Networking per l'Hybrid Cloud: NAT Gateway centralizzato con AWS Transit Gateway

4 Marzo 2022 - 7 min. read

Advanced Networking | *Amazon VPC* | *AWS Transit Gateway* | *Hybrid Cloud* | *Landing Zone* | *NAT Gateway*

Introduzione

Il cloud ibrido è uno scenario sempre più comune utilizzato in molte aziende che hanno la necessità di connettere il loro ambiente on-premises con il cloud in modo sicuro.

Lo scopo di questo articolo è di illustrare un modo per costruire un networking centralizzato su AWS sfruttando un servizio chiamato Transit Gateway. Questa risorsa è molto utilizzata per connettere l'ambiente on-premises con il cloud soprattutto attraverso VPN e Direct Connect e in questo articolo, abbiamo presentato un modo per scegliere la giusta connessione da implementare.

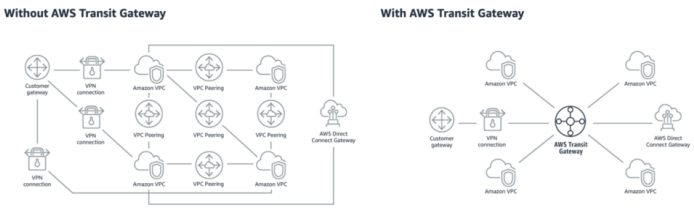
Tuttavia, questo non sarà il focus di questo articolo. L'obiettivo è di presentare come condividere gli stessi NAT gateway in più ambienti attraverso l'utilizzo del transit.

Prima di partire con la descrizione della centralizzazione del networking, è necessario spendere qualche parola per descrivere le caratteristiche del Transit Gateway e come configurare il networking in cloud seguendo le best practice di AWS.

Transit Gateway

Transit Gateway è una risorsa presentata nel 2018 e il suo scopo è di connettere le VPC e l'ambiente on-premises attraverso un unico hub.

Prima del suo avvento, le connessioni tra VPC venivano fatte con il VPC peering e questo portava ad un'architettura molto complessa dove c'erano tante risorse di network collegate fra loro siccome esso non supporta la transitività. Quindi, il primo vantaggio nell'utilizzo del transit è la possibilità di avere la transitività tra le varie VPC connesse e, come mostrato nella figura in basso, questa caratteristica semplifica di molto l'architettura.



Un'altra cosa importante è che è possibile utilizzare un unico account principale con il solo scopo di controllare il networking sul cloud; questo vuol dire che, se una nuova connessione è necessaria, essa può essere configurata solo nella configurazione del Transit senza preoccuparsi delle configurazioni degli ambienti collegati ad esso. Possiamo dare dei permessi granulari al team di networking e centralizzare le connessioni in un unico account con una significativa riduzione dei costi di networking. Siccome abbiamo un unico hub che funge da router per tutte le

connessione, possiamo condividere gli stessi NAT gateway per tutti gli ambienti e, se necessario, creare un'unica connessione VPN.

In questo articolo non entreremo nei dettagli riguardo le connessioni on-premises, ma è importante sapere che possiamo utilizzare il Transit per collegare un'unica Direct Connect e andare in tutti gli ambienti grazie alla transitività.

Networking

Un approccio comune è quello di creare 3 livelli di networking ognuno con 3 subnets per sfruttare tutte le availability zones della regione:

- Livello pubblico: qui ci sono tutte le risorse che hanno bisogno di una connessione per e da internet attraverso l'internet gateway;
- Livello nattato: qui ci sono quelle risorse che sono private (senza un ip pubblico) e necessitano di raggiungere internet ma di non essere raggiunte attraverso internet. Per avere questa caratteristica è necessario utilizzare un NAT gateway;
- Livello privato: qui infine ci sono tutte le risorse che devono essere completamente private, quindi senza connessione internet in nessun verso.

Come descritto precedentemente, il NAT Gateway è la risorsa che permette di raggiungere internet e, se non implementata correttamente, potrebbe diventare il collo di bottiglia per la nostra infrastruttura.

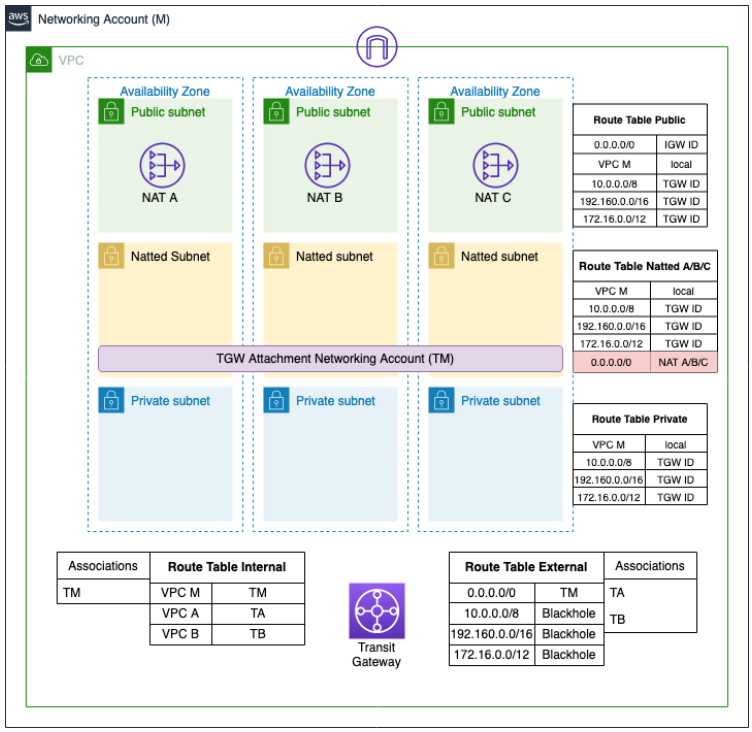
AWS mette a disposizione un servizio gestito per implementare il NAT. Esso ha una banda di 5 Gbps e scala automaticamente fino a 45 Gbps. Per avere l'alta disponibilità, è necessario creare 3 NAT, uno per ogni availability zone. In questo modo abbiamo più banda siccome le risorse sono splittate sulle AZ, ognuna con il suo NAT. Facendo un ragionamento sui costi, bisogna tenere presente che ogni NAT ha un costo di 30$/mese, quindi 90$/mese per 3 NAT in HA e se abbiamo più ambiente, i costi saranno replicati. Ora vedremo come utilizzare gli stessi per NAT per tutti gli ambienti in modo tale da non replicare i costi del NAT.

Configurazione del Transit gateway con NAT centralizzati

L'architettura che andremo a presentare in questo articolo è una landing zone composta da 1 account principale e 2 sotto account chiamati sviluppo e produzione. Per semplicità, li chiameremo M (account principale), A (account di produzione) e B (account di sviluppo).

La struttura della VPC è praticamente la stessa per tutti gli account. La differenza principale sta nell'account principale dove verrà configurato il Transit Gateway con i NAT.

Configurazione della VPC
Iniziamo a configurare l'account M.



Come illustrato nell'immagine, abbiamo configurato una VPC con i 3 livelli di networking e i 3 NAT Gateway per l'alta disponibilità come descritto precedentemente.

I NAT saranno condivisi con tutti gli account attraverso il Transit Gateway. Il prossimo passo è di creare il Transit Gateway è condividerli con gli altri account utilizzando il servizio AWS Resource Access Manager (RAM). Infine, le ultime risorse da creare sono i Transit Gateway attachments. Queste sono le uniche risorse che andranno create in tutti gli account.

N.B. Quando creiamo gli attachments, è importante selezionare le subnet corrette siccome l'attachment andrà ad utilizzare le tabelle di routing delle subnet per indirizzare il traffico. Le subnet corrette sono quelle nattate altrimenti se utilizzassimo quelle private, non riusciremmo ad andare su internet con le risorse private siccome non passerebbero attraverso i NAT.

Per gli account A e B configuriamo le VPC nello stesso modo ma non abbiamo più i NAT gateway e il Transit gateway, solo i 3 livelli delle subnet con i transit gateway attachment. Utilizzeremo gli stessi NAT e il Transit dell'account M.

Tabelle di routing

Finita la costruzione della struttura del networking, lo step finale è di costruire le tabelle di routing per ogni subnet e per il Transit Gateway.

Tabelle di routing del Transit gateway

Le tabelle di routing del Transit Gateway sono presenti **solo** nell'account M e sono state suddivise in due tipi: interna (contiene le regole per indirizzare il traffico proveniente dall'esterno verso l'interno) ed esterna (contiene le regole per indirizzare il traffico proveniente dall'interno verso l'esterno).

La prima è associata solo con il transit gateway attachment dell'account M. Questa definisce il percorso che il traffico deve prendere quando arriva sulla VPC dell'account M. Le rotte al suo interno indirizzano il traffico diretto verso le VPC degli account M, A e B sui corrispettivi attachments TM, TA e TB.

La seconda è associata agli attachment degli account A e B.

Al suo interno, abbiamo definito le rotte per redirigere tutto il traffico verso l'attachment TM e 3 rotte blackhole per tutti gli indirizzamenti privati. In questo modo evitiamo che un sotto account possa raggiungere un altro sotto account a meno di aggiungere una rotta più specifica verso un sotto account.

Tabelle di routing delle Subnet

Per quanto riguarda le subnet, al momento ci siamo limitati a costruirle senza definire se siano pubbliche, nattate o private. Gli elementi che definiscono questa proprietà sono le rotte all'interno delle tabelle di routing. La tabella pubblica ha una rotta verso internet che passa attraverso l'internet gateway, la tabella nattata ha una rotta verso internet che passa attraverso il NAT gateway, mentre la tabella privata non ha nessuna rotta verso internet. Tutte quante indirizzano il traffico per gli indirizzamenti privati verso il Transit gateway in modo da delegare ad esso la loro gestione. Le tabelle delle subnet sono essenzialmente le stesse per tutti gli accounts a meno della tabella nattata. Qui definiamo le rotte in maniera tale che i NAT gateway dell'account M vengano utilizzati dagli altri account.

Natted Table Accoun M	
VPC M	local
10.0.0.0/8	TGW ID
192.168.0.0/16	TGW ID
172.16.0.0/12	TGW ID
0.0.0.0/0	NAT A/B/C

Natted Table Account A/B	
VPC A/B	local
0.0.0.0/0	TGW ID

La tabella natta per l'account M ha la rotta verso internet che passa attraverso il **nat,** mentre per l'account A e B ha la rotta verso internet che passa attraverso il **transit**. Per la prima, è necessario inoltre inserire le rotte che indirizzano il traffico verso indirizzamenti privati al transit, mentre per la seconda non abbiamo bisogno di queste rotte siccome tutto il traffico è indirizzato di default al transit.

Fatto! In questo modo stiamo utilizzando gli stessi NAT gateway per tutti gli ambienti collegati al Transit gateway. Quindi, se vogliamo fare un test di connettività, possiamo accendere un'istanza ec2 in una subnet nattata in uno dei due sub-account e provare a pingare 8.8.8.8 per vedere se usciamo su internet.

Nell'immagine di sotto è illustrata la configurazione dell'infrastruttura che abbiamo costruito.

Conclusioni

In questo articolo abbiamo presentato come configurare una landing zone con la centralizzazione dei NAT in un unico ambiente sfruttando il Transit Gateway. Esso permette di avere solo un unico hub centrale in cui gestiamo tutto il networking, evitiamo di replicare le risorse di networking e riduciamo i costi e la complessità architetturale.

Nicholas Farina

DevOps Engineer @ beSharp. Mi occupo dell'implementazione e della gestione di infrastrutture Cloud su AWS. Ma questa non è la mia unica passione: sono un amante del crossFit e un pescatore. Di pesci... ed opportunità!
