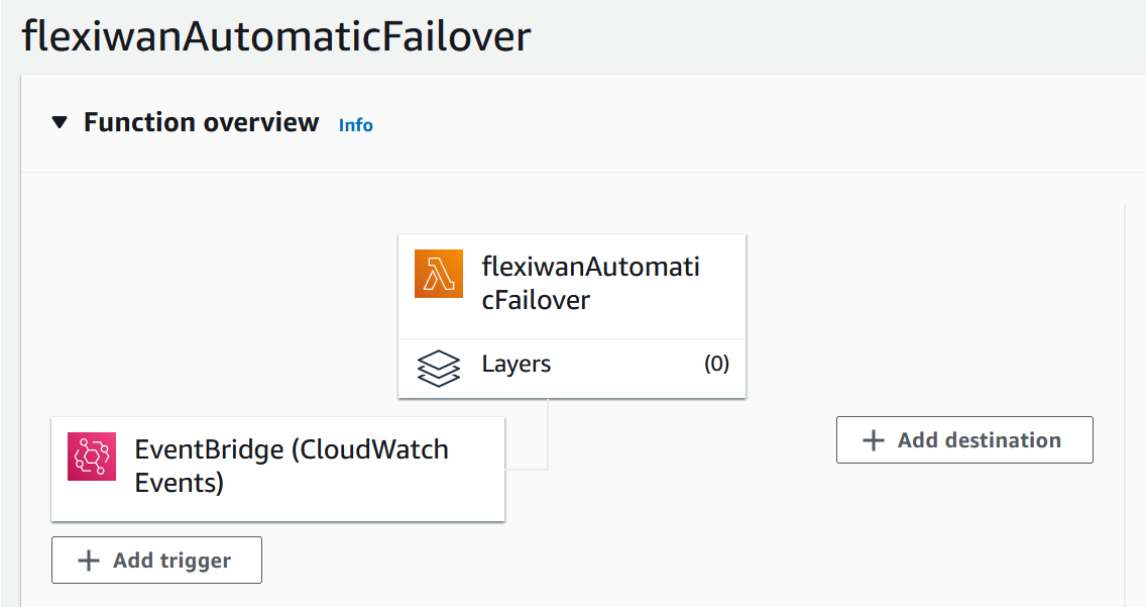


Figura 5-14 Impostazione del trigger della funzione Lambda

A questo punto andremo a scrivere il codice della funzione Lambda sfruttando Boto3, ovvero l'SDK ufficiale di AWS per Python che permette di creare, configurare e gestire i servizi AWS in maniera molto semplice tramite degli script.

La funzione andrà prima a selezionare tutte le entry nelle routing table delle subnet "interne" dei due router; in particolare è stata creata un'unica routing table, **LAN-RT**, associata sia a LAN-A che a LAN-B, dal momento che esisterà sempre un solo router active per gli host delle due LAN. Nello stato iniziale, prima che si inneschi il meccanismo di failover, la routing table sarà la seguente:

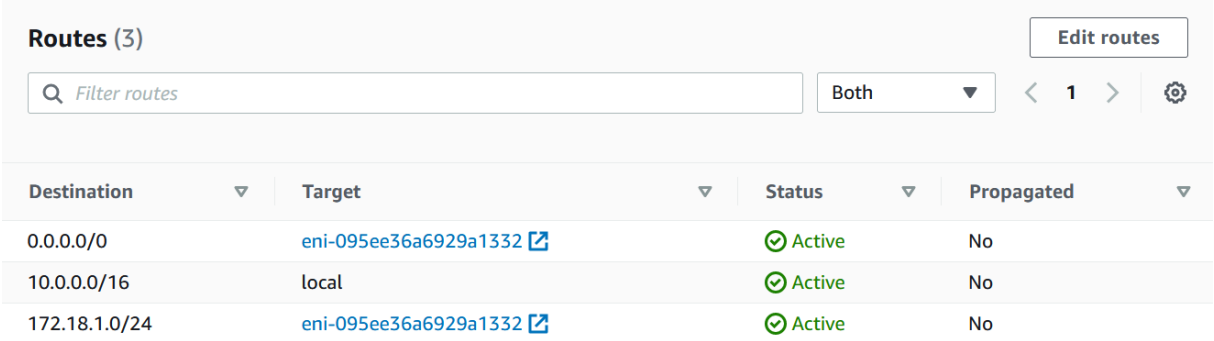


Figura 5-15 Tabella di routing della LAN prima del failover

Una volta ottenute le entry, che punteranno tutte all'interfaccia LAN di flexiEdge-A (**eni-095ee36a6929a1332**), bisognerà modificare il campo Target per far sì che puntino verso flexiEdge-B, ottenendo una nuova routing table, dove si evince che il nuovo router active è flexiEdge-B, e quindi il nuovo Target delle entry nella tabella sarà proprio la sua interfaccia LAN (**eni-00188941b16a73615**):

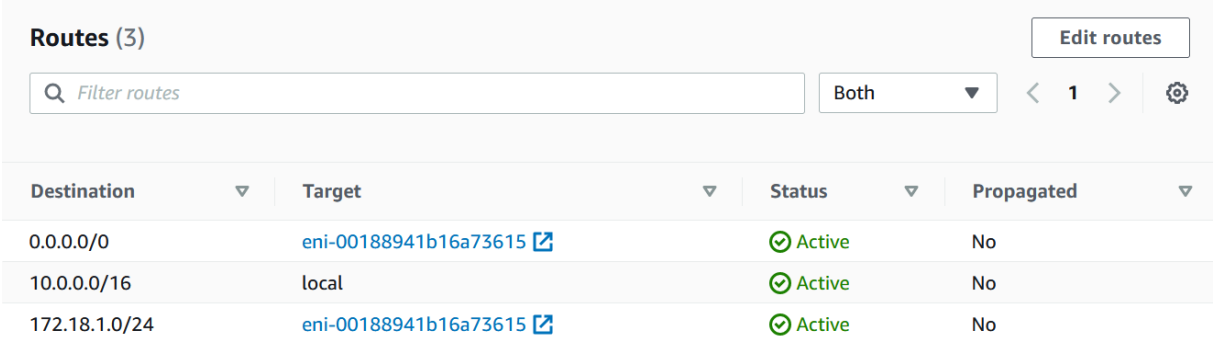


Figura 5-16 Tabella di routing della LAN dopo il failover

Prima che la funzione Lambda possa essere operativa, è necessario creare un ruolo e associargli gli opportuni permessi, tramite il servizio **AWS Identity and Access Management (IAM).** Ci sarà bisogno di due IAM Policy, una per far sì che la funzione abbia accesso agli eventi su Cloudwatch e un'altra per permettere alla funzione di leggere/scrivere le entry della routing table. Le due policy saranno quindi aggiunte ad un ruolo IAM da associare alla funzione Lambda.

Infine, è possibile ricevere delle notifiche al verificarsi del failover, utilizzando il servizio **AWS Simple Notification Service (SNS).** A tale scopo, bisognerà configurare un nuovo SNS Topic e aggiungerlo come Destination della funzione Lambda; gli utenti sottoscritti a quel topic saranno avvertiti (tramite email, SMS, etc.) dell'avvenuta esecuzione dell'operazione di failover dell'edge router, come mostrato in Figura 5-17.

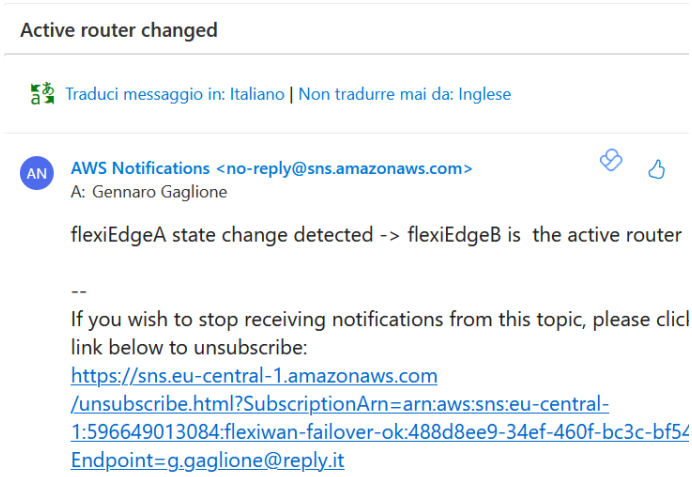


Figura 5-17 Ricezione di una notifica SNS (email) quando si verifica il failover

5.6.5 Calcolo del tempo di failover

Nella situazione iniziale il router "active" è flexiEdge-A, per cui tutto il traffico in ingresso alla VPC proveniente dalla rete on premise (POLITO) sarà inoltrato verso di lui attraverso il tunnel col router flexiEdge-POLITO.

I tunnel che sono stati instaurati tra le istanze SD-WAN, con i relativi dettagli sugli indirizzi IP (di loopback), sono i seguenti:

ID	Device A	Interface A	Device B / Peer	Interface B	Path Label	AVG Latency	Drop Rate	Encrypt	Adv.Options	Status	Actions
1	flexiEdge-A (Loopback: 10.100.0.4)	ens5 IP: 10.0.7.24:4789 Public: 35.156.4.169:4789	flexiEdge-POLITO (Loopback: 10.100.0.5)	ens5 IP: 172.18.254.238:4789 Public: 52.16.112.110:4789	Fiber	24.56ms	0.00 %	IKEv2	MTU: auto MSS Clamp: yes Routing: OSPF OSPF Cost: 100	Connected	
2	flexiEdgeB (Loopback: 10.100.0.6)	ens5 IP: 10.0.8.189:4789 Public: 3.69.177.216:4789	flexiEdge-POLITO (Loopback: 10.100.0.7)	ens5 IP: 172.18.254.238:4789 Public: 52.16.112.110:4789	Fiber	24.65ms	0.00 %	IKEv2	MTU: auto MSS Clamp: yes Routing: OSPF OSPF Cost: 100	Connected	

Dopo aver istanziato una macchina virtuale nella subnet LAN-A (IP: 10.0.5.188), ci proponiamo di effettuare un ping test da una macchina della LAN della rete on premise. La macchina 10.0.5.188 verrà raggiunta inizialmente passando per flexiEdge-A, come si evince dalla tabella di routing di flexiEdge-POLITO, visibile da flexiManage:

Destination	Gateway	Metric	Protocol
0.0.0.0/0	172.18.254.1	100	dhcp
10.0.3.0/24	10.100.0.6	20	ospf
10.0.5.0/24	10.100.0.4	20	ospf

Figura 5-18 Tabella di routing di flexiEdge-POLITO prima del failover

Dopodiché abbiamo simulato un guasto su flexiEdge-A (che può consistere banalmente nello stop della macchina virtuale). A questo punto, riceveremo una notifica SNS che ci segnalerà che il router primario non è più disponibile e verrà effettuato il failover, con la conseguente

modifica della tabella di routing associata alla LAN su AWS per puntare all'altro router. Di conseguenza, la tabella di routing di flexiEdge-POLITO, vista da flexiManage, diventa la seguente:

Destination	Gateway	Metric	Protocol
0.0.0.0/0	172.18.254.1	100	dhcp
10.0.3.0/24	10.100.0.6	20	ospf
10.0.5.0/24	10.100.0.6	20	ospf

Figura 5-19 Tabella di routing di flexiEdge-POLITO dopo il failover

Si evince chiaramente che adesso la subnet LAN-A (10.0.5.0/24) viene annunciata come raggiungibile passando per 10.100.0.6, ovvero per flexiEdge-B.

Il numero di pacchetti Echo Reply persi dall'istante in cui viene innescato il failover fino a quando il router secondario non prende il posto di quello principale, rendendo disponibile un nuovo percorso verso la destinazione finale, rappresenta proprio la misura del failover time (vedi Figura 5-20).

```
64 bytes from 10.0.5.188: icmp_seq=12 ttl=63 time=24.7 ms
64 bytes from 10.0.5.188: icmp_seq=13 ttl=63 time=24.6 ms
64 bytes from 10.0.5.188: icmp_seq=14 ttl=63 time=24.6 ms
From 10.100.0.5 icmp_seq=29 Destination Host Unreachable
From 10.100.0.5 icmp_seq=30 Destination Host Unreachable
From 10.100.0.5 icmp_seq=31 Destination Host Unreachable
From 10.100.0.5 icmp_seq=32 Destination Host Unreachable
From 10.100.0.5 icmp_seq=33 Destination Host Unreachable
From 10.100.0.5 icmp_seq=34 Destination Host Unreachable
From 10.100.0.5 icmp_seq=35 Destination Host Unreachable
From 10.100.0.5 icmp_seq=36 Destination Host Unreachable
From 10.100.0.5 icmp_seq=37 Destination Host Unreachable
From 10.100.0.5 icmp_seq=38 Destination Host Unreachable
From 10.100.0.5 icmp_seq=39 Destination Host Unreachable
From 10.100.0.5 icmp_seq=40 Destination Host Unreachable
From 10.100.0.5 icmp_seq=41 Destination Host Unreachable
From 10.100.0.5 icmp_seq=42 Destination Host Unreachable
From 10.100.0.5 icmp_seq=43 Destination Host Unreachable
From 10.100.0.5 icmp_seq=44 Destination Host Unreachable
From 10.100.0.5 icmp_seq=45 Destination Host Unreachable
From 10.100.0.5 icmp_seq=46 Destination Host Unreachable
From 10.100.0.5 icmp_seq=47 Destination Host Unreachable
From 10.100.0.5 icmp_seq=48 Destination Host Unreachable
From 10.100.0.5 icmp_seq=49 Destination Host Unreachable
From 10.100.0.5 icmp_seq=50 Destination Host Unreachable
From 10.100.0.5 icmp_seq=51 Destination Host Unreachable
From 10.100.0.5 icmp_seq=52 Destination Host Unreachable
64 bytes from 10.0.5.188: icmp_seq=54 ttl=63 time=25.4 ms
64 bytes from 10.0.5.188: icmp_seq=55 ttl=63 time=25.5 ms
64 bytes from 10.0.5.188: icmp_seq=56 ttl=63 time=25.4 ms
```

Figura 5-20 Calcolo del tempo di failover ottenuto con l'automatismo

Su una serie di cinque misurazioni successive, la media aritmetica del failover time è risultata essere:

$$(38 + 38 + 40 + 38 + 36) / 5 = 38 \text{ sec.}$$

Il tempo di failover ottenuto, pari a 38 secondi, rappresenta un downtime non trascurabile ma comunque comparabile con i tempi di convergenza di altri protocolli, sia di livello 2 come lo Spanning Tree (compreso tra 30 e 50 secondi), sia protocolli di livello 3 come OSPF (circa 40 secondi).

6 Conclusioni

La tecnologia SD-WAN viene concepita allo stesso tempo come l'applicazione più promettente dell'SDN (*Software Defined Networking*) ma anche come quella più sfidante sotto molti punti di vista. Infatti essa ha il potenziale di cambiare completamente il modo di concepire e organizzare l'infrastruttura WAN delle reti aziendali, permettendo di migliorarne sostanzialmente la latenza, l'impiego di banda e l'utilizzo di risorse.

Lo scopo che è stato perseguito durante la tesi è stato innanzitutto quello di sperimentare in prima persona la tecnologia SD-WAN; quindi, dopo averne studiato e analizzato tutte le caratteristiche, ci siamo soffermati su una specifica implementazione di SD-WAN, ovvero quella di *flexiWAN*, per via della sua natura open-source che lo differenzia dalle soluzioni SD-WAN degli altri vendor (per l'assenza appunto del cosiddetto "vendor lock-in") e lo rende particolarmente adatto a essere integrato con altri prodotti (es. un firewall esterno, software di terze parti, etc.) La parte centrale del lavoro è stata quindi quella di familiarizzare con questo prodotto e testarne le funzionalità in scenari diversi, con particolare attenzione all'integrazione col Cloud.

Ciò che sorprende maggiormente è la facilità di installazione di flexiwan, sia quella di tipo *bare metal* (ovvero su server fisici) sia quella su macchine virtuali nel Cloud, il che permette di ridurre il tempo necessario ad adottare una soluzione SD-WAN da parte di un'azienda. Inoltre, anche la gestione e il monitoraggio del sistema SD-WAN considerato si sono rilevati molto flessibili e facili da usare, grazie all'impiego di un'interfaccia grafica (*flexiManage*) che permette di imporre complesse configurazioni di rete con pochi semplici click (per es. abilitare i protocolli di routing sulle interfacce, instaurare tunnel VPN tra i nodi on premise e sul Cloud, creare policy per l'instradamento del traffico, etc.).

L'utilizzo dell'SD-WAN per connettere una rete on premise a cloud provider diversi si è dimostrato possibile, nonostante alcuni di essi presentassero delle incompatibilità con flexiWAN, per via ad esempio dell'utilizzo di un tipo di virtualizzazione non supportato (es. Microsoft Azure, che utilizza Hyper-V) per l'esecuzione di *flexiEdge* come router virtuale.

Per quanto riguarda il requisito del supporto di configurazioni ad alta affidabilità, si è scoperto che flexiWAN è in grado di supportarle solo in parte, rendendo quindi necessario progettare e implementare meccanismi alternativi per garantire a pieno tale requisito: nel nostro caso, è stata implementata un'automazione che sfrutta alcuni dei principali servizi AWS per realizzare il failover dell'edge router posto nella rete cloud. Tale automazione, peraltro, è strettamente legata all'infrastruttura di rete e ai servizi offerti dallo specifico cloud provider (AWS), e quindi potrebbe dover essere modificata notevolmente (in termini sia dei servizi cloud utilizzati sia della logica di funzionamento) passando ad un cloud provider differente.

Appendice: MetroEthernet

Introduzione e terminologia

Con il termine *MetroEthernet* si intende una serie di tecnologie di connettività WAN che hanno principalmente due caratteristiche in comune, ovvero:

- Ogni CPE è connesso alla rete del service provider tramite dei collegamenti fisici Ethernet (con le limitazioni dello standard Ethernet per quanto concerne la distanza massima raggiungibile, e.g. 5Km per Gigabit Ethernet);
- Viene fornito un servizio di connettività di livello 2, poiché il service provider inoltra frame Ethernet da un CPE all'altro, fornendo un'astrazione di "big L2 switch".

Consideriamo ad esempio il problema di collegare tre sedi remote di un'azienda fra di loro, ognuna con il proprio router CPE. Dal punto di vista del customer, per poter usufruire di un servizio MetroEthernet ogni sede deve potersi connettere al servizio con un cavo Ethernet, senza la necessità di dover collegarsi a ciascuno degli altri CPE. Dal punto di vista del service provider, questi dovrà costruire un'infrastruttura di rete che possa fornire un servizio di connettività MetroEthernet. Tipicamente il provider posiziona un suo switch nelle vicinanze delle sedi del customer, all'interno di un *point of presence* (PoP); questo switch dovrà essere quanto più vicino possibile ai router del customer, così che la distanza tra PoP e router sia minima e comunque compatibile con uno degli standard Ethernet (vedi Figura A-0-1).

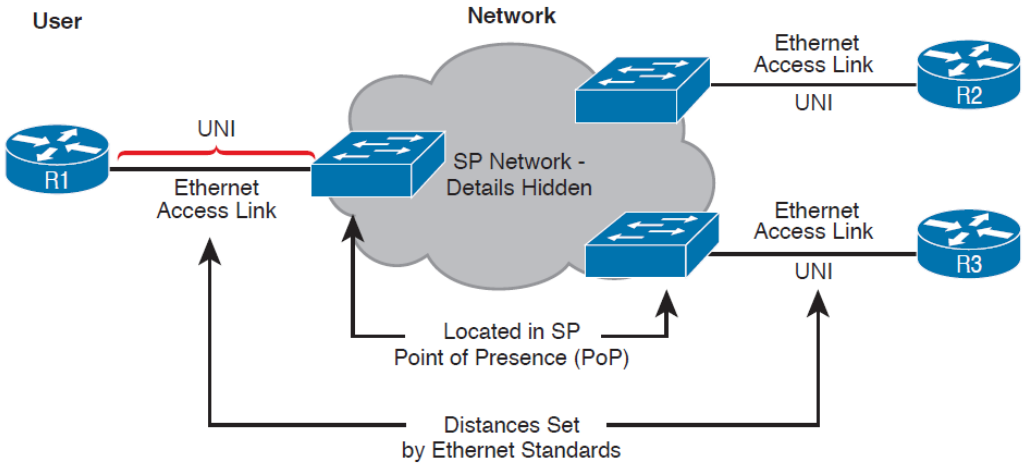


Figura A-0-1 MetroEthernet: schema di principio

I link fisici tra CPE e rete del provider sono detti *access link,* o anche *user network interface (UNI)*, perché rappresentano l'interfaccia tra il router del customer (user) e la rete del sercie provider. Come è evidente dalla figura, la rete del service provider è fondamentalmente ignota; ciò che viene offerto al customer è la garanzia di un servizio di connettività L2, ovvero l'inoltro di frame Ethernet da un punto all'altro della rete del provider, a seconda dei circuiti virtuali che vengono instaurati tra i CPE del customer.

Esistono diversi tipi di servizi MetroEthernet che possono essere forniti ad un customer, i quali si differenziano tra loro per le diverse topologie utilizzate, ciascuna volta a soddisfare particolari requisiti.

Ethernet Line Service (point-to-point WAN)

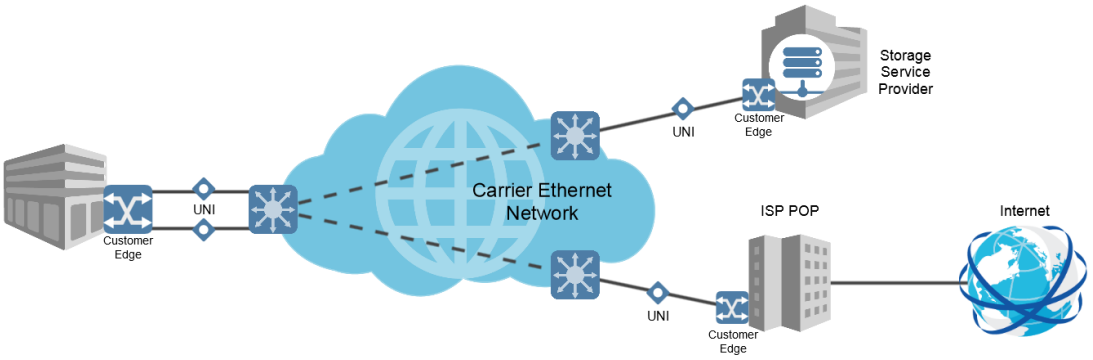


Figura A-0-2 Esempio di Ethernet Line Service

Ethernet Line Service è il servizio MetroEthernet più semplice possibile, in cui il customer collega i CPE di due sedi remote tramite un cavo Ethernet. Come per tutti i servizi MetroEthernet, la garanzia offerta dal servizio è quella di consegnare frame Ethernet dall'altra parte del cavo, come se idealmente i router dei due customer fossero collegati da un cavo crossover.

Secondo la definizione del MEF, un E-Line è un servizio per collegare solo una coppia di UNI alla volta, le quali possono comunicare soltanto tra di loro.

Con il termine *Ethernet Virtual Connection (EVC)* si definisce il circuito virtuale che viene creato per permettere la comunicazione tra due endpoint in un servizio MetroEthernet. Nel caso di Ethernet Line Service, viene creato un circuito punto-punto per ciascuna coppia di endpoint che si vuole far comunicare (vedi Figura A-0-2).

A livello di routing IP, i due router CPE si troveranno nella stessa subnet e stabiliranno un'adiacenza OSPF.

Un caso d'uso interessante è quello di una sede centrale (con il suo CPE) che deve essere collegata a un certo numero N di sedi remote (diciamo N = 50). Come abbiamo visto, con un servizio Ethernet Line puro, ci vorrebbero 50 interfacce del CPE della sede centrale, da collegare a ciascuna delle interfacce dei router delle sedi remote, una soluzione assai costosa e poco scalabile.

In alternativa, si potrebbe progettare la soluzione in maniera tale che:

- Il CPE della sede centrale utilizza un solo access link con elevata banda (es. 10Gbps)
- Dal CPE partono N=50 circuiti, uno per ciascun router remoto, tutti dalla stessa interfaccia
- Tutti i circuiti invieranno e riceveranno frame dallo stesso access link (vedi Figura A-0-3).

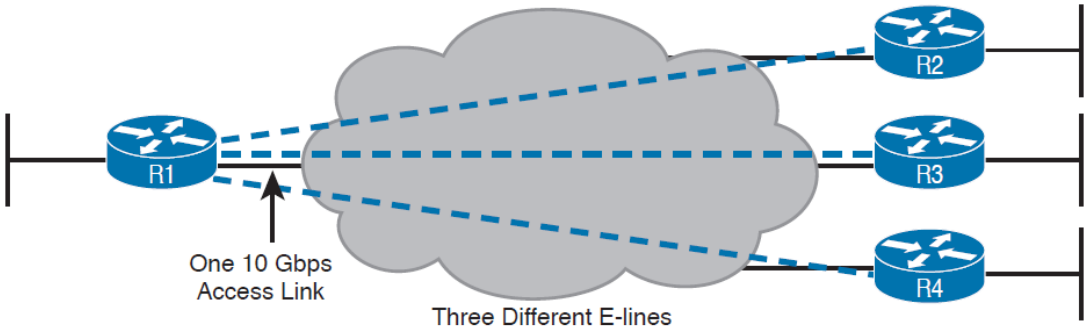
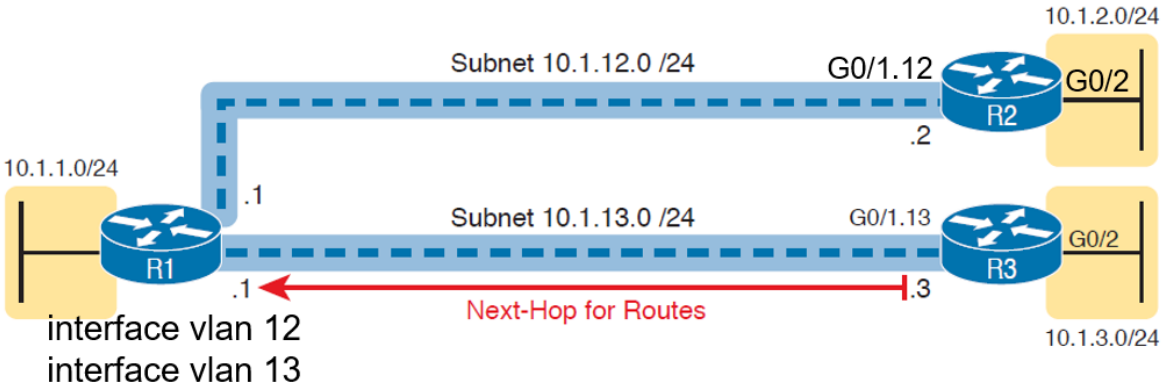


Figura A-0-3 Configurazione di E-Lines su singolo access link

Notiamo che per ottenere una soluzione simile, con più circuiti che partono dallo stesso access link, si potrebbe usare la tecnica del trunking 802.1Q, utilizzando un VLAN ID diverso per ciascun circuito; di conseguenza, il CPE della sede centrale dovrà essere configurato con tante *subinterface* quante sono le VLAN e i frame Ethernet inviati sul link apparterranno a un dato circuito a seconda del tag VLAN 802.1Q che portano con sé.



R2's routing table

C	10.1.2.0/24	G0/2
C	10.1.12.0/24	G0/1.12
O	10.1.1.0/24	10.1.12.1 (R1)
O	10.1.13.0/24	10.1.12.1 (R1)
O	10.1.3.0/24	10.1.12.1 (R1)

Figura A-0-4 Esempio di routing IP per le E-lines

Un altro aspetto interessante da comprendere è il funzionamento del routing IP in una topologia di questo tipo. In Figura A-0-4 è mostrato un esempio in cui si vede una tipica configurazione di rete (con i dettagli sull'assegnazione degli indirizzi, le subnet, etc.) per questa topologia

MetroEthernet; in particolare, è interessante analizzare le rotte OSPF all'interno della tabella di routing di uno dei router remoti (in questo caso R2).

Consideriamo la entry nella tabella di routing relativa alla subnet 10.1.1.0/24, che è la LAN su cui affaccia R1. Tale entry presenta come next-hop 10.1.12.1, che è l'indirizzo IP di R1 nella subnet che lo collega a R3 (passando per l'infrastruttura di rete L2, che però è trasparente a livello di routing IP). Pertanto, non stupisce che R2, per inviare un pacchetto IP a una subnet direttamente connessa a R1, debba passare per quest'ultimo.

Consideriamo adesso la entry relativa alla subnet 10.1.3.0/24; dal momento che R2 non può inviare direttamente un pacchetto IP a R2 (sono entrambi nodi foglia), è perfettamente lecito aspettarsi che R2 impari la rotta per 10.1.3.0/24 da R1 e che quest'ultimo rappresenti il next-hop per raggiungere la LAN di R3.

Ethernet LAN Service (full mesh)

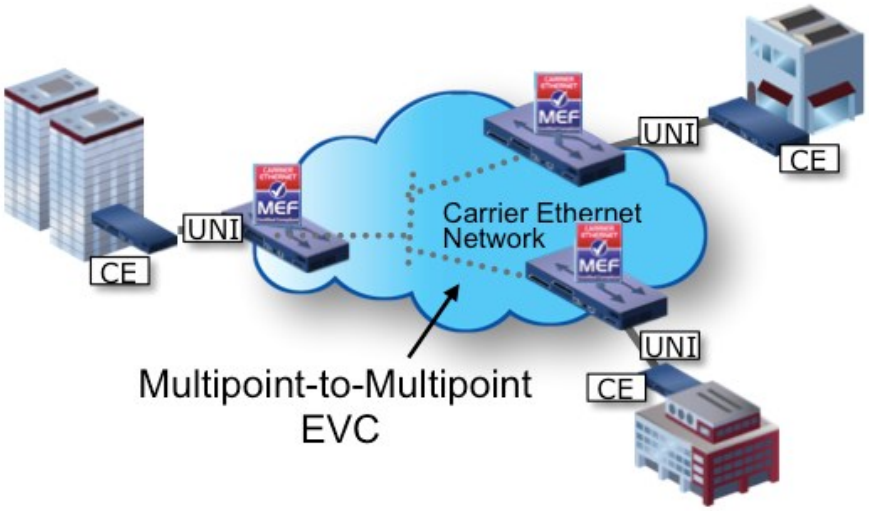


Figura A-0-5 Esempio di Ethernet LAN Service

Si consideri ora il caso di un'azienda che ha bisogno di collegare sedi diverse in modo che ogni sede possa inviare frame direttamente verso tutte le altre sedi (topologia *full mesh*). Se volessimo realizzare questa topologia utilizzando le E-Line, la soluzione non scalerebbe affatto, giacché il numero C di circuiti cresce molto velocemente al crescere del numero N di nodi da collegare. Per esempio:

$$N = 4\ sedi \rightarrow 6\ circuiti$$

$$N = 5\ sedi \rightarrow 10\ circuiti$$

$$N = 6\ sedi \rightarrow 15\ circuiti$$

...

$$N = 10\ sedi \rightarrow 45\ circuiti$$

E così via, seguendo la formula:

$$C = N * (N - 1)/2$$

Tuttavia, esiste un servizio MetroEthernet creato appunto per soddisfare una topologia di questo tipo, in cui ciascun router deve comunicare con tutti gli altri, proprio come accade in una LAN Ethernet; per questo motivo, il servizio in questione si chiama *Ethernet LAN service (E-LAN).*

Una E-LAN è definito dal MEF come un servizio *multipoint-to-multipoint* che permette di collegare fra loro un certo numero di UNI fornendo una connettività full mesh alle sedi del customer. Ogni UNI può comunicare con qualunque altra UNI connessa a quel servizio MetroEthernet

Dal punto di vista del routing IP, una E-LAN rappresenta una singola subnet IP in cui tutti i dispositivi (CPE) possono inviare frame tra di loro, proprio come se stessero sulla stessa LAN. Il servizio E-LAN permette dunque a ciascun CPE di inviare frame Ethernet a tutti gli altri, fornendo l'astrazione detta "big switch". Inoltre, ogni CPE vedrà gli altri come *OSPF neighbors* e scambierà informazioni di routing con questi. In Figura A-0-5 sono rappresentate tre sedi remote, con i rispettivi router, collegate fra di loro con un servizio E-LAN, quindi in full mesh.

Il termine *full mesh* indica una topologia in cui ciascuna coppia di nodi è collegata direttamente, in contrapposizione a *partial mesh*, che si riferisce a una topologia dove solo alcuni nodi comunicano direttamente.

Ethernet Tree Service (point-to-multipoint WAN)

Ethernet Tree service (E-Tree) è definito dal MEF come un servizio *rooted-multipoint* che collega un certo numero di UNI, fornendo alle corrispondenti sedi aziendali una connettività di tipo "hub and spoke": il CPE della sede centrale (detto "nodo root") può comunicare direttamente con i router delle sedi remote ("nodi leaf"), ma quest'ultimi non possono comunicare direttamente con il CPE centrale.

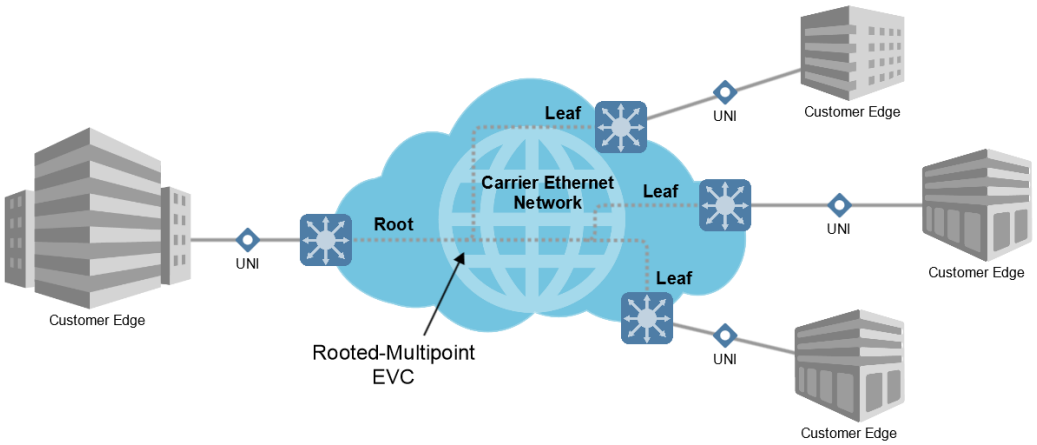


Figura A-0-6 Esempio di Ethernet Tree Service

In Figura A-0-6 viene mostrato un esempio di topologia, in cui il router di sinistra è il nodo root e può inviare frame verso tutti i router di destra, mentre quest'ultimi posso inviare frame solamente verso il nodo root. Notiamo ancora una volta come il CPE radice sia collegato con un solo link (sovradimensionato) da cui partono più circuiti virtuali verso ciascuno dei router leaf.

A livello di routing IP, anche in questo caso ci sarà una sola subnet per tutti i CPE, tuttavia il CPE root stabilirà delle adiacenze OSPF con tutti i CPE leaf, mentre quest'ultimi non stabiliranno adiacenze fra loro.

Bibliografia

Al-Dulaimi, A., Mumtaz, S., Al-Rubaye, S., Zhang, S., & I, C. «A Framework of Network Connectivity Management in Multi-Clouds Infrastructure.» *IEEE Wireless Communications*, 2019.

Arnold, Todd and Gürmeriçliler, Ege and Essig, Georgia and Gupta, Arpit and Calder, Matt and Giotsas, Vasileios and Katz-Bassett, Ethan. «(How Much) Does a Private WAN Improve Cloud Performance?» *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, 2020.

Carvajal, Jorge Martínez and Gilabert, Francisco Torrecillas and Cañadas, Joaquín. «Corporate network transformation with SD-WAN. A practical approach.» *Eighth International Conference on Software Defined Systems (SDS)*, 2021.

Diaz, C.J.M. et al. «Analysis about Benefits of Software-Defined Wide Area Network: A New Alternative for WAN Connectivity.» *International journal of advanced computer science & applications*, 2022.

Korsakov, S.V. and Sokolov, V.A. «On the Way to SD-WAN Solution.» *Modelirovanie i analiz informacionnyh sistem*, 2019.

Marco Iorio, Fulvio Risso, and Claudio Casetti. «When latency matters: measurements and lessons learned.» *SIGCOMM Comput. Commun. Rev.*, 2021.

Mine, Gao and Hai, Jiao and Jin, Luo and Huiying, Zhou. «A design of SD-WAN-oriented wide area network access.» *International Conference on Computer Communication and Network Security (CCNS)*, 2020.

Persico, V., Marchetta, P., Botta, A., & Pescapè, A. «Measuring network throughput in the cloud: The case of Amazon EC2.» *Computer Networks*, 2015.

Rajagopalan, S. «An Overview of SD-WAN Load Balancing for WAN Connections.» *4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, 2020.

Salazar-Chacón, G. «Hybrid Networking SDN and SD-WAN: Traditional Network Architectures and Software-Defined Networks Interoperability in digitization era.» *Journal of computer science and technology (La Plata)*, 2022.

Scarpitta, Carmine and Ventre, Pier Luigi and Lombardo, Francesco and Salsano, Stefano and Blefari-Melazzi, Nicola. «EveryWAn- An Open Source SD-WAN solution.» *International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, 2021.

Segeč, P. and Moravčik, M. and Uratmová, J. and Papán, J. and Yeremenko, O. «SD-WAN - architecture, functions and benefits.» *18th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, 2020.

Troia, Sebastian and Moreira Zorello, Ligia Maria and Maier, Guido. «SD-WAN: how the control of the network can be shifted from core to edge.» *International Conference on Optical Network Design and Modeling (ONDM)*, 2021.

Troia, Sebastian and Zorello, Ligia M. Moreira and Maralit, Alvin J. and Maier, Guido. «SD-WAN: An Open-Source Implementation for Enterprise Networking Services.» *22nd International Conference on Transparent Optical Networks (ICTON)*, 2020.

Wood, M. «How to make SD-WAN secure.» *Network Security*, 2017.

Yalda, Khirota Gorgees and Hamad, Diyar Jamal and Ţăpuş, Nicolae. «A survey on Software-defined Wide Area Network (SD- WAN) architectures.» *International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2022.

Zheyang, Qin. «SD-WAN for Bandwidth and Delay Improvements on the Internet,.» 2022.

Indice delle figure