Alma Mater Studiorum · Università di Bologna

SCUOLA DI INGEGNERIA E ARCHITETTURA

Corso di Laurea Magistrale in Ingegneria Informatica

ANALISI DI PERFORMANCE E SICUREZZA DI UN'ARCHITETTURA DI RETE PER INTERCONNESSIONE DI DATACENTER

Relatore:
Chiar.mo Prof.
Marco Prandini

Presentata da:
Riccardo Roveri

Sessione II
Anno Accademico 2023/2024

Indice

Capitolo 1

Introduzione

Negli ultimi anni, l'espansione esponenziale dei servizi digitali e delle infrastrutture di rete ha reso i datacenter un elemento centrale per il funzionamento di molte aziende e organizzazioni. Tuttavia, l'interconnessione tra questi datacenter (Data Center Interconnect, DCI) rappresenta una sfida crescente, poiché la necessità di scalabilità, sicurezza e prestazioni elevate diventa sempre più urgente. La crescente adozione di tecnologie come il cloud computing, il big data e l'intelligenza artificiale ha portato a un aumento senza precedenti della quantità di dati elaborati e trasferiti tra datacenter. Questa trasformazione ha creato la necessità di reti più complesse, capaci di garantire affidabilità e sicurezza, soprattutto in ambienti distribuiti. Un'interconnessione efficace tra datacenter permette alle organizzazioni di distribuire i carichi di lavoro su più sedi, migliorare la resilienza contro guasti e disastri, e mantenere operativa la propria infrastruttura anche in presenza di incidenti o attacchi informatici.

Uno degli elementi centrali che giustifica l'importanza di un'analisi approfondita delle architetture DCI riguarda la crescente dipendenza dalle infrastrutture IT per la business continuity. Il minimo downtime di un sistema può portare a danni significativi se impattano i sistemi più critici su cui facciamo affidamento. Per questo motivo, garantire una business continuity efficiente richiede reti robuste, ridondate e capaci di failover automatico tra datacenter. A questo si aggiunge l'importanza del disaster recovery, una pratica critica per mitigare le conseguenze di interruzioni operative a causa di eventi straordinari. La sicurezza ha un ruolo altrettanto importante nelle infrastrutture moderne che per motivi analoghi li ha resi un obiettivo di alto valore. Diventa quindi fondamentale avere una architettura che permetta di segmentare la rete e limitare la comunicazione tra le varie parti.

Nel contesto del public cloud, molte delle problematiche legate all'inter-

connessione dei datacenter, come la scalabilità, la ridondanza e la sicurezza, sono già state risolte dai principali provider di servizi cloud, come Amazon Web Services (AWS), Microsoft Azure e Google Cloud. Questi fornitori offrono infrastrutture globali altamente ottimizzate, con reti distribuite e tecnologie avanzate che garantiscono affidabilità, latenza minima e protezione contro le minacce informatiche. I datacenter nel public cloud sono progettati per gestire in modo nativo l'interconnessione, permettendo la mobilità fluida dei carichi di lavoro, il bilanciamento automatico del traffico, e l'integrazione di servizi di sicurezza avanzati come crittografia e microsegmentazione. Di conseguenza, gli utenti finali non devono occuparsi direttamente della complessità della gestione delle reti, poiché i provider cloud si occupano di tutti gli aspetti legati a prestazioni e sicurezza.

Tuttavia, nel private cloud, la gestione dell'interconnessione dei datacenter rimane una sfida importante che le aziende devono affrontare autonomamente. Laddove nel public cloud le soluzioni sono integrate e trasparenti, nel private cloud l'implementazione di infrastrutture DCI efficaci richiede una pianificazione accurata, configurazioni personalizzate e un controllo diretto sulle risorse fisiche e virtuali. Questo impone alle organizzazioni di bilanciare esigenze di sicurezza, prestazioni e costi, senza potersi affidare a soluzioni standardizzate preconfezionate. Di conseguenza, l'analisi delle architetture di interconnessione nel private cloud diventa cruciale per garantire lo stesso livello di affidabilità e protezione offerto dai provider di public cloud, ma con maggiore controllo e flessibilità operativa, elementi fondamentali per molte realtà aziendali che gestiscono dati sensibili o necessitano di infrastrutture su misura.

1.1 Sfide principali

L'utilizzo di datacenter in un contesto private cloud pone diverse sfide tra cui le principali sono performance, sicurezza e business continuity.

1.1.1 Performance

I datacenter vengono utilizzati per la maggior parte dei servizi è quindi importante garantire performance adeguate che possano sostenere il workload. Verranno analizzati alcuni KPI (Key Performance Indicator) che permetteranno di identificare quale architettura riesce a garantire la qualità di servizio richiesta dai vari servizi. Gli obiettivi di QoS (Quality of Service) vengono misurati sia in condizioni normali che in caso di guasti per assicurare la re-

silienza del sistema. Spesso i datacenter private cloud non sono progettati per essere interconnessi tra loro fin dall'inizio, come nel caso studio analizzato, portando a necessitare maggiore attenzioni alla latenza che può raggiungere anche le decine di millisecondi. La maggior latenza è dovuta sia alla distanza che spesso alla mancanza di un link dedicato tra i due che ne limita anche la banda.

1.1.2 Business continuity

Nonostante le ridondanze da guasti all'interno dei DC, rimane il rischio di un guasto logico oppure di molteplici guasti portando alla non disponibilità dell'intero DC. L'utilizzo di un secondo datacenter permette di continuare l'operatività dei sistemi più critici e per questo viene spesso impiegato per garantire business continuity. Garantire un ambiente medesimo dei server in entrambi i datacenter richiede tecnologie l'impiego di tecnologie VPN che creano una rete uniforme verso i server indipendentemente dal DC.

1.1.3 Sicurezza

La sicurezza all'interno dei DC sta diventando sempre più centrale richiedendo una segmentazione sempre più granulare dei vari sistemi. In passato, la sicurezza della rete si concentrava principalmente sul proteggere la connessione tra i client e i server, con firewall che agivano come barriera per impedire accessi non autorizzati o il passaggio di dati sensibili. Tuttavia, con l'evoluzione delle minacce, come i movimenti laterali degli attaccanti (lateral movement) all'interno della rete dopo un'infiltrazione iniziale, è diventato evidente che non basta proteggere la frontiera tra client e server. Ora, è necessario estendere le protezioni anche tra i vari server stessi all'interno del datacenter. L'utilizzo di NGFW (Next-Generation Firewall) permette di utilizzare anche tecnologie di packet inspection per avere un controllo ancora maggiore sulle connessioni ad esempio dando la possibilità di bloccare il traffico in base a firme di attacchi noti.

1.1.4 Obiettivo

Le singole sfide legate alla sicurezza, alla segmentazione della rete, e alle prestazioni nei datacenter sono già state ampiamente trattate nella letteratura accademica e implementate in soluzioni commerciali da numerosi fornitori di tecnologia. Ad esempio, la segmentazione della rete è un concetto ben consolidato, con approcci come VLAN, VXLAN e la microsegmentazione

che hanno permesso di isolare i diversi segmenti di rete per limitare la diffusione di eventuali attacchi. Allo stesso modo, la sicurezza dei datacenter ha beneficiato di tecnologie avanzate come firewall di nuova generazione (NGFW), sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS), e crittografia end-to-end, che sono diventati standard nelle implementazioni aziendali. Anche il miglioramento delle prestazioni è stato affrontato tramite tecniche come il load balancing, la ridondanza dei server e l'utilizzo di tecnologie SDN (Software-Defined Networking) per ottimizzare il traffico di rete e garantire la qualità del servizio (QoS).

Tuttavia, queste soluzioni, pur essendo ampiamente adottate e sperimentate singolarmente, spesso non riescono a fornire un'integrazione armoniosa che risolva contemporaneamente tutte le sfide in modo coordinato e ottimale. Ad esempio, una soluzione che migliora le prestazioni della rete potrebbe complicare la gestione della sicurezza o viceversa. Questo è il motivo per cui molte implementazioni aziendali finiscono per adottare una combinazione di tecnologie diverse, con conseguenti compromessi tra sicurezza, performance e facilità di gestione. La sfida più complessa e cruciale è trovare un'architettura unificata che sia in grado di affrontare simultaneamente tutte e tre le aree: sicurezza, prestazioni e gestione della rete. Questa tesi si propone di colmare questo vuoto, esplorando una soluzione architetturale integrata che non solo affronti ciascuna sfida singolarmente, ma che armonizzi e ottimizzi il loro funzionamento combinato. L'obiettivo è quello di progettare un'infrastruttura capace di fornire elevati livelli di sicurezza e segmentazione senza sacrificare le prestazioni della rete o la facilità di gestione.

1.2 Caso studio

La scelta di un caso studio all'interno di questa tesi riveste un'importanza centrale per diverse ragioni. In primo luogo, esso consente di validare in modo pratico le soluzioni architetturali proposte, applicando i concetti teorici a uno scenario reale. Questo approccio pratico è cruciale per testare l'efficacia e la fattibilità delle diverse architetture di interconnessione per datacenter, poiché permette di osservare come tali scelte si comportano in un contesto operativo concreto. L'analisi di un caso studio offre la possibilità di approfondire le complessità e le sfumature che potrebbero sfuggire a modelli generici, fornendo una visione dettagliata su aspetti fondamentali come le prestazioni, la scalabilità e la sicurezza. Inoltre, il caso studio fornisce un quadro contestuale che aiuta a comprendere come i vari elementi dell'architettura interagiscono in un ambiente reale, evidenziando le sfide e le limitazioni che non sempre emergono in un'analisi astratta. Dimostrare l'applicazione

delle scelte architetturali nel contesto del caso studio rafforza ulteriormente la tesi, non solo mostrando le soluzioni possibili, ma evidenziando come e perché esse siano efficaci all'interno di un dato contesto.

Va sottolineato, tuttavia, che l'adozione di un caso studio non limita la generalizzabilità del lavoro. Sebbene si tratti di un'analisi legata a un'istanza specifica, i principi, le metodologie e le conclusioni tratte da questa analisi possono essere estese e applicate a una varietà di scenari con caratteristiche simili. Il caso studio scelto rappresenta un esempio di sfide comuni e ambienti tipici nel campo dell'interconnessione dei datacenter, rendendo le soluzioni proposte rilevanti per un ampio spettro di situazioni. Inoltre, i risultati empirici del caso studio possono fornire una base per la costruzione di teorie e modelli più generali. Attraverso una chiara distinzione tra gli aspetti unici del caso specifico e quelli di portata più ampia, questa tesi contribuisce a creare un quadro di riferimento applicabile a un contesto più ampio, mantenendo così la rilevanza accademica e pratica delle soluzioni proposte.

Capitolo 2

Analisi dei requisiti

La varietà di architetture di rete attualmente presenti è dovuta alla grande differenza di requisiti e limitazioni di ogni realtà. I requisiti e le necessità di un provider a livello nazionale oppure una piccola realtà sono molto differenti. Inoltre le reti non sono entità statiche ma bensì crescono e cambiano nel tempo in base alle necessità dell'organizzazione. Questo comportamento può portare ad avere situazioni in cui la configurazione non risulta ottimale ma è la conseguenza dell'evoluzione della rete stessa dato che risulta solitamente dispendioso una riprogettazione totale in termini di costi e impatto ai servizi.

In questo capitolo verranno stabiliti quali sono i requisiti e le limitazioni imposti dalla attuale configurazione. Stabilire questi requisiti ci permetterà successivamente di valutare e scegliere la miglior infrastruttura.

2.1 Requisiti di performance

I requisiti di performance sono definiti attraverso indicatori chiave di prestazione (Key Performance Indicators, KPI), quali latenza, packet loss e throughput. Questi parametri sono fondamentali per valutare l'efficienza operativa della rete in contesti distribuiti.

2.1.1 Affidabilità

L'affidabilità si misura come il rapporto tra il tempo in cui la rete è operativa e il tempo totale, ma la valutazione precisa di questi parametri non è sempre semplice. Occorre tenere conto che la rete in considerata è geograficamente distribuita e non tutte le sue componenti hanno la medesima

importanza. Ad esempio, l'inaccessibilità della parte dedicata al disaster recovery avrà un impatto molto diverso rispetto a quella del sito di produzione attivo. Per ottenere una misura accurata, sarebbe ideale monitorare l'affidabilità in tutti i punti della rete, ma questa soluzione risulta poco pratica data l'estensione della rete. Per questi motivi è necessario fare un'analisi che va oltre il singolo valore e che invece prendere in considerazione come i vari scenari di guasto vadano ad impattare il corretto funzionamento della rete.

2.1.2 Quality of Service

Parlando dell'affidabilità è importante decidere come valutare se un segmento di rete è effettivamente degradato. Per farlo anche in questo caso dobbiamo utilizzare metriche differenziate in base all'uso di quel specifico segmento. Ad esempio la comunicazione tra un database ed un server applicativo ha requisiti differenti rispetto a quella tra un client ed un server web. Le due principali metriche che possiamo usare per misurare questo degrado sono il packet loss e la latenza.

Packet Loss
Il packet loss rappresenta il rapporto tra i pacchetti persi e il numero totale di pacchetti inviati. Solitamente è causato da una saturazione della rete oppure a problemi degli apparati di rete stessi. Questo fenomeno è più comune su reti geografiche o su internet, dove la banda disponibile è spesso più limitata rispetto alle reti locali (campus), che hanno generalmente capacità maggiori grazie ai costi inferiori della loro realizzazione.

Latenza
La latenza misura il tempo, espresso in millisecondi, che un pacchetto impiega per essere inviato e ricevuto tra due host (round trip time). In questo contesto, la latenza è una metrica particolarmente rilevante, poiché molte applicazioni, soprattutto quelle più datate, sono estremamente sensibili a aumenti di latenza anche di pochi millisecondi. Mantenere bassa la latenza è cruciale nelle comunicazioni tra server, soprattutto ora che molte architetture stanno passando da sistemi monolitici a microservizi. Questo implica che i servizi possono dover comunicare tra datacenter diversi, rendendo il controllo della latenza ancora più importante.

2.2 Requisiti di sicurezza

La sicurezza di rete ha un ruolo fondamentale nella protezione delle organizzazioni da conseguenze potenzialmente devastanti degli attacchi informatici. Comprende diverse tecnologie, protocolli e misure progettate per rilevare, prevenire e limitare accessi non autorizzati che possono portare ad una compromissione dei sistemi [21]. In particolare la sicurezza di rete mira a difendere l'integrità dei dati e dei sistemi critici ponendosi tra essi ed un potenziale attaccante. Per ottenere queste caratteristiche è importante studiare un infrastruttura che dia modo di utilizzare gli strumenti all'interno della rete.

2.2.1 Firewall

Lo scopo di un firewall è quello di ispezionare il traffico ip e decidere, in base alle policy al suo interno, se consentirne o meno il passaggio. Rappresenta lo strumento principale che ci permette di isolare i dispositivi permettendo solo le comunicazioni autorizzate. Solitamente questi dispositivi sono anche dotati di funzionalità UTM (Unified Threath Managment) e possono svolgere funzioni di IDS/IPS, SSL inspection e web filtering. Poiché il traffico IP deve necessariamente passare attraverso il firewall per l'applicazione delle politiche di sicurezza, esso può essere configurato come gateway di rete o collegato a diverse VRF (Virtual Routing and Forwarding) per mediare le comunicazioni tra di esse. Data l'importanza dei firewall è cruciale che vengano posizionati correttamente all'interno della rete in modo da dare il massimo grado di sicurezza. Idealmente infatti ogni comunicazione dovrebbe essere esplicitamente consentita, soluzione che risulta però spesso impraticabile.

2.2.2 Segmentazione

La segmentazione di rete consente di suddividere i dispositivi in categorie distinte in modo tale che la comunicazione tra di essi avvenga tramite firewall. In reti di piccole dimensioni possiamo configurare il gateway della rete sul firewall stesso, architettura non scalabile nel caso di grandi reti. In contesti più ampi, come le reti campus, intere categorie di dispositivi vengono assegnate a diverse VRF, e il firewall gestisce il traffico tra le di esse, garantendo maggiore flessibilità nella gestione e modifica delle reti.

2.3 Requisiti di gestione

I requisiti di gestione comprendono una serie di requisiti non funzionali, volti a garantire un'efficace gestione operativa quotidiana della rete. Questi requisiti sono strettamente collegati a quelli di sicurezza, poiché ne assicurano il mantenimento e l'applicazione nel tempo.

2.3.1 Regole firewall

Considerando la complessità delle reti moderne e il crescente numero di regole è indispensabile avere un sistema centralizzato per la gestione delle policy firewall. Chi si occupa della gestione delle policy, come i consulenti esterni, potrebbe non avere una conoscenza approfondita della rete aziendale. Per questo motivo, il sistema deve essere in grado di creare nuove regole firewall in modo intuitivo, evitando errori e assicurando che le policy vengano applicate correttamente. In presenza di più firewall, non è sempre evidente su quali dispositivi applicare le policy, quindi è necessario disporre di misure preventive che impediscano la creazione di regole errate o inefficaci.

2.3.2 Segmentazione

In un contesto di sicurezza, la segmentazione della rete è fondamentale per filtrare le comunicazioni tramite firewall. In ambienti di piccole dimensioni, con una singola sede, la creazione di nuove subnet è relativamente semplice, ma nelle reti estese geograficamente la situazione diventa più complessa. È necessario configurare il routing in modo che il nuovo segmento di rete sia accessibile da qualsiasi punto della rete stessa. Alcune soluzioni non offrono la flessibilità necessaria per creare nuovi segmenti in maniera agile richiedendo l'intervento del provider, rallentando l'operazione e generando un carico operativo che può diventare insostenibile.

2.4 Business continuity e DR

Nell'attuale contesto globale, le organizzazioni sono esposte a potenziali interruzioni causate da disastri naturali, attacchi informatici o guasti ai sistemi. Questi eventi possono generare impatti devastanti, comportando danni operativi, finanziari e di reputazione. La dipendenza critica dai sistemi tecnologici rende particolarmente gravi le conseguenze di tali interruzioni, ad esempio l'impossibilità di accedere a dati sanitari o il blocco di una linea

produttiva. Per ridurre al minimo i tempi di inattività e prevenire perdite di dati significative, è fondamentale disporre di un piano di business continuity.

BCMS (Business Continuity Management System) è la gestione di queste strategie che ci permettono di mantenere il servizio attivo o con minime interruzioni. Questo processo deve essere in grado di valutare l'impatto dei vari componenti in modo da identificarne gli elementi di criticità e avere un piano di ripristino adeguato. A testimonianza dell'importanza di questi sistemi, la norma ISO 22301 fornisce un quadro di riferimento per la gestione del BCMS [19] [7].

2.4.1 Disaster Recovery

La business continuity (BC) è un concetto generale che si riferisce alla capacità di mantenere operativi i sistemi più critici anche in condizioni eccezionali. DR (disaster recovery) è un sottoinsieme della BU che permette a fronte di questi eventi di riprendere il servizio nel breve termine ma con una parziale perdita di dati. Sono presenti tecniche e framework specifici per la gestione di questi eventi, che spesso data la loro estensione richiedono spesso interventi molto invasivi e manuali [33].
Ad esempio, il disaster recovery può essere implementato tramite la replica dei dati tra due data center. Se il data center principale diventa inaccessibile per un periodo prolungato, viene attivato un failover sul sito secondario. Tuttavia, poiché i dati nel sito secondario potrebbero non essere aggiornati, è necessaria una successiva riconciliazione dei dati una volta risolto il problema.

2.4.2 Business Continuity

Definiamo la BC in senso stretto come la capacità di mantenere il funzionamento dei servizi a fronte di guasti, mantenendo lo stato coerente. Richiede sistemi di failover automatici e una costante sincronia dei dati tra i due siti dati i brevi tempi di reazione richiesti.
La gestione della ridondanza viene spesso fatta a livello infrastrutturale, necessità quindi che entrambi i siti si comportino uniformemente creando un overlay network che è indipendente dal sito reale. Questa caratteristica della BC la rende particolarmente complessa da implementare, richiedendo un control plane in grado di gestire i due siti e un underlay network in grado di mantenere la latenza bassa. Dato che gli indirizzamenti ip rimangono i medesimi è anche necessario fare correttamente routing nelle VRF geografiche per indirizzare il traffico al DC corretto.

2.4.3 Confronto

Sebbene sia la business continuity che il disaster recovery vengano gestiti a livello di sistema o applicazione, è essenziale che l'infrastruttura di rete supporti adeguatamente il comportamento richiesto dalle applicazioni.
Nel caso della BC, i server devono operare in un ambiente di rete uniforme tra i vari data center. Questo requisito, combinato con la necessità di mantenere una bassa latenza, rappresenta una delle sfide più stringenti di questa architettura.
Nel caso del disaster recovery, le operazioni sono manuali e comportano una certa tolleranza ai disservizi. Tuttavia, è cruciale che l'infrastruttura sia il più indipendente possibile da attori esterni, come descritto nella sezione 2.3.2. I requisiti in questo caso sono poco stringenti in quanto il sistema di produzione e di DR sono completamente distinti, con indirizzamenti differenti per poter essere più indipendenti possibili.

Capitolo 3

Architettura attuale

Per valutare un'evoluzione della attuale architettura è necessario analizzarla in modo da poter valutarne le caratteristiche dopo la sua evoluzione.

3.1 Rete campus

La rete campus più grande e rilevante è quella della sede principale, oltre alle reti al suo interno sono presenti anche le interconnessioni con i datacenter e le sedi periferiche. Il core della rete è composto da due router, denominati cs1 e cs2, ciascuno configurato con più VRF (VPN Routing and Forwarding tables, come descritto in [30]). Il protocollo OSPF (Open Shortest Path First [11]) viene utilizzato per il routing interno, mentre il BGP [29] gestisce il routing esterno. Per filtrare il traffico verso le altre sedi ed il datacenter è installata una coppia di firewall, nominati fw1 ed fw2, mentre per l'interconnessione con internet è presente un'altra coppia di firewall denominati fwint1 e fwint2.
Il routing tra le sedi periferiche e quella principale viene effettuato tramite la rete MPLS [36] del provider, utilizzando router dedicati in ogni sede (CPE), i quali comunicano tramite OSPF [24] con i router di sede (CE).
All'interno della sede principale le reti vengono terminate da una coppia di router per ogni edificio che a loro volta sono bi-attestati con cs1 e cs2. Il routing anche in questo caso viene gestito tramite OSPF utilizzando un'unica area. Per mantenere comunque segmentazione anche all'interno di questa rete campus sono presenti diverse VRF che mantengono divisi i domini di routing, ad esempio separando pc client da apparati medicali. La comunicazione tra queste VRF passa attraverso fw1/2 che permettono di filtrare il traffico, dando la possibilità quindi di isolare i domini di routing permetten-

do solo le comunicazioni volute. Il risultato è la presenza di diverse istanze OSPF, una per ciascuna VRF, in cui le reti dei vari edifici vengono apprese dinamicamente. Le reti vengono poi indirizzate verso i firewall utilizzando la rotta di default per internet mentre tramite rotte statiche per raggiungere le altre VRF.

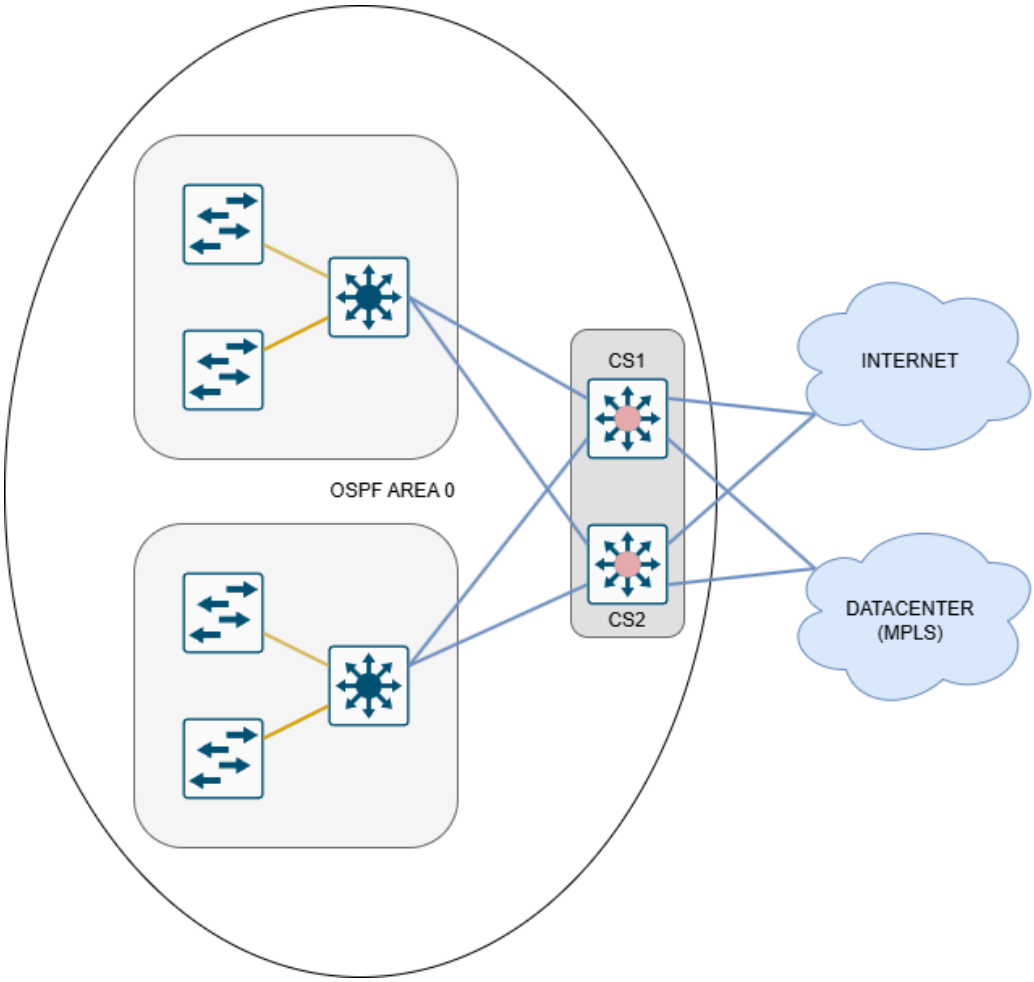

Figura 3.1: Schema rete Campus

3.2 Rete geografica

La comunicazione a livello geografico tra la sede principale e l'esterno avviene verso tre tipologie di entità distinte: internet, datacenter, aziende

partner. Ciascuna di queste comunicazioni avviene in modo differenziato per soddisfare i rispettivi requisiti.

3.2.1 Comunicazione verso internet

La comunicazione verso internet avviene tramite due connettività dedicate di due provider differenti, necessitando di due classi di indirizzi pubblici diversi. L'interconnessione con ciascun provider avviene tramite una coppia di CPE che effettua peering BGP con i router interni cs1 e cs2, all'interno di una VRF dedicata. Questo approccio garantisce ridondanza sia tra i provider che tra ciascun provider e la rete interna, mantenendo flessibilità grazie al routing dinamico. Per gestire il traffico internet, sono presenti due firewall dedicati (fwint), ciascuno con interfacce sia sulla VRF interna che sulle due VRF dedicate a Internet.
I servizi esposti internet vengono gestiti principalmente con un WAF (web application firewall) verso cui vengono indirizzati direttamente gli ip pubblici, il resto dei servizi invece viene gestito dai firewall tramite DNAT. Per gestire più blocchi di indirizzi pubblici, sono state configurate policy SNAT, che consentono di instradare correttamente il traffico in uscita verso il provider appropriato. Considerata l'importanza e i rischi di sicurezza legati alla comunicazione verso Internet, oltre alle normali policy firewall, è stato implementato un proxy aziendale che filtra gli URL accessibili. Il traffico SSL viene ispezionato grazie alle funzionalità di SSL inspection dei firewall mentre il resto del traffico non http viene sottoposto ad un IDS. Poiché sono necessari molti componenti per garantire la sicurezza di questa comunicazione, anche le sedi periferiche e il datacenter utilizzano queste connettività Internet, passando attraverso la rete MAN aziendale. Solitamente, questo compromesso in termini di latenza è accettabile per le applicazioni che devono comunque accedere a Internet, che è per sua natura best-effort.

3.2.2 Comunicazione verso il datacenter

L'interconnessione verso i datacenter è la più importante in quanto al loro interno sono presenti tutti i servizi critici per il funzionamento dell'organizzazione. Come per la comunicazione con internet è presente routing dinamico tramite BGP con 2 peering per CPE con rispettivamente cs1 e cs2 in modo da fornire ridondanza nel caso di guasto di un router sia del provider che interno. Le rotte annunciate alle CPE sono provenienti dall'istanza OSPF della VRF interna che vengono ridistribuite nel BGP e poi filtrate tramite l'utilizzo di prefix-list. Nei datacenter invece non sono presenti router di proprietà ed è

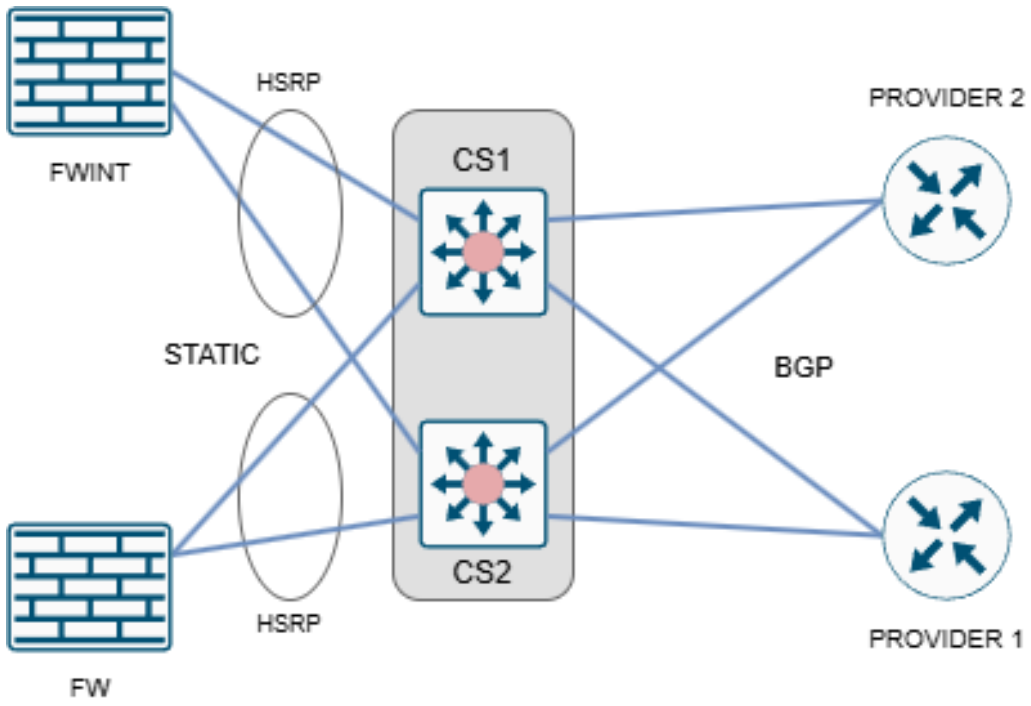

Figura 3.2: Schema rete internet

presente solo una coppia di firewall per datacenter, che però non hanno BGP configurato. Il routing avviene tramite rotte statiche che vengono inserite dal provider sui propri router per poter annunciare le reti di datacenter sul firewall sono poi presenti delle statiche per instradare dal datacenter verso le altre sedi. La creazione di una nuova rete richiede l'aggiunta di una rotta sul router del provider richiedendo un coinvolgimento del provider, creando una dipendenza da esso e un allungamento dei tempi di creazione di una rete.

Nel datacenter non sono presenti server di proprietà ma il provider offre un servizio IaaS in cui mette a disposizione dei server fisici in cui il cliente effettua la virtualizzazione. L'infrastruttura di rete all'interno è piatta e composta da diverse subnet con il gateway sul firewall, queste reti tramite vlan vengono trasportate dal provider fino ai corretti server.

3.2.3 Comunicazione verso organizzazioni partner

Un'ulteriore comunicazione fondamentale è quella verso le organizzazioni partner, che spesso richiedono un canale di comunicazione privilegiato. Nel

contesto della pubblica amministrazione, è comune la necessità di comunicare in modo preferenziale con altre entità sul territorio, per esempio per accedere ai servizi regionali. Anche per le aziende private, può essere utile far parte di un consorzio che richiede flussi di dati per favorire la collaborazione. In questo caso studio è il provider stesso che permette questa comunicazione tramite l'utilizzo di diverse VRF che coinvolgono aziende diverse in base agli scopi. L'interconnessione con queste VRF avviene allo stesso modo di quella per il datacenter essendo tutte gestite dallo stesso provider.

Il routing verso e da queste VRF è gestito in maniera distinta nella sede principale rispetto ai datacenter. Nella sede principale sono presenti altri peering BGP con il provider in VRF differenti, che passano tramite fw1/fw2 per accedere al resto della rete. Nel datacenter invece oltre che una rete di trasporto per la VRF interna sui firewall di datacenter sono presenti altre interfacce collegate alle VRF geografiche tramite reti di trasporto verso i router del provider. Quando la comunicazione avviene tra due organizzazioni situate nello stesso datacenter, il traffico rimane all'interno del datacenter, riducendo così al minimo la latenza.

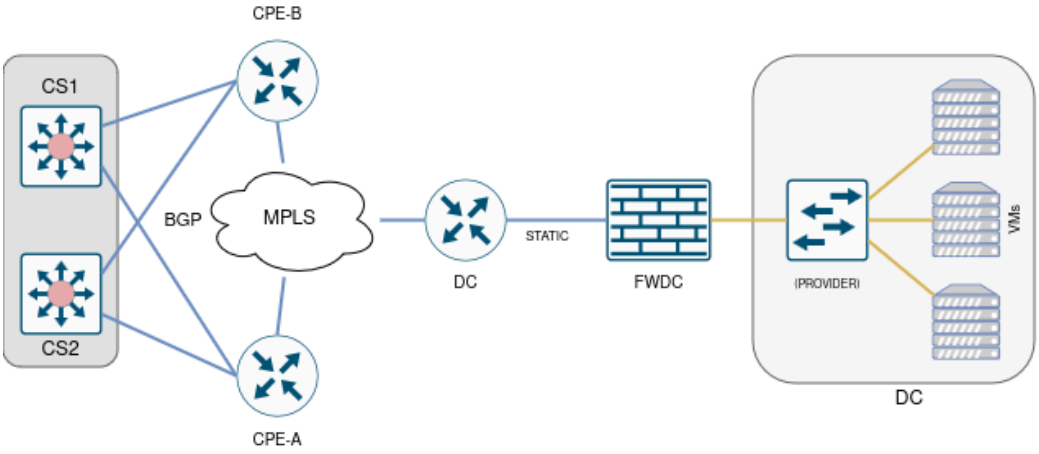

Figura 3.3: Schema rete verso datacenter

3.3 Configurazione dei datacenter

Il provider inizialmente forniva servizi di private cloud che non erano ridondati tra datacenter, pertanto, il guasto di uno rendeva inaccessibili tutti

i servizi ospitati al suo interno. Con il tempo, per rispondere alle esigenze di maggiore affidabilità dei clienti, è stato introdotto un servizio di VPLS (Virtual Private LAN Service), consentendo di estendere una rete Layer 2 tra due datacenter, formando delle coppie di datacenter interconnessi. Tuttavia, poiché il servizio VPLS opera a livello di Layer 2, non unifica completamente i due datacenter, infatti il routing con le reti geografiche può essere fatto soltanto tramite un datacenter. Di conseguenza, ogni rete è attestata in Layer 3 su un singolo datacenter, il che può portare a percorsi subottimali nel caso il gateway della rete si trovi in un altro sito. In questi casi il traffico ha un RTT maggiore dovendo percorrere il collegamento tra i due DC. L'attuale architettura offre maggiori garanzie per i servizi di storage e compute, poiché questi possono essere ridondati. Tuttavia, la comunicazione geografica rimane priva di ridondanza. Attualmente, esistono il sito principale e il sito di disaster recovery, che operano in modo indipendente. Per soddisfare i requisiti di Business Continuity (BC), verrà aggiunto un terzo datacenter che opererà in combinazione con il primo.

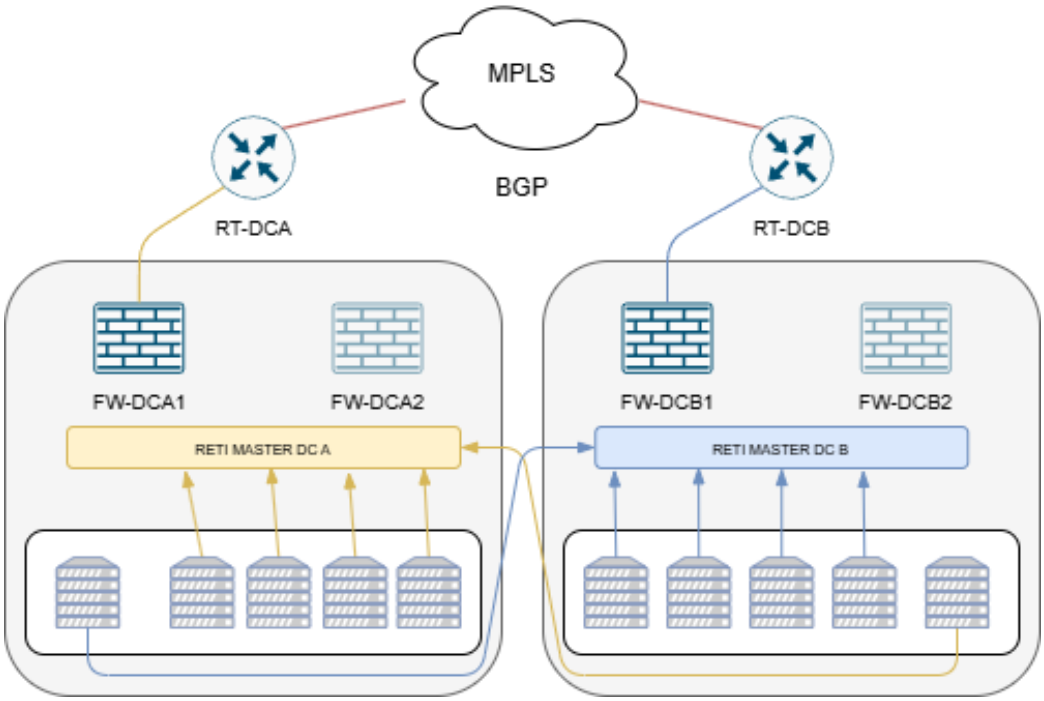

Figura 3.4: Schema configurazione attuale datacenter

3.4 Gestione policy firewall

Attualmente, le policy firewall sono gestite in modo semplice, configurando manualmente sorgente, destinazione, porta e interfacce su ciascun firewall. Nel caso di fwint, vengono applicati i profili UTM appropriati, come SSL inspection, DNS filtering o IPS. Si presume che la decisione di permettere o meno il traffico venga gestita dal sistema ricevente. Per questo motivo le comunicazioni che attraversano più firewall, come quelle dal datacenter a Internet o tra datacenter, esistono policy che permettono il traffico verso destinazioni già protette da firewall.
Questo tipo di gestione presenta diversi svantaggi: prima di tutto, richiede una conoscenza approfondita della posizione delle reti, poiché è necessario individuare il firewall corretto e le interfacce di sorgente e destinazione. Inoltre anche la verifica della presenza di una regola presenta lo stesso problema: per risolvere problemi di comunicazione, è necessario controllare in diversi punti se il traffico è consentito. La creazione o lo spostamento di una rete richiede di individuare e modificare tutte le regole associate, incluse quelle che gestiscono le connessioni con altri firewall, aggiungendo ulteriore complessità.
Sebbene le regole siano corrette, la loro gestione è complessa e richiede molto tempo, spesso necessitando del supporto di personale con una conoscenza approfondita della rete.

Capitolo 4

Analisi tecnologiche

Per proporre soluzioni migliorative è utile prima esaminare alcune delle tecnologie attualmente più utilizzate in contesti simili. Partendo da queste tecnologie si analizzerà poi come queste tecnologie possano essere implementate nell'architettura esistente.

4.1 EVPN

EVPN, acronimo di Ethernet Virtual Private Network [9] [31], è una tecnologia avanzata utilizzata per fornire servizi di rete virtuale su infrastrutture fisiche condivise. È diventata una soluzione popolare nelle reti di datacenter e nei servizi di provider per la sua capacità di supportare reti Layer 2 e Layer 3 con alta scalabilità ed efficienza. Per garantire queste caratteristiche, EVPN separa la topologia fisica (underlay network) da quella virtuale (overlay network). La possibilità di configurare l'overlay network in modo indipendente dall'underlay network offre flessibilità mantenendo la rete sottostante invariata [38] [10].
La tecnologia viene solitamente impiegata per DCI (Data Center Interconnect) in alternativa alle tradizionali tecnologie VPLS. In particolare [4]:

- **control plane**: EVPN utilizza BGP per distribuire informazioni su indirizzi ip e mac, mentre VPLS può anche usare LDP, ma risulta meno efficiente poiché si basa su metodi flood-and-learn.

- **servizi**: VPLS è stata pensata per servizi puramente Layer 2 mentre EVPN può offrire anche connettività Layer 3

- **ridondanza**: la possibilità di fare multi-homing è presente in VPLS ma con un solo link attivo mentre EVPN permette di utilizzare active-active load balancing.

4.1.1 Control Plane

Data l'estrema scalabilità delle tecnologie EVPN è possibile utilizzare un approccio SDN (Software Definied Networking) per il deployment di nuove EVIs (EVPN instances) sopra un underlay network esistente. In questo modo è possibile integrare la tecnologia con soluzioni datacenter come OpenStack per automaticamente provisionare reti che si estendono tra datacenter con un overhead minimo [26]. Tramite framework come OpenDaylight (ODL) si può anche applicare policy based routing tramite routing policies, load balancing e multi-homing. Questa flessibilità permette di utilizzare policy ottimali per la configurazione attuale oltre che a poter stabilire SLO (Server Level Objectives) [3].

4.1.2 Data Plane

Il data plane rappresenta l'underlay network che trasporta i dati in base alle decisioni prese dal control plane. Tra le tecnologie utilizzabili ci sono MPLS o il nuovo standard VXLAN.

La tecnologia MPLS è matura e affidabile, con meccanismi di QoS e una rapida convergenza ma è generalmente più complessa e costosa da creare ed operare. Le VXLAN, nate come estensione delle VLAN per offrire maggiore scalabilità e sono invece più semplici da implementare. Le VXLAN, da sole, risultano poco pratiche, ma in combinazione con un control plane come quello di EVPN, sono generalmente preferite rispetto a un'architettura basata su MPLS, che viene solitamente impiegata su infrastrutture esistenti [15].

4.1.3 VXLAN

Le VXLAN [22] sono una tecnologia di incapsulamento Layer 2 che è nata per superare le limitazioni delle tradizionali VLAN in contesti large-scale come i datacenter. In particolare sfruttano un esistente rete Layer 3 per incapsulare i pacchetti Layer 2 in pacchetti UDP che poi sfruttano il routing esistente per arrivare a destinazione. Per effettuare queste operazioni devono essere presenti dei device VTEP (VXLAN Tunnel Endpoint) in cui sono configurati dei VNI (VXLAN Network Identifier), analoghi ai vlan id, che identificano verso quali VTEP va instradato il traffico. Per la gestione del

traffico BUM (broadcast, unknown unicast, multicast) si utilizza solitamente la tecnica chiamata "head-end replication". In questa tecnica è previsto che ogni VTEP trasformi il traffico BUM in unicast verso le altre VTEP, non richiedendo quindi il supporto a multicast e broadcast dell'underlay network.

4.1.4 Anycast Gateway

L'anycast gateway è una tecnologia che permette di configurare un ip su più device in modalità active-active, per essere utilizzato come gateway. Questa configurazione si distingue dai protocolli FHRP (First Hop Redundancy Protocol), come VRRP o HSRP, in cui solo un dispositivo alla volta detiene l'IP in una configurazione active-passive. Nel contesto dei DCI, questa funzionalità può essere sfruttata per mantenere il gateway di rete all'interno del datacenter, riducendo le latenze di comunicazione e alleggerendo il traffico tra i datacenter.

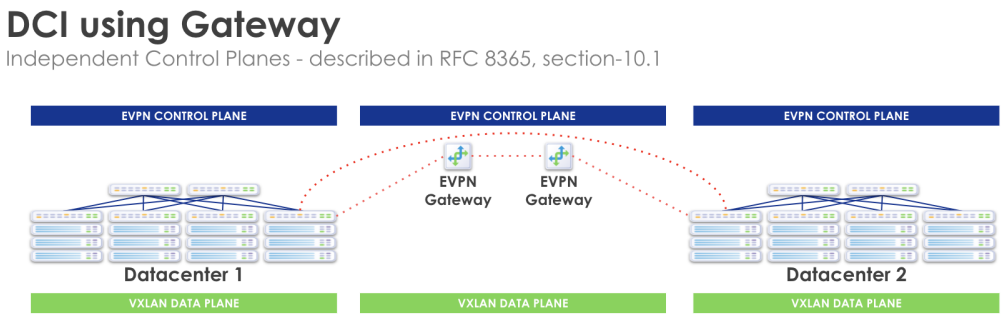

Figura 4.1: Schema anycast gateway

4.2 SD-WAN

Le Software-Defined Wide Area Network (SD-WAN) rappresentano un'evoluzione significativa nel modo in cui le reti WAN vengono gestite e ottimizzate. Tradizionalmente, la gestione di queste reti era esclusivamente gestita dai provider, che utilizzano tecnologie come l'MPLS (Multiprotocol Label Switching) per garantire l'interconnessione delle diverse sedi aziendali, offrendo al contempo garanzie di Qualità del Servizio (QoS). Tuttavia, l'internet tradizionale, noto per il suo approccio best-effort, non riusciva a fornire lo stesso livello di affidabilità e prestazioni [39] [23].

L'introduzione di protocolli innovativi come OpenFlow, che consente la configurazione automatica dei dispositivi di rete, e la crescente maturità dei controller software, ha reso possibile l'espansione della tecnologia Software-Defined Networking (SDN) anche alle reti WAN, offrendo una serie di vantaggi strategici:

- **Efficienza**: La capacità di effettuare traffic engineering su reti a costi inferiori, come quelle basate su broadband o LTE, comporta significativi risparmi economici mantenendo prestazioni paragonabili a quelle delle soluzioni tradizionali. Questo approccio ottimizza l'uso delle risorse di rete, riducendo i costi senza compromettere la qualità del servizio.

- **Gestione centralizzata**: La gestione della rete passa dalle mani del provider a quelle dell'utente finale, il quale acquisisce maggiore flessibilità e controllo sull'intera infrastruttura, potendo configurare e monitorare la rete in modo unificato e integrato. Questo approccio centralizzato consente una visibilità completa e una gestione più agile delle operazioni di rete.

- **Flessibilità**: L'utilizzo di connettività standard, come la comune banda larga, permette alle aziende di scegliere tra diversi provider, anche in aree geografiche diverse e remote. Inoltre, queste connessioni sono solitamente più rapide e semplici da attivare, consentendo una messa online delle sedi aziendali in tempi molto ridotti, facilitando l'espansione e l'agilità operativa.

- **Sicurezza**: Con una visibilità più approfondita del traffico di rete, è più semplice integrare soluzioni avanzate di sicurezza come firewall e strumenti di rilevamento delle minacce (threat detection), migliorando significativamente la protezione dei dati e delle comunicazioni aziendali. La capacità di monitorare e controllare il traffico in modo granulare consente una protezione più reattiva e proattiva contro le minacce emergenti.

Nonostante i numerosi vantaggi in termini di flessibilità e scalabilità, le soluzioni SD-WAN presentano anche alcune criticità. In particolare, la configurazione iniziale può rivelarsi complessa, richiedendo l'intervento di specialisti con competenze specifiche sul vendor selezionato. Inoltre, si pone il problema del vendor lock-in: a causa della scarsa standardizzazione e dell'interoperabilità limitata tra i diversi sistemi, il passaggio da un vendor all'altro comporta spesso una completa riconfigurazione dell'intera rete. Per le aziende di piccole e medie dimensioni, che necessitano di una scalabilità

inferiore, le soluzioni basate su MPLS potrebbero risultare più performanti e con minori costi di gestione, offrendo un equilibrio ottimale tra prestazioni e semplicità operativa.

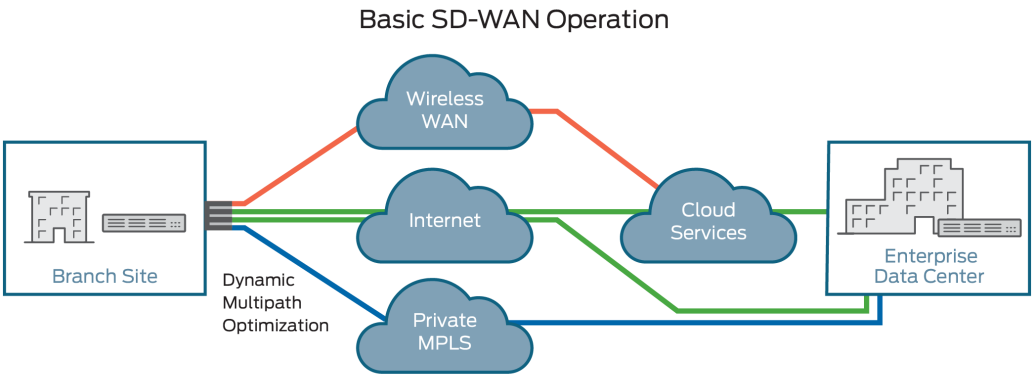

Figura 4.2: Schema SD-WAN

4.3 Microsegmentazione

Virtualized Network Function (VNF) è un approccio innovativo alla gestione delle reti che sposta le funzioni fatte in hardware in servizi software, permettendo una maggiore flessibilità e scalabilità nella gestione delle reti.Le VNFs permettono di provisioning rapido e dinamico di servizi di rete come firewall, load balancer e IDS, adattandosi alle esigenze di rete [18]. Tuttavia, l'uso delle VNFs comporta sfide come il mantenimento di performance elevate e costanti, la sicurezza specialmente in ambienti multi-tenant e l'ottimizzazione nell'orchestrazione di queste funzioni [2] [12]. Questa tecnologia ha il vantaggio di poter essere implementata ovunque senza richiedere nuovo hardware, favorendone l'adozione della microsegmentazione.

La microsegmentazione di rete è una strategia che mira a ridurre al minimo la dimensione dei segmenti di rete per avere controllo della comunicazione tra essi [32] [25]. In una rete tradizionale il traffico all'interno di una stessa subnet non può essere facilmente sottoposto a firewalling, per questo motivo è nata la necessità di creare segmenti di rete e mediare la comunicazione tramite un firewall. In particolare la microsegmentazione mira a ridurre i movimenti laterali di un possibile attaccante andando ad agire sul singolo

host al posto che sul segmento di rete. In un'architettura virtualizzata, grazie alle VNFs, è possibile applicare policy direttamente sulle NIC dei server virtuali. Questo approccio consente di avere un'unica subnet per l'intera infrastruttura virtuale, in cui il firewall non è centralizzato ma distribuito e gestito per ciascun server virtuale. Le prestazioni delle VNFs possono essere superiori grazie alle smart NIC, che, grazie a hardware specializzato, aumentano il throughput e riducono le latenze [8].
Un approccio simile può essere realizzato configurando i firewall sui server stessi, ma presenta diverse limitazioni. La prima limitazione riguarda la gestione, poiché richiederebbe di provisionare e mantenere il firewall in ambienti eterogenei, mentre un'infrastruttura virtuale centralizzata semplifica la gestione. Ci sono anche limiti di sicurezza, poiché un attaccante che prende il controllo della VM può disattivare le funzioni di sicurezza, se invece queste sono gestite dall'hypervisor, l'attaccante non ha alcun controllo su di esse.
Le principali soluzioni commerciali a sono VWARE NSX [37] e Cisco ACI [5] [20]. La piattaforma NSX è progettata per offrire un SDDC (Software-Defined Data Center), concentrandosi sulla parte virtualizzata, in particolare a livello di hypervisor fornendo un controllo granulare delle policy. Cisco ACI è più mirata ad essere una soluzione per la gestione della parte fisica e virtuale che unifica la gestione tramite un approccio policy-driven.

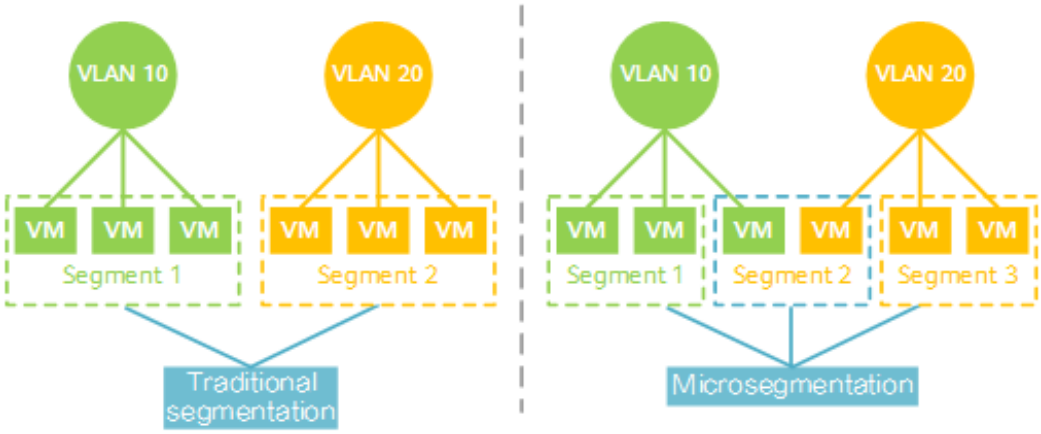

Figura 4.3: Schema funzionamento microsegmentazione

Capitolo 5

Analisi architetture

Data l'architettura attuale e le tecnologie viste nei capitoli precedenti in questo capitolo analizzeremo dei possibili scenari architetturali per poi valutarli in base ai requisiti. Gli scenari rappresentano solo una parte dell'architettura finale che sarà composta da una combinazione di essi

5.1 Reti con anycast gateway

Nel contesto dei due datacenter in BC le attuali reti configurate sui firewall verrebbero trasformate in reti EVPN con anycast gateway sui router su una VRF dedicata per ogni rete. Nella VRF è presente anche una rete di trasporto per l'interconnessione con i firewall, i quali continuano a filtrare il traffico come in precedenza, mantenendo invariata la comunicazione con le reti geografiche.
I due datacenter funzionerebbero come un'unica entità, richiedendo che i firewall (una coppia per datacenter) applichino le stesse policy su entrambi. Inoltre, per garantire che lo spostamento di un server tra datacenter sia completamente trasparente, è necessario che i firewall condividano anche le sessioni TCP e in caso contrario, la comunicazione verrebbe interrotta e dovrebbe essere ristabilita. Per ottenere questa configurazione, i 4 firewall devono operare come un unico cluster in ciascun datacenter, i firewall lavorano in modalità active-passive, mentre tra i datacenter operano in modalità active-active.
Per comunicare con le reti esterne geografiche, è necessario configurare il peering BGP per ogni VLAN/VRF tra i firewall e i router, così che i firewall possano annunciare alle VRF geografiche quali host risiedono in ciascun datacenter. Nella sede principale, le modifiche sono minime e consistono

nell'aggiornare le prefix-list in ingresso per accettare le stesse reti di prima, aggiungendo però il modificatore 'le 32' per includere anche le reti con prefisso /32.

5.1.1 Analisi

Il vantaggio di questa architettura è che i due datacenter si comportano come un'unica entità, ma, a differenza di prima, il traffico in ingresso e in uscita non deve mai transitare attraverso l'altro datacenter. Per garantire il funzionamento dell'EVPN, i router annunceranno reti /32, derivate dalle entry ARP, ai firewall, che a loro volta diffonderanno questi prefissi alle varie VRF geografiche per instradare il traffico al datacenter corretto. Le comunicazioni provenienti dalla sede principale o dalle organizzazioni partner avranno così latenze minime, poiché seguiranno il percorso più efficiente.
Tuttavia, questo approccio comporta un livello di complessità molto più elevato rispetto alla configurazione attuale, poiché per creare una nuova rete è necessario gestire numerosi componenti (vlan, vrf, peering), con un notevole coinvolgimento da parte del provider. Di conseguenza questa configurazione non risulta scalabile per un datacenter in espansione che necessiti di mantenere un elevato livello di segmentazione.

La soluzione è nel complesso ottimale per performance riducendo al minimo necessario l'utilizzo della banda e il packet loss, soddisfacendo inoltre i requisiti di sicurezza mantenendo le comunicazione protette da firewall. Tuttavia, la gestione di questa configurazione risulta troppo complessa a causa della continua necessità di creare nuove reti e dell'elevata dipendenza dal provider.

5.2 Reti di trasporto con anycast gateway

L'idea di questa configurazione è sfruttare i vantaggi dell'anycast gateway, limitando però il suo impiego a determinati casi. Attualmente, se una rete si trova in un datacenter e quest'ultimo subisce un guasto nella connessione geografica, sono necessari interventi manuali per spostarla. Utilizzando l'anycast gateway su entrambi i datacenter, possiamo automatizzare questo processo. Dobbiamo quindi configurare la rete in modo tale che, anche se un intero datacenter diventa irraggiungibile, la comunicazione continui a funzionare senza bisogno di interventi manuali.
In precedenza, ogni datacenter aveva una coppia di firewall in modalità

active-passive; ora manterremo questa configurazione, ma con la particolarità che il firewall passivo di ciascun datacenter si troverà fisicamente nell'altro datacenter. In caso di guasto nel datacenter A, perderemo il firewall primario di quel datacenter, ma esso verrà riattivato tramite i meccanismi di alta disponibilità (HA) nel datacenter B. Allo stesso tempo, il firewall secondario nel datacenter B, che già prima non era utilizzato, risulterà indisponibile. Dovremo estendere le reti dei firewall tra i due datacenter utilizzando EVPN o VPLS, in modo da spostare i server mantenendo la stessa subnet.
La parte più complessa è l'interconnessione con le VRF geografiche, infatti anche in questo caso sarà necessaria la ridondanza a livello di routing. Poichè i firewall sono in HA devono avere la stessa configurazione tra i due datacenter. Per questo motivo sfruttiamo l'anycast-gateway per le reti di trasporto verso i router in modo da avere una configurazione analoga tra i due DC. Per ogni VRF configureremo un peering verso ogni router di datacenter, in questo modo ogni rete viene annunciata da entrami i DC verso il medesimo next-hop. Nel caso di un fault di uno dei due router l'altro continuerà ad annunciare le reti, nel caso invece di failover grazie al graceful restart del BGP il firewall secondario potrà in breve tempo ripristinare gli annunci. L'utilizzo dell'anycast gateway è necessario per poter instaurare la sessione BGP allo stesso modo in entrambi i DC, altrimenti il firewall vedrebbe una configurazione differente tra i due siti.

5.2.1 Analisi

Lo schema proposto si pone come come una combinazione tra la configurazione attuale e quella precedentemente presentata. Il routing dei pacchetti da e verso la rete geografica è ottimale in quanto una volta che il pacchetto viene consegnato alla rete del provider sceglierà lui il percorso migliore verso il firewall, di cui sa la posizione grazie all'EVPN mentre prima erano presenti rotte statiche limitate ad un unico datacenter. Il fault di un datacenter viene gestito in automatico per quanto riguarda la rete e ci sono tutte le condizioni per implementare un failover anche sui virtualizzatori. Il traffico viene ispezionato dai firewall come la situazione precedente e non è necessario creare un cluster di 4 dispositivi.
L'architettura presentata non riesce però a migliorare la situazione all'interno del datacenter stesso, infatti il gateway delle reti in datacenter è il firewall stesso che è attivo in un solo dei due datacenter. Per ottenere latenze e banda ottimali quindi è necessario che i server ed il firewall siano nello stesso datacenter, in caso contrario bisognerà pagare le latenze del DCI. Non possiamo infatti affermare che i datacenter si comportino come un unico datacenter,

rimangono quindi delle reti che sono nativamete di un datacenter limitando la flessibilità nel bilanciamento del carico tra essi.
L'architettura presentata è un ibrido tra quella attuale e quella precedentemente presentata, offrendo un ottimo compromesso tra gestione e performance. Le latenze sono più impattanti per le interconnessioni geografiche che in questo caso risultano ottimali. La gestione della sicurezza ha una complessità analoga a quella attuale. Creare un nuovo segmento di rete in datacenter non richiede l'intervento del provider dato che il routing è completamente dinamico e gestito dall'organizzazione stessa. Il coinvolgimento del provider è legato unicamente alla configurazione di una nuova interconnessione ad una VRF geografica.

5.2.2 Virtual Clustering

Tra le limitazioni di questa architettura è la penalità da pagare nel caso di failover del firewall, infatti in quel caso tutte le comunicazioni dovrebbero passare tramite il DCI diminuendo le performance ed alzando le latenze. Se si verifica un problema hardware sul firewall primario di un datacenter durante il tempo necessario per la sostituzione si avrebbe questa situazione non ottimale. Teoricamente l'hardware per continuare le operazioni nello stesso datacenter è presente e tramite tecnologie come il virtual clustering di Fortinet [17] oppure i Virtual System Paloalto [35] ne possiamo trarre vantaggio.
Queste soluzioni permettono di dividere un cluster HA in più unità logiche indipendenti, possiamo creare quindi due cluster virtuali da 4 firewall ciascuno utilizzando al meglio l'hardware. La configurazione prevederebbe di avere comunque una configurazione active-passive ma in cui il primo failover è nello stesso datacenter mentre il secondo e terzo nel secondo DC. Per farlo è però necessario che ogni tra i due firewall virtuali nello stesso hardware non vengano condivise interfacce fisiche che comporta avere il doppio di interconnessioni fisiche. Un dispositivo moderno deve poter gestire almeno 10Gbit/s di traffico ed essere ridondato da un fault dello switch collegato, quindi richiede due interfacce da 10G aggregate. Significa quindi che per il ottenere la configurazione proposta sono necessarie per ogni dispositivo 4 interfacce 10G, requisito che oltre a richiedere hardware più avanzato richiede che il provider accetti di dare il doppio delle porte. Inoltre queste tecnologie sono ancora più ad-hoc per ogni vendor aumentando il vendor-lockin oltre che aumentare la complessità nella gestione. La complessità aggiuntiva rispetto ai vantaggi che porta la rendono una soluzione difficilmente applicabile.

5.3 EVPN con microsegmentazione

Il principale difetto della prima soluzione risiede nell'elevato overhead e nella complessità di gestione di numerose reti. Questo modello mira a risolvere tale problema attraverso l'uso delle tecnologie di microsegmentazione. La rete del datacenter sarebbe composta da poche subnet e non richiederebbe un firewall centrale, grazie a tecnologie di microsegmentazione come VMware NSX. Grazie a queste tecnologie infatti possiamo andare ad applicare policy a livello di virtual machine e non sono più rilevanti i concetti di subnet per segmentare. Il gateway delle reti sarebbe il router del provider, che utilizza un anycast gateway per consentire la mobilità tra i due datacenter. Sarà comunque necessario un router aggiuntivo per gestire i collegamenti con le VRF geografiche. Per evitare l'aggiunta di nuovo hardware si può utilizzare una VM (una coppia per datacenter per ridondanza) con quagga [28] o FRRouting [14]. Le interconnessioni in questo caso non necessitano l'utilizzo di EVPN ma possono essere normali reti di trasporto, diverse tra i due datacenter.

5.3.1 Analisi

La soluzione proposta è la più performante, poiché offre i vantaggi di EVPN senza le problematiche legate alla segmentazione. Infatti tramite anycast gateway si ottiene routing ottimale dei pacchetti sia verso le VRF geografiche che internamente al datacenter. Come nella prima soluzione si ottiene il vantaggio che i due datacenter si comportano come un'unica entità. I requisiti di sicurezza sono rispettati in quanto tramite microsegmentazione si ottiene una gestione delle policy ancora più efficiente. L'overhead di gestione viene ulteriormente ridotto, poiché non è più necessario gestire gli indirizzamenti di rete nel datacenter. La segmentazione viene eseguita a livello di virtualizzatore, eliminando la necessità di creare e gestire reti aggiuntive. I costi di implementazione delle tecnologie di microsegmentazione sono attualmente elevati, poiché si tratta di soluzioni proprietarie e prive di valide alternative open-source. Inoltre comportano un vendor lock-in maggiore in quanto la gestione delle policy è differente tra i vari vendor. Per quanto riguarda le policy, sarebbe necessario dividere la gestione tra la sede centrale e il datacenter, il che richiederebbe una formazione specifica del personale. Nel complesso questa architettura offre un maggiore livello di sicurezza grazie all'utilizzo di microsegmentazione senza introdurre overhead di gestione che sarebbero proibitivi. Grazie all'integrazione con le tecnologie di virtualizzazione e la mancata dipendenza dal provider si pone come una soluzione

molto scalabile. Tuttavia, i costi di migrazione e manutenzione di questa tecnologia sono molto elevati, rendendola non sostenibile per alcune realtà, come quella presa in considerazione.

5.4 EVPN sui firewall

Diversamente dalla prima architettura si può configurare l'EVPN allo stesso modo anche sui firewall stessi gestendo la comunicazione geografica come descritto in 5.2. Così facendo si elimina la forte dipendenza e maggiore complessità descritta in 5.1 ma mantenendo i suoi vantaggi. L'architettura prevede di utilizzare una coppia active-passive per datacenter che hanno peering separati per VRF geografica, senza utilizzare meccanismi EVPN del provider. Sfruttando questo underlay viene stabilita una EVPN-VXLAN tra i due DC, ogni VLAN server viene trasformata in EVPN con anycast-gateway fatto dai firweall al contrario delle architetture precedenti che era gestito dal provider. Per gestire correttamente il multi-homing dei server è necessario che le due coppie di firewall si scambino le sessioni come se fossero un unico cluster, oltre che dover avere le stesse policy gestendo a tutti gli effetti le stesse reti. Le comunicazioni geografiche vengono gestite ridistribuendo le rotte EVPN verso le VRF geografiche dinamicamente, permettendo anche in qeusto caso di gestire la mobilità di un server tra i due DC.

5.4.1 Analisi

I vantaggi sono analoghi a 5.1 dato che sfruttiamo la stessa idea di convertire ogni VLAN in rete EVPN. Il routing è sempre ottimale in ogni combinazione dato che il gateway è sempre nello stesso DC e dalle VRF geografiche il next-hop è sempre verso il DC corretto. I due DC si comportano come uno unico dando il maggior grado di flessibilità nell'utilizzo delle risorse e anche nella gestione, dando completa ridondanza in caso di guasto. La tecnologia è relativamente nuova e non supportata sui firewall commerciali che la implementano solo nelle ultime versioni di firmware nel caso di Fortinet [34] e Palo Alto [6] ma solo nella versione EVPN Layer 2, senza la possibilità di sfruttare anycast gateway. Una volta che la tecnologia è più matura per questo tipo di apparati questa architettura si pone come naturale upgrade rispetto a quanto previsto in 5.2.

5.5 SDN

La rapida crescita di soluzioni SDN ha permesso una più flessibile e conveniente nella gestione delle reti, portando a una grande adozione anche nei datacenter [1]. I vantaggi portati da una architettura SDN sono stati estesi all'intero datacenter integrando concetti software-defined in ambiti come compute e storage portando ai Software-Defined Data Centers (SDDC) [16]. Questi concetti sono particolarmente efficaci nelle installazioni di grandi dimensioni, rendendoli più adatti ai provider o a grandi organizzazioni con decine di sedi da interconnettere. Nel caso in cui un provider adotti una soluzione SDDC, il cliente finale otterrà una soluzione già ottimizzata, ma con una minore visibilità sull'infrastruttura sottostante, rendendola simile a un public cloud.

5.6 Gestione policy firewall

Finora ora è stata discussa la parte di routing ma l'architettura dovrebbe anche supportare un processo ottimale per la gestione delle regole. Poiché sono necessari più firewall, diventa complesso gestire dove inserire le policy e come trattare i casi in cui il traffico attraversa due firewall (uno verso internet e uno verso la sede). Esistono soluzioni per la gestione centralizzata dei firewall (supponendo l'uso dello stesso vendor), che offrono un punto centrale per la gestione e la condivisione degli oggetti. Tuttavia, l'operatore deve ancora sapere dove applicare le regole in base all'interfaccia e al firewall corretto, oltre a gestire i casi in cui la comunicazione passa attraverso più firewall. Per risolvere il problema la gestione proposta prevede di unificare le regole in un unico pacchetto che viene distribuito in egual modo su tutti i firewall. Essendo le regole su tutti i firewall se esiste una regola da A verso B sulla porta X è assicurato che il traffico venga permesso, mentre prima bisognava verificare il flusso su potenzialmente più dispositivi.

Per ottenere tale configurazione bisogna rimuovere dalle configurazioni attuali le interfacce e basare le policy unicamente sulla quintupla ip per decidere se permettere il flusso. Inoltre è necessario rimuovere tutte le regole che in precedenza supponevano che il traffico venisse bloccato da un firewall, come ad esempio nel caso di comunicazioni tra sede e datacenter. Data la necessità di unificare le regole è però consigliabile di escludere il firewall internet da questa gestione data la peculiarità delle sue policy. Con questa configurazione e utilizzando uno strumento di gestione centralizzata come Panorama [27] o Fortimanager [13], è possibile creare un unico pacchetto di

policy e assegnarlo a più firewall. In questo modo, le regole vengono modificate in un solo punto e distribuite su più dispositivi. La gestione proposta aggiunge un numero maggiore di regole ai singoli dispositivi rispetto a quanto strettamente necessario. Tuttavia, in realtà piccole, con le dovute ottimizzazioni, l'impatto è minimo; invece in situazioni in cui l'hardware è già al limite, però, questa soluzione non è applicabile. La gestione dei NAT risulta più complessa, poiché non possono essere centralizzati e devono essere specifici per ogni dispositivo. In questo caso, le soluzioni di gestione centralizzata aiutano, permettendo di limitare alcune regole a un solo dispositivo, pur mantenendo il pacchetto condiviso. Nel complesso la soluzione proposta per una realtà di medie dimensioni è sostenibile e diminuisce la complessità nella gestione dei firewall. La migrazione a questa configurazione dipende da quella attuale e può quindi variare molto di complessità.

Capitolo 6

Implementazione

Sulla base delle architetture esaminate nel capitolo precedente, analizziamo come sarà strutturata la rete finale e le sue caratteristiche. Inoltre, valuteremo scenari alternativi per ambienti con configurazioni o requisiti differenti.

L'architettura di routing più adatta, in base ai requisiti di ridondanza, latenza e QoS, prevede l'uso delle tecnologie EVPN con anycast-gateway, che però possono risultare complesse da gestire. La soluzione proposta con il minor impatto nella gestione gestione è quella che sfrutta l'anycast-gateway per le interconnessioni geografiche come descritto in 5.2. Per quanto riguarda la gestione delle policy, la soluzione centralizzata proposta in 5.6 offre un approccio più efficiente rispetto a quello attuale, senza compromettere le prestazioni. Nei prossimi paragrafi valutiamo come l'architettura attuale si comporta rispetto ai requisiti esposti nel capitolo 2.

6.1 Requisiti di performance

6.1.1 Affidabilità

Per analizzare l'affidabilità, esaminiamo il comportamento della rete in caso di potenziali guasti:

- **Guasto di un datacenter**: può essere provocato da guasti fisici o logici nelle comunicazione geografiche. Grazie alle interconnessioni geografiche in EVPN il failover avverrà in modo automatico e senza interruzioni verso il datacenter secondario. In precedenza, questa ridon-

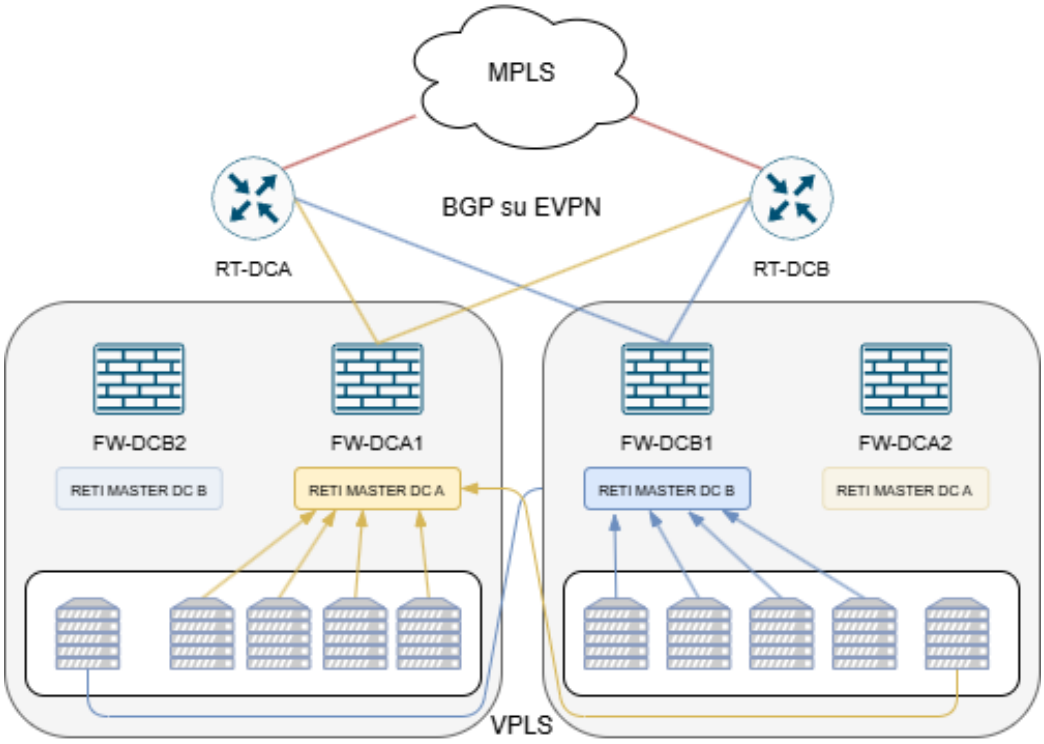

Figura 6.1: Diagramma di rete con architettura EVPN

danza non era disponibile e la ridondanza era imitata a guasti solo all'interno del DC.

- **Guasto di un router**: tutti i dispositivi e le loro comunicazioni sono ridondati come in precedenza quindi il guasto di un singolo dispositivo non va ad impattare la raggiungibilità. Nella sede principale, due router comunicano con altri due router del provider, e grazie al routing dinamico, il traffico viene reindirizzato verso il router ancora funzionante. In caso di guasto del router di datacenter, se non causa l'isolamento completo del datacenter, essendo presente un peering anche con il router secondario il routing viene mantenuto intatto.

- **Guasto di un firewall**: ogni cluster firewall è composto da una coppia di dispositivi in HA che possono fare failover senza impatto sugli utenti in quanto condividono anche le sessioni. Fisicamente ogni dispositivo è bialimentato e con un aggregato LACP collegato a due switch dando ulteriore ridondanza. In caso di guasto del firewall principale in

un datacenter, il traffico viene reindirizzato al datacenter secondario, con un conseguente aumento della latenza fino al ripristino del firewall primario, ma mantenendo la raggiungibilità.

6.1.2 Quality of Service

Latenza
Durante le normali operazioni la latenza rimane invariata rispetto all'architettura precedente, con lo svantaggio di un tempo di round-trip (RTT) aggiuntivo nel caso in cui il server si trovi fisicamente in un datacenter diverso da quello del proprio gateway. Al contrario dell'architettura precedente, in cui la raggiungibilità delle reti dietro ad un firewall era legato ad un singolo DC, in questa architettura tramite il failover dei firewall nel DC secondario vengono modificati anche i puntamenti geografici rendendo ottimale il routing e di conseguenza il QoS. Nel caso tutti i servizi vengono spostati nel DC secondario a causa di un problema nel primario la soluzione proposta offre completa ridondanza e non compromette la latenza.
Packet Loss
Anche in questo caso, analizziamo se, nei diversi scenari di guasto, la rete mantiene queste caratteristiche, in relazione all'entità del guasto. In caso di guasti, la perdita di pacchetti si verifica esclusivamente durante il failover dei dispositivi, che avvenendo in modalità totalmente automatica ha spesso tempi brevi.

6.2 Requisiti di sicurezza

Rispetto all'attuale architettura, la sicurezza è gestita in modo simile, poiché i segmenti di rete restano invariati e continuano a essere separati da un firewall. Se questo requisito venisse eliminato, l'utilizzo dell'EVPN sarebbe più semplice da gestire e migliorerebbe le prestazioni, ma comprometterebbe completamente la sicurezza, che è invece un pilastro fondamentale. La possibilità di creare nuove reti per mantenere la segmentazione rimane invariata, poiché la struttura delle reti dietro i firewall non cambia.
Per migliorare il livello di sicurezza le soluzioni di microsegmentazione offrono una migliore granularità nelle policy e una visione centrale. Tuttavia, il costo delle licenze e la formazione necessaria spesso le rendono impraticabili, oltre a imporre un forte vendor lock-in e una migrazione complessa; per questi motivi, la soluzione non è stata adottata.

6.3 Requisiti di gestione

La gestione della sicurezza è migliorata grazie all'uso di policy centralizzate, che consentono una maggiore efficienza, in particolare per l'ambiente datacenter. Infatti spesso le comunicazioni con i DC passano anche dai firewall di sede, rendendo necessario implementare policy doppie e controllare due set di log. Inoltre, la possibilità di spostare le reti da un datacenter all'altro può rendere complesso individuare il firewall su cui apportare le modifiche.
La gestione centralizzata inoltre permette di spostare una rete dal cluster A al cluster B andando semplicemente a spostare l'ip dei firewall senza dover intervenire quindi sulle policy. Questa soluzione permette di poter bilanciare meglio il carico tra i due DC dando maggiore flessibilità nella gestione delle reti. Anche lo spostamento di un server da una subnet ad un altra diventa più semplice dato è sufficiente modificare un unico pacchetto policy e unicamente l'ip, dato che le policy non distinguono l'interfaccia.

6.4 Business continuity

Uno dei requisiti più importanti è il supporto alla business continuity e disaster recovery che richiedono la presenza di almeno tre DC con diversi tipi di comunicazioni tra essi. In particolare la comunicazione con il DC di DR rimane standard con l'unico requisito di non dover richiedere il passaggio dalla sede principale per le comunicazioni tra DC. Questo è possibile senza configurazioni particolari, assumendo che le connessioni dei datacenter appartengano allo stesso provider, il quale può instradare il traffico senza passare per la sede principale.
I requisiti per la business continuity diventano molto più stringenti, poiché è necessario rendere trasparente la ridondanza tra due datacenter agli occhi degli applicativi, mantenendo gli stessi indirizzi ip. Con l'architettura proposta, i server possono migrare liberamente tra i datacenter, rimanendo resilienti anche in caso di guasto di un intero datacenter. Assumendo che i livelli di calcolo e storage siano ridondanti, la rete è in grado di supportare pienamente la BU, garantendo le prestazioni descritte nei capitoli precedenti.

Capitolo 7

Conclusione e sviluppi futuri

Come abbiamo visto le reti sono dinamiche ed è importante valutare anche come si può evolvere la rete attuale per meglio seguire i bisogni dell'organizzazione. L'architettura presentata in 5.4 è un naturale upgrade rispetto alla configurazione attuale quando le implementazioni saranno mature su hardware commerciale. Rispetto all'architettura presentata offre maggiori performance ottimizzando l'rtt oltre che una gestione semplificata dato che si comportano come un unico DC.

La architettura attuale nonostante le ottimizzazioni fatte rimane relativamente complessa rispetto all'utilizzo di un public cloud provider che nativamente rispetta a pieno tutti i requisiti. Grazie all'utilizzo degli SDDC possono provisionare risorse di rete in modo efficiente su larga scala e sfruttando VNFs riescono ad offrire la parte di security. Nel contesto del private cloud possiamo aspettarci che queste tecnologie vengano sempre più adottate sollevando il cliente finale dall'onere di dover configurare la rete tramite apparati in housing. Per il singolo utilizzatore l'utilizzo delle SDN non offre vantaggi, ma alla scala di un cloud provider è uno strumento che permette di offrire servizi analoghi a quelli di un public cloud.

Le tecnologie di microsegmentazione con Vmware NSX offrono grandi vantaggi per la sicurezza e danno grande flessibilità per la parte di rete con spesso costi di licenza molto elevati. In un futuro potrebbero sorgere soluzioni meno costose o preferibilmente open source che permettono una maggiore adozione in ambienti datacenter. Le soluzioni di microsegmentazione essendo software based si hanno anche il vantaggio di facile integrazione con il mondo SDN offrendo una gestione centralizzata.

Bibliografia

[1] Taimur Bakhshi. «State of the Art and Recent Research Advances in Software Defined Networking». In: *Wirel. Commun. Mob. Comput.* 2017 (2017). DOI: 10.1155/2017/7191647.

[2] Md. Faizul Bari et al. «Orchestrating Virtualized Network Functions». In: *IEEE Transactions on Network and Service Management* 13 (2015), pp. 725–739. DOI: 10.1109/TNSM.2016.2569020.

[3] Cristian Hernandez Benet et al. «Policy-based routing and load balancing for EVPN-based data center interconnections». In: *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*. 2017, pp. 1–7. DOI: 10.1109/NFV-SDN.2017.8169841.

[4] Wang Shengnan Chen Li. *Why Do We Need EVPN?* URL: https://info.support.huawei.com/info-finder/encyclopedia/en/EVPN.html (visitato il giorno 25/08/2024).

[5] *Cisco Application Centric Infrastructure (ACI)*. URL: https://www.cisco.com/site/us/en/products/networking/cloud-networking/application-centric-infrastructure/index.html (visitato il giorno 25/08/2024).

[6] *Deploying a L2 VXLAN EVPN Network with Palo Alto Networks Firewalls*. URL: https://www.paloaltonetworks.com/resources/techbriefs/deploying-l2-vxlan-evpn-network-with-palo-alto-networks-firewalls (visitato il giorno 25/08/2024).

[7] Manik Dey. «Business Continuity Planning (BCP) methodology — Essential for every business». In: *2011 IEEE GCC Conference and Exhibition (GCC)*. 2011, pp. 229–232. DOI: 10.1109/IEEEGCC.2011.5752503.

[8] *DPU-based Acceleration for NSX*. URL: https://blogs.vmware.com/networkvirtualization/2022/08/announcing-dpu-based-acceleration-for-nsx.html/ (visitato il giorno 25/08/2024).

[9] John Drake et al. *BGP MPLS-Based Ethernet VPN*. RFC 7432. Feb. 2015. DOI: 10.17487/RFC7432. URL: https://www.rfc-editor.org/info/rfc7432.

[10] *Ethernet VPN (EVPN)*. URL: https://www.nokia.com/networks/ethernet-vpn/ (visitato il giorno 25/08/2024).

[11] Dennis Ferguson, Acee Lindem e John Moy. *OSPF for IPv6*. RFC 5340. Lug. 2008. DOI: 10.17487/RFC5340. URL: https://www.rfc-editor.org/info/rfc5340.

[12] Mahdi Daghmehchi Firoozjaei et al. «Security challenges with network functions virtualization». In: *Future Gener. Comput. Syst.* 67 (2017), pp. 315–324. DOI: 10.1016/j.future.2016.07.002.

[13] *Fortigate - Fortimanager*. URL: https://www.fortinet.com/products/management/fortimanager (visitato il giorno 27/08/2024).

[14] *FRRouting*. URL: https://frrouting.org/.

[15] A Shaji George e AS Hovan George. «A Brief Overview of VXLAN EVPN». In: *Ijireeiceinternational Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering* 9.7 (2021), pp. 1–12.

[16] Ghazanfar et al. «Software-Defined Data Center». In: *Encyclopedia of Wireless Networks* (2013). DOI: 10.1007/978-3-319-78262-1_300617.

[17] *HA virtual cluster setup*. URL: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/599385/ha-virtual-cluster-setup (visitato il giorno 26/08/2024).

[18] B. Han et al. «Network function virtualization: Challenges and opportunities for innovations». In: *IEEE Communications Magazine* 53 (2015), pp. 90–97. DOI: 10.1109/MCOM.2015.7045396.

[19] Mohammad Hafiz Hersyah e Derisma. «A Literature Review on Business Continuity Based on ISO 22301, Six Sigma and Customer Satisfaction Evaluation». In: *2018 International Conference on Information Technology Systems and Innovation (ICITSI)*. 2018, pp. 392–397. DOI: 10.1109/ICITSI.2018.8696075.

[20] Palash Ijari. «Comparison between Cisco ACI and VMWARE NSX». In: *IOSR J. Comput. Eng.(IOSR-JCE)* 19 (2017), pp. 70–72.

[21] G. Kumar e Krishan Kumar. «Network security – an updated perspective». In: *Systems Science & Control Engineering: An Open Access Journal* 2 (2014), pp. 325–334. DOI: 10.1080/21642583.2014.895969.

[22] Mallik Mahalingam et al. *Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks*. RFC 7348. Ago. 2014. DOI: 10.17487/RFC7348. URL: https://www.rfc-editor.org/info/rfc7348.

[23] Gao Mine et al. «A design of SD-WAN-oriented wide area network access». In: *2020 International Conference on Computer Communication and Network Security (CCNS)*. 2020, pp. 174–177. DOI: 10.1109/CCNS50731.2020.00046.

[24] John Moy. *OSPF Version 2*. RFC 2328. Apr. 1998. DOI: 10.17487/RFC2328. URL: https://www.rfc-editor.org/info/rfc2328.

[25] Muhammad Mujib e Riri Fitri Sari. «Performance Evaluation of Data Center Network with Network Micro-segmentation». In: *2020 12th International Conference on Information Technology and Electrical En-*

gineering (ICITEE). 2020, pp. 27–32. DOI: 10.1109/ICITEE49829.2020.9271749.

[26] Kyoomars Alizadeh Noghani et al. «Automating Ethernet VPN deployment in SDN-based Data Centers». In: *2017 Fourth International Conference on Software Defined Systems (SDS)*. 2017, pp. 61–66. DOI: 10.1109/SDS.2017.7939142.

[27] *Palo Alto Networks - Panorama*. URL: https://www.paloaltonetworks.com/network-security/panorama (visitato il giorno 27/08/2024).

[28] *Quagga*. URL: https://www.nongnu.org/quagga/.

[29] Yakov Rekhter, Susan Hares e Tony Li. *A Border Gateway Protocol 4 (BGP-4)*. RFC 4271. Gen. 2006. DOI: 10.17487/RFC4271. URL: https://www.rfc-editor.org/info/rfc4271.

[30] Yakov Rekhter e Eric C. Rosen. *BGP/MPLS IP Virtual Private Networks (VPNs)*. RFC 4364. Feb. 2006. DOI: 10.17487/RFC4364. URL: https://www.rfc-editor.org/info/rfc4364.

[31] Ali Sajassi et al. *Integrated Routing and Bridging in Ethernet VPN (EVPN)*. RFC 9135. Ott. 2021. DOI: 10.17487/RFC9135. URL: https://www.rfc-editor.org/info/rfc9135.

[32] Nabeel Sheikh, Mayur Pawar e Victor Lawrence. «Zero trust using Network Micro Segmentation». In: *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2021, pp. 1–6. DOI: 10.1109/INFOCOMWKSHPS51825.2021.9484645.

[33] Abdelfatah A Tamimi, Raneem Dawood e Lana Sadaqa. «Disaster Recovery Techniques in Cloud Computing». In: *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*. 2019, pp. 845–850. DOI: 10.1109/JEEIT.2019.8717450.

[34] *Using MP-BGP EVPN with VXLAN*. URL: https://docs.fortinet.com/document/fortigate/7.4.0/new-features/52499/using-mp-bgp-evpn-with-vxlan (visitato il giorno 25/08/2024).

[35] *Virtual Systems Overview*. URL: https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/virtual-systems/virtual-systems-overview (visitato il giorno 26/08/2024).

[36] Arun Viswanathan, Eric C. Rosen e Ross Callon. *Multiprotocol Label Switching Architecture*. RFC 3031. Gen. 2001. DOI: 10.17487/RFC3031. URL: https://www.rfc-editor.org/info/rfc3031.

[37] *VMware NSX*. URL: https://www.vmware.com/products/cloud-infrastructure/nsx (visitato il giorno 25/08/2024).

[38] *What is EVPN-VXLAN?* URL: https://www.hpe.com/us/en/what-is/evpn-vxlan.html.

[39] Zhenjie Yang et al. «Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities». In: *2019 28th International Conference on Computer Communication and Networks (ICCCN)*. 2019, pp. 1–9. DOI: 10.1109/ICCCN.2019.8847124.