VPC shared VS multi-VPC: scegliere la migliore infrastruttura di rete per la tua azienda

29 Settembre 2023 - 9 min. read

Advanced Networking | Amazon VPC | governance and compliance | Landing Zone

Introduzione

Come abbiamo visto nello scorso articolo, ormai quando si parla di infrastrutture di rete per la nostra Landing zone non pensiamo più soltanto al Transit Gateway ma a una gamma di possiblità più ampia.
La vera domanda che dobbiamo porci adesso è capire quando utilizzare un opproccio a discapito di un altro, capendo quali benefici o svantaggi questa decisione porterà con se.

Nel corso di questo articolo cercheremo di esporvi i vantaggi e gli svantaggi di ognuna delle soluzioni e, successivamente, portarvi anche dei piccoli esempi di use-case per ognugna di queste soluzione.

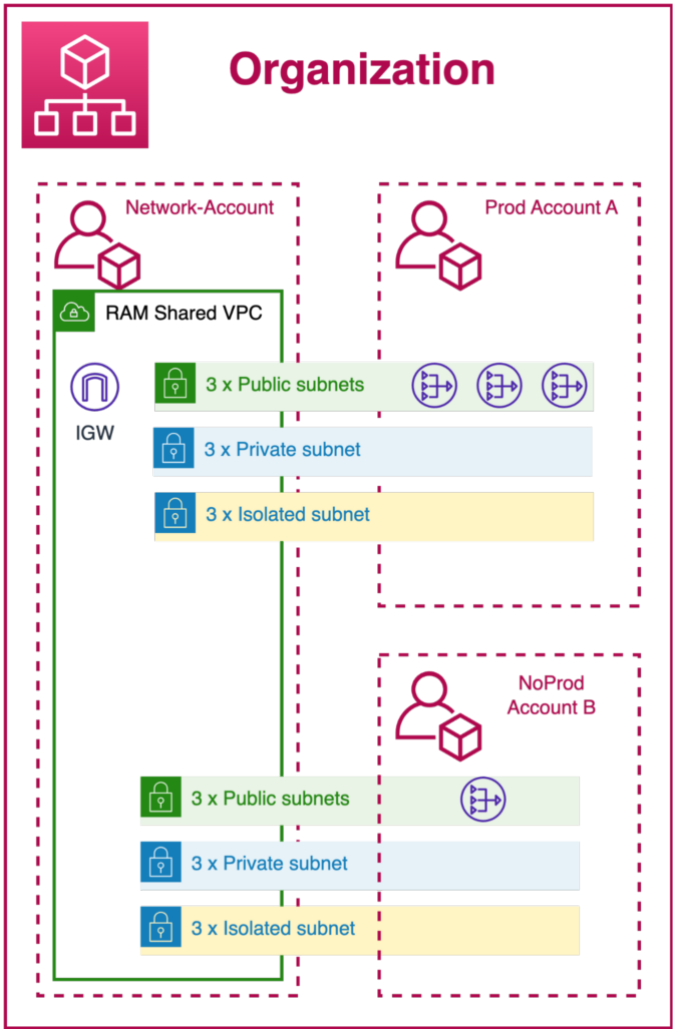
Use Cases

Dopo aver capito quali sono le varie possibilità che abbiamo per configurare la rete della nostra landing zone, capiamo quali potrebbero essere alcuni scenari possibili che ci aiuteranno a capire quale approccio fa al caso nostro e delle nostre esigenze.
Di seguito proveremo a proporre 3 possibili scenari e insieme capiremo quale delle possibilità si adatta a quello descritto. Ricordiamo che magari potreste avere esigenze particolari non contemplate in questo articolo, quello che vi proponiamo noi sono solo delle linee guida per prendere le vostre decisioni senza imporre una vera e propria regola.

Use case Singola VPC condivisa

Poniamoci nel caso più popolare; un'azienda che ha deciso di appoggiarsi al cloud per tutta la sua infrastruttura è che molto probabile nell'arco degli anni ha fatto proliferare il numero dei suoi account. Per la nostra azienda ipotetica, tematiche come la Landing Zone, la gestione dei costi e la centralizzazione dei servizi principlai è orami pane cuotidiano.
Purtroppo però l'IT non è cresciuto al pari passo degli applicativi e del buisiness quindi, spesso si trovano a combattere contro il troppo overhead per gestire la loro infrastruttura.
In questo caso tra tutte le varie opzioni, la singola VPC condivisa potrebbe essere proprio quel tassello che darà una marcia in più all'operatività quotidiana del nostro IT, senza dover rinunciare a tutti i benefici di scalabilità e compliances che siamo abbiatuti a vedere in una Landing Zone ben strutturata.
A differenza di come avremmo con un Transit Gateway, con questa soluzione potremo gestire la rete di tutti gli account direttamente da una console centralizzata nel nostro "network-account". Come spiegato nell'articolo precedente, quando ci riferiamo a "network-account" intendiamo un account AWS all'interno della nostra Organization adibito alla creazione della VPC e di tutte le sue subnet che successivamente verranno condivise coi vari account.
Poter modificare le rotte, creare nuove subnet e gestire il traffico cross-account direttamente da una console ci permetterà di risparmiare moltissimo tempo che andrebbe "speso" per cambiare account con l'assumeRole o con il nostro portale di SSO qual'ora fossimo federeati con il nostro IDP. Per quanto ormai la gestione multi-account sia diventata la quotidianità per questo genere di aziende, poter risparmiare del tempo significativo ci aiuterebbe meglio a concentrarci su tematiche più importante come la security e la segregazione. Un altro punto a favore per questa soluzione sta nella segregazione dei permessi legati alle risorse di rete negli account applicativi. Gestendo l'ownershi della VPC all'interno del nostro account centralizzato, potremo limitare i permessi IAM legati agli utenti che lavorano sui vari account, così anche da assicurarci che configurazioni errate possano provocare dei buchi per la nostra sicurezza di rete.
Se volessi aggiungere un altro tassello alla nostra ipotetica azienda potremmo dire che i vari applicativi, presenti sui nostri account, spesso devono comunicare tra loro per scambiarsi informazioni preziose e necessarie per fornire un servizio di qualità a dei possibili clienti.

Se vi siete trovati già in questa situazione sicuramente saprete che in questi casi i costi extra-VPC la fanno da padrone. Ricordiamoci che su AWS il traffico che rimane all'interno di una VPC e il traffico che passa da una VPC ad una ltra (anche nella stessa region di AWS) hanno due costi significativamente diversi. Se poi immaginiamo che si trovi anche un Transit Gateway tra le due VPC i costi aumentano ancora.



Anche in questo caso la singola VPC condivisa con AWS RAM ci permetterà di abbatere tutti questi costi accessori.
Il traffico dei nosti pacchetti pur spostandosi da una subnet ad un altra, o da un account ad un altro, rimarrà sempre all'interno della nostra singola VPC non andando ad incappare nei costi accessori menzionati poco fa.

Facendo una piccola postilla su questa situzione, se durante il nostro percorso su AWS avessimo deciso di implementare ABAC come metodologia di gestion accessi, questa decisione potrebbe non funzionare bene con questa architettura di rete. La soluzione più semplice sarebbe taggare nuovamente le risorse una volta che le subnet saranno condivise.

Use case Transit Gateway

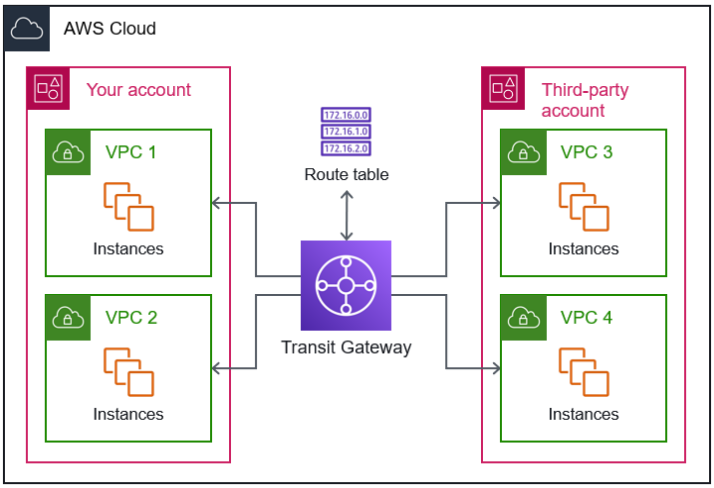
Se prima abbiamo parlato di un'azienda di medie dimensioni che ha basato l'infrastruttura sul cloud, opra parliamo di una grande multinazionale che sta compiendo la sua migrazione verso il cloud al fine di modernizzare i suoi applicativi. Rispetto all'esempio di prima il numero dei dipendenti IT e di persone in grado di gestire la rete è sicuramente maggiore. Immaginiamo anche che ogni azienda che comporrà la nostra Company avrà il suo IT dedicato e che tra loro abbiano anche differenti modi di lavorare. Sicuramente in questo caso la Singola VPC condivisa causerebbe soltanto problemi avendo troppi attori coinvolti nella sua configurazione. La secelta più saggia ricade sull'approccio Transit Gateway e sulla creazione di almeno una VPC in ognuno degli account della nostra Organization AWS. Come nell'altro esempio, anche qui, avremo un account centrale dove risiederà il Transit Gateway e a cui probabilmente avranno accesso soltanto alcuni responsabili IT o figure di particolare spicco tecnitco. Per tutti gli altri account invece, i singoli dipartimenti IT saranno liberi di creare rotte interne, dhcp reservetion, network ACl e quant'altro per far si che l'operatività cuotidiniana dell'azienda contunui senza intoppi.
Il Tranist Gateway risulta la scelta più vantaggiosa in questo ambito dato che molto probabilmente per la nostra Landing Zone non avremo optato per una singola region ma bensi per svariate. Questa decisione magari sarà stata presa per avvicinare le sedi sparse per il mondo ai datacenter dove risiedono effettivamente le VM, così da ridurre al più possibile la latenza.

Tale implementazione multi-region non sarebbe possibile utilizzando il metodo della VPC Shared dato che appoggiandosi su un servizio "regionale" come RAM, potremo adoperare le subnet condivise con i nostri account solo qualora ci trovassimo nella stessa Region originaria della VPC.

Un'altra situazione che ci spinge verso questa soluzione è la possibilità di attestare sul Transit Gateway tutte le VPN S2S proveniente dalle nostre sedi on-premise verso il Cloud. Questa operazione è necessaria per consentire ai gestori IT di operare al meglio sulle numerosissime Virtual Machine del loro parco macchine.

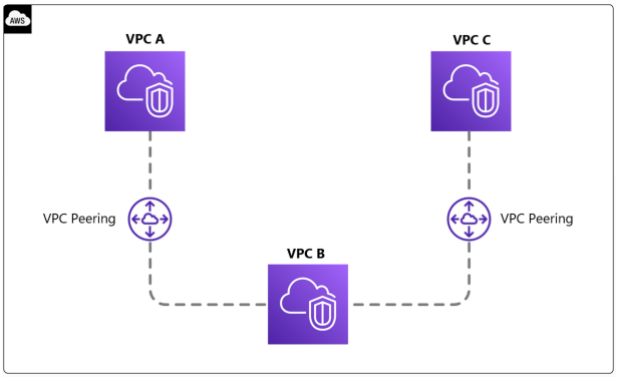
Come descritto nella sezione del Transit Gateway dello scorso articolo, tutto il traffico e il routing potranno essere gestiti con la modifica delle routing table assegnate ad ogni Transit Gateway Attachment. Ci basterà configurare le rotte in modo tale che ogni sede on-premise possa raggiungere soltanto il suo corrispettivo account AWS. Questo ci porterebbe anche ad un grado di sicurezza abbastanza elevato qual'ora un malintenzionato cercasse di fare del "Lateral Moving" all'interno della nostra rete.

Purtroppo se per questo approccio dovesse bastare tale configurazione delle routing table, per la VPC condivisa potrebbe risultare più macchinoso restringere questo genere di problematiche. Essendo tutte le subnet comunicanti tra di loro e non potendo creare rotte (all'iterno delle routing table) più esclusive del nostro CIDR l'unico modo per segregare ogni gruppo di subnet sarebbe adottare delle network ACL molto stringenti.



Use case VPC Peering

Dopo aver parlato di medie e grandi imprese, non ci resta che trattare lo scenario emergente ovvero piccole aziende o sturtup. Possiamo immaginarci questa azienda come ai suoi albora e che dopo i suoi primi passi sul cloud ha deciso di abbozzare una Landing Zone in formato ridotto. Quando pensiamo a questo genere di aziende non dobbiamo immaginarci sedi disparse per il mondo, smisurate quantità di account, particolare gestione per policy di compliance e sicuramente la presenza forte di un IT dedicato. Gli unici due aspetti che possiamo identificare come principali nella progettazione della nostra lanfing zone sono i costi e la facilità di gestione.
Se parlaimo di infrastrutture di rete che rispecchino questi due principipi la scelta non può che ricadere nel VPC Peering. La semplicità di questa funzionalità, che molto spesso la esclude dalla pool di possibile soluzioni, in questo caso la rende la perfetta candidata per rispecchiare al meglio le nostre esigenze chiare e ben definite.



In questo scenario la nostra Landing Zone sarà composta da un numero davvero ridotto di account, lasciando perdere gli account spesso adibiti alla gestione della sceruty e all'auditing. Anche per quanto riguarda il network-accont risulta superfluo e quindi tranquillamente trascurabile.

Con il VPC peering potremo mettere in comunicazione i nostri due applicativi che sono stati rilasciati su due account distinti (o che magari sono stati realizzati in due momenti diversi) semplicemente con pochi click. Sicuramente l'utilizzo del peerign non ci permetterò di adoperare funzionalità complesse e articolate come si potrebbe fare con un Transit Gateway, ma nel nostro caso non sarà un problema dato che la gestione della rete non sarà uno dei nostri principali interessi per questa fase del nostro sviluppo su AWS.

Purtroppo il peering non sarà una soluzine definitiva se intendiamo far creasce la nostra azienda, e di conseguenza la nostra AWS organization, nel arco dei prossimi anni. Il difetto principle di questa soluzione è la sua scalabilità che, con il creascere degli account, perde il suo principio di semplicità e aggiunge moltissimo overhead di gestione.
Comunque questa potrebbe essere una fase di transizione per consolidarci sul cloud, prima di adottare una soluzione più strutturata come VPC Share o Transit Gateway

Conclusione

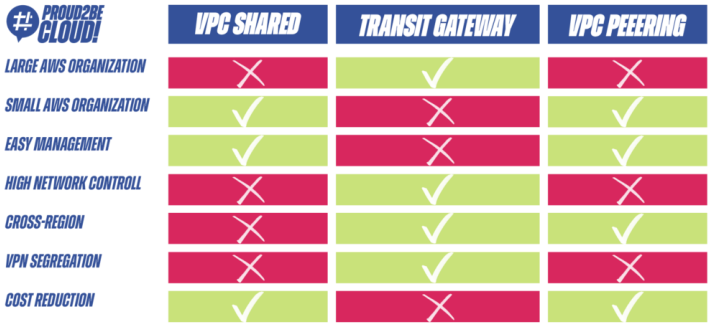
Come ogni volta è il momento di tirare delle conclusioni su quanto abbiamo trattato nel corso di questi due articoli sul networking centralizzato in una lading zone e le varie possibili infrastrutture.

Abbiamo visto che ognuna delle varie possibilità che ci vengono messe a disposizione da AWS ha i suoi vantaggi e svantaggi non che particolari casi di utilizzo.

Sarebbe difficile dire quale di queste soluzione sia la migliore perchè come spesso accade la risposta è "dipende". Sicuramente il primo step è capire quali sono le esigneze dalla nostra azienda e quali valori vogliamo portare avanti durante la creazione della Landing Zone. Come molto spesso è stato spiegato su questo blog, la progettazione di una Landing Zone è qualcosa che va studiato nei minimi dettagli e adattato alle richieste, come se fosse un vestito sartoriale su misura.

Ricordiamoci anche che una infrastruttura ben progettata ci accompagnerà nel percorso di crescita della nostra azienda. Per questo, cerchiamo di progettare una soluzione che riesca a creascere di pari passo con le nostre esigenze e di conseguenza con la creascita della nostra Landing Zone su AWS

Una volta capita quale struttura la nostra Landing Zone adotterà, sarà necessario interfacciarsi con gli steackholder dei nostri applicativi per capire anche dal loro punto di vista che esigenze potremmo aver trascurato o non tenuto in considerazione. Ricordiamoci che un'infrastruttura ad hoc e che permette a tutti di lavorare in maniera efficente e sicura è sempre la starada da intraprendere in fase di progettazione e rinnovo.



About Proud2beCloud

Proud2beCloud è il blog di beSharp, APN Premier Consulting Partner italiano esperto nella progettazione, implementazione e gestione di infrastrutture Cloud complesse e servizi AWS avanzati. Prima di essere scrittori, siamo Solutions Architect che, dal 2007, lavorano quotidianamente con i servizi AWS. Siamo innovatori alla costante ricerca della soluzione più all'avanguardia per noi e per i nostri clienti. Su Proud2beCloud condividiamo regolarmente i nostri migliori spunti con chi come noi, per lavoro o per passione, lavora con il Cloud di AWS. Partecipa alla discussione!

Riccardo Fragnelli

DevOps @beSharp.Ho un passato on-prem prima di redimermi con il Cloud. Molto pignolo e abbastanza pigro. Mi piace passare il tempo fra videogiochi e GDR. Con AWS ho scoperto una branca dell’informatica tutta nuova che mi affascina sempre di più.
