Networking Avanzato: Come nattare il traffico AWS con qualsiasi IP privato

29 Aprile 2022 - 6 min. read

Advanced Networking *AWS Transit Gateway* *Hybrid Cloud* *Landing Zone* *NAT Gateway*

Introduzione

In un modello Hybrid Cloud ci sono un sacco di complessità riguardanti il networking quando vogliamo creare un perfetto ecosistema tra il cloud e l'ambiente on premises.

In particolare, una connessione attraverso una VPN site-to-site è molto delicata siccome possiamo avere diverse complicanze, ad esempio la sovrapposizione dei CIDR degli ambienti.

Un altro problema potrebbe essere quando si vuole stabilire una VPN e dall'altra parte ci sono delle limitazioni per quanto riguarda la dimensione di rete della VPC e non possono riservare ad esempio una rete /16 per una connessione ma una rete /27. O ancora, in un caso peggiore, bisogna utilizzare una rete /27 che non appartiene alla stessa classe di CIDR della VPC.

Nello specifico, l'ultimo è un caso reale che ci è capitato durante la configurazione di una vpn tra la nostra architettura su AWS e un ambiente on premises.

La terza parte non poteva stabilire una connessione con lo spazio di rete della nostra VPC siccome troppo esteso (/16) ed inoltre, si sovrapponeva.

In un ambiente on premises non ci sarebbero stati problemi siccome è possibile nattare sotto uno spazio di rete il traffico verso un altro ambiente creando una rete

virtuale ma nel cloud questo non è possibile di default.

Per cui abbiamo dovuto scegliere uno spazio di rete più piccolo che andasse bene per entrambi da utilizzare per nattare il nostro traffico verso di loro e, allo stesso tempo, permettere loro di raggiungere i nostri applicativi collocati in spazi di rete differenti.

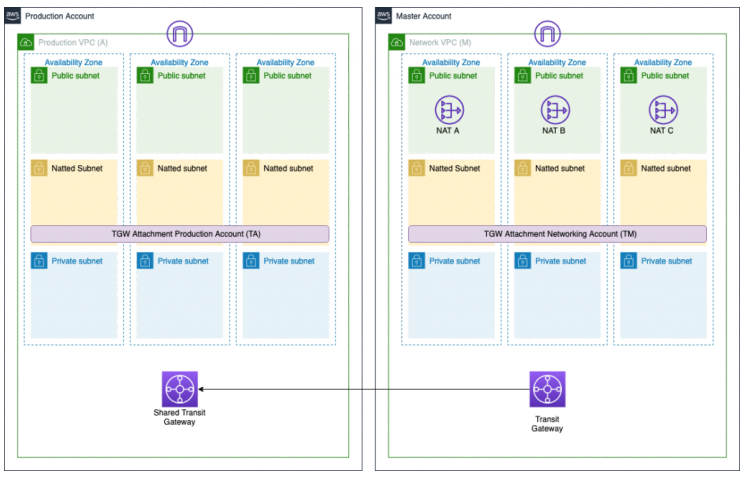
Non ci concentreremo sulla spiegazione delle caratteristiche dei componenti di networking. In uno dei nostri prercedenti articoli abbiamo presentato come configurare gli account con il transit gateway e i nat centralizzati. Questo articolo si può considerare come un'estensione dei concetti teorici descritti, quindi consigliamo di dargli un'occhiata per comprendere al meglio i contenuti che stiamo per affrontare.

L'architettura

Supponiamo di aver già creato una piccola landing zone composta da due account - master e produzione - ognuno con la sua VPC collegata tramite il transit gateway (la stessa architettura presentata nell'articolo al link precedente, ma, per semplicità, con solamente gli account master e produzione).

Il master account è responsabile della configurazione del networking mentre nell'account di produzione abbiamo il nostro applicativo. Vogliamo creare una connessione VPN con un ambiente on premises che deve accettare e inviare il traffico solo ad una rete con CIDR /27 diverso dai CIDR delle VPC di master e produzione. Che cosa è possibile fare in questo caso? Cominciamo con la parte divertente e disegnamo una soluzione a questo problema.

La nostra configurazione del networking per i due account è la seguente illustrata in figura.



Qui abbiamo i due account presentati precedentemente, connessi attraverso il transit gateway. I cidr delle loro VPC sono 10.100.0.0/16 per il master account (VPC M) e 10.150.0.0/16 per l'account di produzione (VPC A). L'ambiente on premises deve creare una connessione VPN con i nostri due account quindi dobbiamo stabilire la connessione solo con l'account master e dopodichè sfruttare la transitività del transit gateway per allargare la connessione all'account di produzione. Il problema è che l'ambiente on premises ha già parecchie connessioni VPN e il cidr 10.100.0.0/16 non è disponibile e sarebbe comunque troppo ampio per stabilire una singola connessione VPN. Scegliamo quindi di utilizzare il cidr 10.179.0.0/27 (è importante scegliere una dimensione di rete sufficiente in modo da evitare il rischio di non avere sufficienti IP).

In poche parole, dobbiamo nattare tutto il traffico in uscita dagli account master e produzione verso la VPN dietro questo cidr.

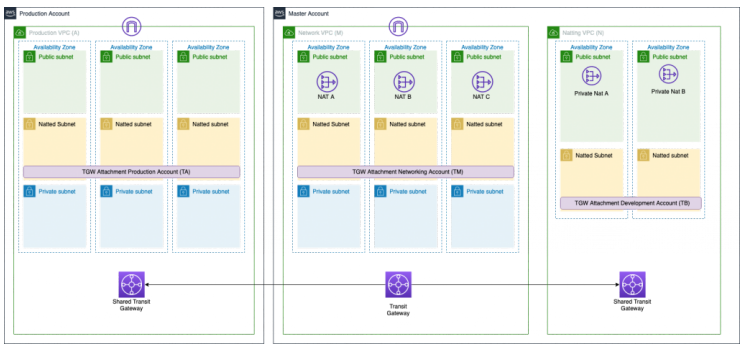
Configurazione della VPC

Creiamo una nuova VPC nell'account master da usare come rete virtuale in modo da nattare il traffico diretto alla vp.

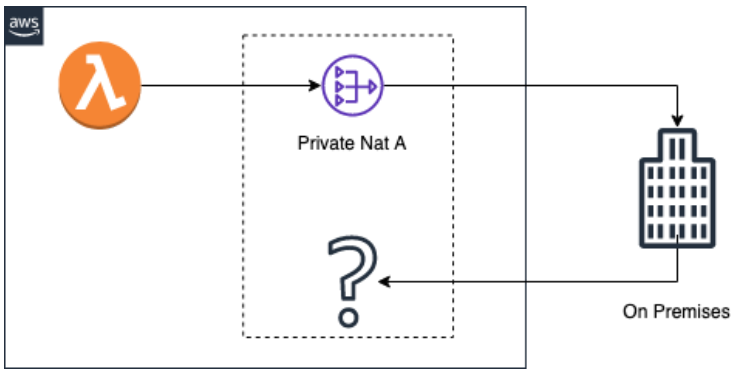
Questa VPC con CIDR 10.179.0.0/16 (per semplicità la chiameremo VPC N) aggiunge un livello di networking in più di fronte alla VPC M.

Nota: se ti stai chiedendo come mai non abbiamo esteso il cidr della vpc, fai bene. Avremmo potuto aggiungere un ulteriore cidr alla vpc e raggiungere lo stesso risultato ma la differenza rispetto alla creazione di una nuova VPC è che il cidr deve appartenere alla stessa classe del cidr primario: ad esempio se il CIDR è all'interno dello spazio di indirizzi 10.x.x.x/8, non puoi usare un cidr all'interno degli altri spazi di indirizzamento privati definiti dal RFC1918 (192.168.x.x/16 and 172.16.x.x/12).

Lo schema architetturale diventa quindi quello mostrato nella figura sottostante.



Con una /27 possiamo creare solo 2 subnet pubbliche con cidr 10.179.0.0/28 e 10.179.0.16/28 e 2 subnet nattate con cidr 10.179.0.32/28 e 10.179.0.48/28. Le subnet pubbliche sono le due che possono comunicare con l'ambiente on premises mentre le subnet nattate sono necessarie per redirigere il traffico diretto verso l'ambiente on premises attraverso il NAT. Infine, nelle subnet pubbliche creiamo i 2 NAT gateway privati che nattano tutto il traffico proveniente dalla VPC M e dalla VPC A. **Notare** che questo è un nat sorgente cioè è utilizzato solamente dal traffico proveniente dagli ambienti aws, quindi il traffico proveniente dall'ambiente on premises necessita di un altro instradamento per comunicare con le VPC A e M.



L'immagine di sopra è una rappresentazione per capire meglio come viene instradato il traffico tra i due ambienti ma al momento solo l'applicativo (una lambda ad esempio) può raggiungere l'ambiente on premises e non viceversa.

Configurazione del Transit

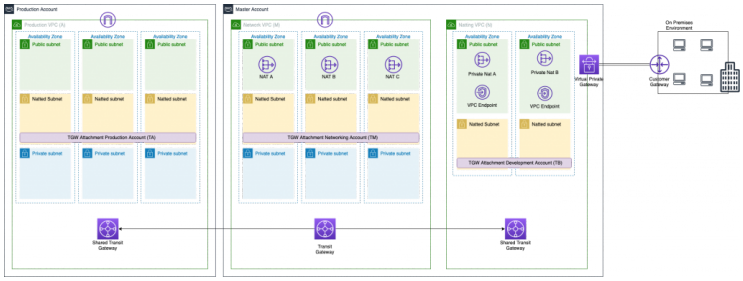
Dopo aver creato la VPC, dobbiamo configurare il transit gateway in modo tale da stabilire la connessione tra le VPC esistenti e quella appena creata. Creiamo un nuovo transit gateway attachment nelle subnet nattate della VPC N e aggiungiamo nelle tabelle del transit le rotte dirette verso gli IP on premises attraverso l'attachment dell VPC N.

Configurazione della VPN

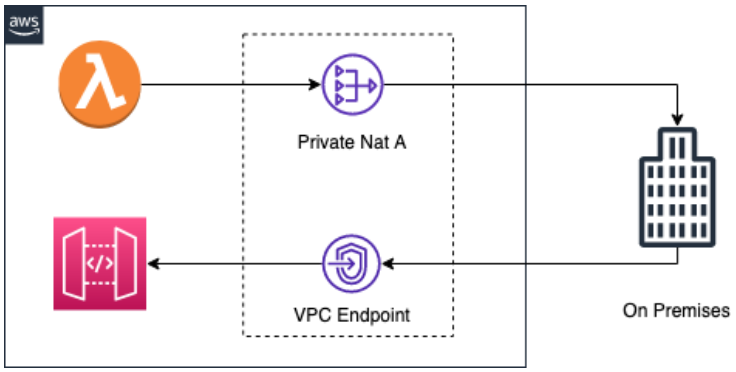
L'ultima cosa che rimane da fare è creare la VPN N. Creiamo una VPN site-to-site direttamente con la VPC N, quindi senza attaccarla al transit gateway ma al virtual private gateway.

Il setup è concluso! Possiamo provare a pingare una macchina on premises da una ec2 all'interno della VPC M o A e se tutto è ok dovremmo vedere il traffico provenire da uno dei due IP dei nat gateway privata all'interno della VPC N.

L’architettura completa è quella mostrata in figura.



Come detto precedentemente, il problema che ha portato a questa soluzione è stato il fatto che l’ambiente on premises può riservare solo una rete /27 per stabilire una connessione VPN, quindi loro possono contattare solo gli ip della rete 10.179.0.0/27. Come possono contattare i nostri applicativi all’interno della VPC A con cidr 10.150.0.0/16?



Come mostrato in figura, In base al tipo di applicazione, l’unica cosa che possiamo fare è creare dei vpc endpoint, per esempio per raggiungere un api gateway. Questi assumono degli ip all’interno del range 10.179.0.0/27 ma l’unico protocollo che possiamo utilizzare è HTTP/S.

Inoltre, abbiamo un numero limitato di ip quindi dobbiamo tenere a mente che possiamo creare solamente un numero limitato di vpc endpoint.

Considerazioni

Anche se inventare questa soluzione non è stato esattamente un gioco da ragazzi - anche per il fatto che non abbiamo trovato casi simili sul web - siamo molto contenti perché ci ha permesso di risolvere questa particolare esigenza di networking.

La bellezza di questa soluzione è dovuta al fatto che per ogni VPN che necessitiamo di creare, se ci sono particolari limitazioni come quella presentata, basta creare una VPC specifica con l’unico scopo di stabilire una connessione vpn. L’altra parte della medaglia è che questo comporta dei costi di networking maggiori siccome bisogna

creare un transit gateway attachment e 2 NAT gateway. Inoltre, è necessario creare un vpc endpoint per ciascun servizio che necessitiamo di contattare dall'ambiente on premises. È importante tenere a mente tutti questi aspetti prima di implementare questa soluzione.

Conosci un altro modo per risolvere questo problema? Faccelo sapere nei commenti :)

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!

Simone Merlini

CEO e co-fondatore di beSharp, Cloud Ninja ed early adopter di qualsiasi tipo di soluzione *aaS. Mi divido tra la tastiera del PC e quella a tasti bianchi e neri; sono specializzato nel deploy di cene pantagrueliche e nel test di bottiglie d'annata.

Copyright © 2011-2022 by beSharp srl - P.IVA IT02415160189