AWS Direct Connect con AWS Site-To-Site VPN come failover

1 Aprile 2022 - 7 min. read

Advanced Networking *AWS Direct Connect*

Introduzione

Oggi, molte soluzioni richiedono approcci che implementino un uso congiunto dei cloud provider pubblici e delle proprie risorse on-premise. In questa serie di articoli, vogliamo fornire una panoramica dei servizi AWS utili per creare una rete ibrida che estende facilmente i carichi di lavoro dalle installazioni locali al cloud pubblico in base alle esigenze aziendali.

In alcuni scenari, le reti cloud ibride si basano su **AWS Direct Connect (DX)**. Questo servizio offre un'altra opzione anziché Internet per connettersi ad AWS, fornendo una **connessione di rete privata tra la struttura on-premise** e il **cloud AWS**.

Se desideri saperne di più su Direct Connect, controlla il nostro post precedente: spiega nel dettaglio che cos'è, come funziona e come sceglierlo in relazione ad alle proprie esigenze.

In alcuni casi, questa connessione da sola non è sufficiente. È sempre meglio garantire una **connessione di fallback** come backup di DX. Ci sono diverse opzioni, ma implementare il tutto con una **VPN Site-To-Site** è una soluzione conveniente che può essere sfruttata per ridurre i costi o, nel frattempo, attendere il setup di un secondo DX.

Bisogna tenere presente che questa soluzione non garantisce alcun Accordo sul Livello del Servizio (SLA) ed è impossibile ottenerlo con una connessione Internet pubblica.

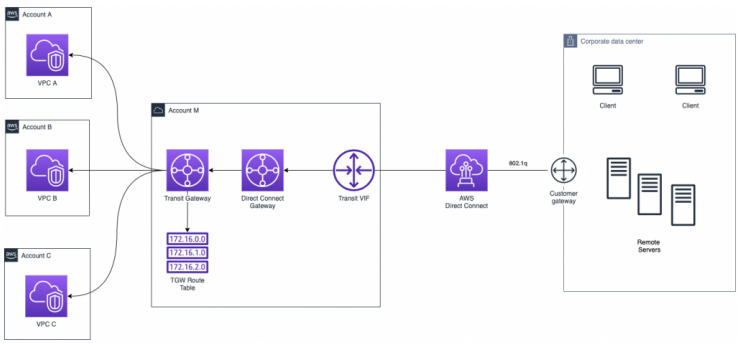
Infrastruttura ad Alto Livello

Questo articolo riprenderà alcuni argomenti di quanto già realizzato nell'articolo precedente (Hybrid Cloud Networking: gateway NAT centralizzato tramite AWS Transit Gateway). Abbiamo presentato come configurare un Transit Gateway e condividere apparati di rete tra account AWS. Quindi, per favore, potrebbe essere utile leggerlo per comprendere al meglio ciò che verrà presentato successivamente.

Si supponga che un'azienda fittizia desideri connettere i propri uffici con gli account AWS direttamente tramite DX utilizzando una VPN da sito a sito come backup.

Prima di procedere è necessario che sia già stato richiesto e ordinato un Direct Connect e che l'intera rete AWS sia stata centralizzata tramite Transit Gateway.

Come mostrato di seguito, la connessione tra la struttura locale e AWS tramite la connessione privata Direct Connect può essere configurata collegando direttamente il DX al Transit Gateway.



Entrando nel dettaglio:

Direct Connect offre una struttura che si basa su un canale di trasporto in fibra ottica Ethernet standard. Un'estremità è collegata al router on-premise e l'altra al router di AWS DX. Un utente può associare direttamente Direct Connect al Transit Gateway tramite **Transit Virtual Interface (VIF)**. Questa specifica interfaccia è differente da una privata/pubblica perché è collegata direttamente con il Transit Gateway. Ciò consente la connettività a tutte le VPC che condividono un Transit Gateway attachment.

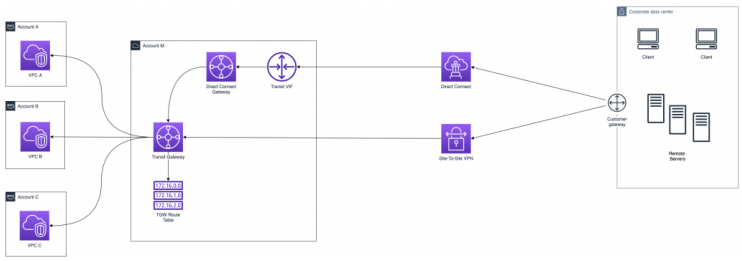
Nota bene! Durante la configurazione, bisogna ricordare che è possibile collegare solo un'interfaccia virtuale per il Transit Gateway per la connessione DX dedicata. Questo limite non può essere aumentato.

Al termine della configurazione, l'azienda desidera utilizzare la **VPN Site-to-Site** come backup. Essa consiste in un collegamento crittografato, chiamato tunnel VPN, che collega gli uffici con AWS. Ogni connessione VPN include due tunnel VPN che si possono utilizzare contemporaneamente per garantire alta disponibilità. Nel nostro caso, i due endpoint saranno il Customer Gateway (CGW) per il lato on-prem e il Transit Gateway per quello AWS.

Si tenga presente che la VPN ha un alcuni limiti che devono essere presi in considerazione per questo progetto:

- Massimo 50 connessioni VPN Site-to-Site per AWS Region.
- Bandwidth massima per tunnel VPN, fino a 1,25 Gbps.

Lo scenario modificato sarà il seguente:



Con questa configurazione aggiornata, il traffico scorrerà principalmente attraverso Direct Connect e, qualora si **verificasse** un **errore sulla DX**, verrà trasferito al **canale VPN di failover**. Lo scopo dell'utilizzo di DX come percorso attivo principale garantisce:

1. Alta velocità, fino a 100 Gbps (solo in alcune regioni AWS)
2. Oltrepassare Internet e quindi evitare eventuale congestione della rete ed altre imprevedibilità.

L'intero routing e il meccanismo di failover è gestito dal protocollo BGP, ed è un requisito necessario che il router gateway del cliente lo supporti. Il funzionamento consiste nel router che invia vari pacchetti (keep alive) per verificare se il percorso DX è attivo. Se viene rilevato un errore, il percorso viene commutato su quello di fallback (VPN). Perciò il Customer Gateway, sia esso software o fisico, deve essere configurato in modo appropriato dall'amministratore di rete per scambiare informazioni di routing tra i vari router. Il dispositivo funziona gestendo una tabella di IP (chiamati prefissi) che fornisce informazioni sulla raggiungibilità delle diverse reti che stiamo osservando.

Quindi, BGP è responsabile dello scambio di annunci di blocchi IP (prefissi IP) ai vari sistemi.
Ma se BGP è responsabile nell'annunciare i prefissi, come sono gestite da AWS le **priorità** delle rotte? Bene, per capirlo bisogna spostare l'attenzione sul Transit Gateway e riassumere l'ordine in una tabella:

Order	Description
1	**Rotte locali** verso la VPC
2	Il **prefisso più specifico**. *Ad esempio,10.0.1.0/24 è preferito piuttosto che 10.0.0.0/16*
3	Voci di **percorso statiche** preferite a quelle **dinamiche**
4	**Rotte Dinamiche** gestite con **BGP**
5	Percorsi statici appresi tramite VPN
6	**Rotte BGP apprese dalla VPN** - Basate sull' AS Path più breve

Quindi, per avere la nostra infrastruttura completamente funzionante, è necessario **notificare lo stesso prefisso** sia per **Direct Connect (VIF)** che per la **VPN**, perché se il CGW notifica gli stessi percorsi verso la VPC di AWS, il percorso tramite Direct Connect è sempre preferito, indipendentemente dall'AS Path prepending.

Per favore, considerando il punto 3 della tabella, si faccia attenzione si configura la VPN Site-to-Site. All'interno del form guidato della VPN, un utente deve specificare "**Dynamic**" come **Routing Option**, altrimenti tutto quanto presentato finora non sarebbe applicabile.

A volte, con questo tipo di configurazione potrebbe verificarsi uno scenario di routing asimmetrico. Il **routing asimmetrico** implica che un pacchetto attraversa da un punto d'origine a una destinazione in un percorso iniziale e prende un secondo percorso diverso quando ritorna all'origine.

Ovvero, il traffico da AWS all'on-premise potrebbe fluire inizialmente attraverso il collegamento Direct Connect, ma per il ritorno, il traffico potrebbe invece attraversare il tunnel VPN.Per risolvere questo problema, si consideri questa guida di AWS che risolve il problema.

Hybrid Cloud

Ora che il networking generale è stato impostato, condivideremo ciò che è possibile ottenere sfruttando queste tecnologie:

- **Latenza e throughput prevedibili:** con AWS DX, è possibile scegliere la giusta banda in base alle proprie necessità. Inoltre, Transit Virtual Interface (VIF) supporta jumbo frames (8500 byte), migliorando di conseguenza il throughput.

Supponiamo quindi di creare una soluzione per l'HPC (High-Performance Computing) con istanze EC2 che opereranno su set di dati di grandi dimensioni, che dovranno essere trasferiti tra la struttura on-prem e il cloud di AWS.

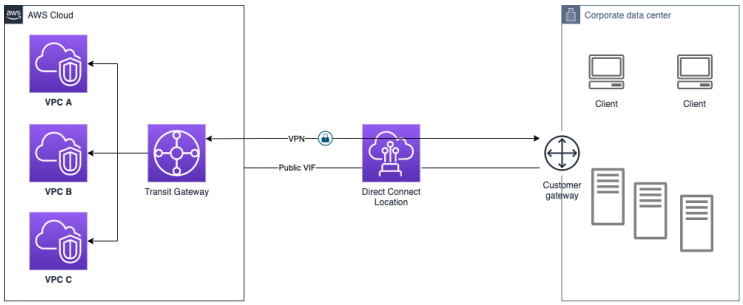
Per velocizzare il trasferimento dei dati, è possibile sfruttare i jumbo frames per inviare i datasets perché più dati verrebbero trasferiti in meno pacchetti. Inoltre, sono anche supportati in modo nativo dall'infrastruttura, comprese le istanze EC2! (solo per la generazione corrente).

- **Un livello di crittografia extra in DX:** E se fosse necessario criptare il canale del Direct Connect per aderire a rigorose conformità riguardo alla sicurezza? Per risolvere la questione è possibile combinare una VPN al Direct Connect.

Se si pensa di utilizzare la VPN Site-to-Site di AWS, ci sarà da considerare dei limiti sulla banda a causa del limite di 1,25 Gbps per il tunnel VPN. Invece, è possibile configurare una VPN IPSec dedicata e sfruttare interamente i 100 Gbps del Direct Connect utilizzando un router di fascia alta. Occhio! Perché potrebbe essere un approccio molto costoso... Solamente gli apparecchi di fascia alta supportano una larghezza di banda così elevata e, ovviamente, non sono per nulla "economici".

Per impostare questa strategia:

1. È necessario prima creare un'interfaccia virtuale pubblica per il Direct Connect.
2. Quindi, una VPN dovrebbe essere configurata come illustrato nell'immagine seguente.
3. Successivamente, si stabilirà una connessione BGP tra AWS Direct Connect e il gateway del cliente sulla VIF pubblica.
4. Infine, una sessione BGP o una rotta statica tra AWS Transit Gateway e il router sul tunnel VPN IPSec.



Questa infrastruttura semplificherà la gestione dell'infrastruttura, minimizzando il costo delle connessioni VPN IPSec a più VPC che sfruttano il Transit Gateway. Inoltre il canale del Direct Connect sarà messo in sicurezza grazie alla VPN.

- **Supporto per la connettività tra diverse Regioni AWS:** Transit Gateway supporta il peering tra regioni. Ciò significa che i Gateway dei Direct Connect collegati a un Transit Gateway (lo stesso discorso si applica anche per le VPN Site-to-Site), ospitato in una specifica regione AWS, possono scambiare traffico con risorse in altre regioni. L'intero traffico attraverserà la **rete globale di AWS** e non sarà esposto su Internet pubblicamente. La rete globale di AWS collega tutte le varie Availability Zones con una rete a bassa latenza e larghezza di banda elevata su fibra ottica dedicata.

Considerazioni

In questo articolo abbiamo illustrato come è possibile aggiungere una VPN Site-to-Site come metodo di fallback per una connessione Direct Connect che collega le strutture on-premise al cloud AWS, e, infine, come si possa beneficiare di una infrastruttura di rete ibrida completamente ridondante.

Facciamo notare nuovamente che una VPN non è progettata per fornire lo stesso livello di larghezza di banda disponibile per la maggior parte delle connessioni Direct Connect, poiché si basa su Internet pubblico, quindi le prestazioni potrebbero essere imprevedibili. D'altra parte, assicura una soluzione affidabile quando il budget è limitato e/o quando è impossibile avere una seconda connessione tramite DX. È necessario disporre di almeno due DX per ottenere un elevato livello di resilienza del 99,9%.

Hai mai considerato questa opzione per il hybrid cloud? O ad una delle soluzioni proposte? Facci sapere cosa ne pensi!

Gabriele Zaccagno

Technical chiacchierone @ beSharp. Mi occupo di Migrazioni Cloud e Data Analytics. Passo le giornate davanti al PC mentre ascolto per intero la discografia dei Radiohead (B-Side comprese).
