Apunte #4: Clase del 10-10-23

Instituto Tecnológico de Costa Rica. Escuela de Ingeniería en Computación. Redes - IC-7602. Grupo 2. Profesor: Gerardo Nereo Campos Araya Estudiante: Daniel Araya Sambucci - 2020207809 Fecha de entrega: 16/10/23

Proyecto

Para dar acceso a internet a la red privada se le da un NAT Gateway. Al definirle en la tabla de ruteo a 0.0.0.0 la salida por el NAT Gateway, a esto se le define una IP. Cuando una máquina va a sacar información, esta corre una tabla de ruteo dentro de la máquina. Esto saca el tráfico por la tabla de ruteo de Amazon. Entonces la máquina manda el tráfico a la tabla de ruteo y esta lo manda al NAT Gateway, lo que hace que salga a internet.

En el proyecto en vez de sacar el tráfico por el NAT, se debe sacar a través de una máquina. Se debe hacer que la máquina viva en dos redes. Una tarjeta de red se debe pegar en la red pública y otra en la tarjeta privada. Esto implica que la máquina agarre una IP de la red privada.

Entonces, se pone una VM en la red privada. Por defecto ella se va al NAT y luego a internet. Para evitar esto, vía chef o vía User Data, se sobreescribe la tabla de ruteo de la máquina (la interna). Para hacer esto se puede agregar otro default Gateway, con una métrica que nos funcione más. Al ejecutar la tabla de ruteo en la máquina, le da prioridad a otra salida hacia internet.

Otra forma de realizarlo, en redes de Amazon, es no dejar que viva en las dos sub redes. Se deja en la red pública y en vez de decirle en la tabla de routeo de Amazon que vaya al NAT, se le dice que vaya a la VM.

Para todos los Cloud Providers, la red recibe un router de algún tipo. Cuando se definen redes adentro, el tráfico sale a través de las redes por medio del IP público. Al probar el vpn, esto se hace externo. No se define en las VM ya que si se va a internet a través del router y luego a la otra máquina, eso es un round trip, entonces es perder ancho de banda y el router no lo permite. Si se desea conectar una VM como cliente del VPN, entonces se maneja la IP interna, para evitar este problema.

Si se levanta la VPN en la VM, entonces se corta la conexión SSH, ya que esta es la que transfiere la consola de la máquina virtual.

Por otra parte, al instalar un servicio DNS, este es aparte de Apache, de Nginx y de Squid. Todos son servicios completamente separados. Squid es un servicio que corre solo y no es necesario usar el DNS que definimos. Esto es lo mismo para Apache y Nginx.

Cuando uno le envía un request al DNS, este remplaza el dominio con una IP. Lo siguiente que se identifica es el protocolo que se está usando para meterse a una máquina (HTTP por ejemplo). Esto corresponde a la capa de aplicación. Luego viene la capa de red y transporte, que corresponde a la IP que se dio, por puerto 80. Esto corresponde a la conexión.

En el caso de que el DNS se esté reiniciando al usar Ubuntu es debido a que el DNS se está escuchando a cada rato en un servicio llamado resolv.conf. Entonces está siempre revisando que tenga los valores correctos y lo sobre escribe. Entonces se desactiva ese servicio para solucionar el problema.

En el caso de Oracle es muy parecido. Se tienen dos redes con sus máquinas. En la pública la VM agarra acceso a internet. En la VM privada se le define un ip route add para redefinir la ruta por defecto. A veces los Cloud Providers bloquean esto, entonces se le puede definir una ruta para poder sacar el tráfico.

Capa de Transporte

Se cuenta con 2 protocolos principales que son los que han construido internet. Normalmente se le conoce a internet como TCP/IP, pero existe otro protocolo llamado UDP (User Datagram Protocol). Este es un protocolo sin garantía. Se envían paquetes y no interesa si llegan. Si el paquete se dañó al viajar o no llegó, no pasa nada.

TCP tiene dos entidades de transporte. Estas se comunican una con al otra y TCP garantiza que los paquetes que salen de una máquina lleguen a la otra. Lo asegura mediante time outs y retries.

En UDP, al bajar algo, entonces si se daña algo a UDP no le importa. No obstante, a la capa de aplicación si le importa esto. En las capas del modelo OSI, si algo falla en una capa, una que está más arriba lo atrapa, pero mientras más arriba más costoso es mantener estos errores.

Una aplicación de esto es por ejemplo en la transmisión de video en tiempo real, en un streaming de datos. Se usa UDP ya que si se pierde un frame por ejemplo, no se pueden guardar los otros frames en buffer hasta que se tenga el que se perdió porque esos que vienen son más recientes. Entonces lo que se hace es que se ignora, puede haber un pequeño corte y luego sigue normal.

Zoom pasa todo por el puerto TCP 443, ya que todo mundo usa https, todo mundo lo tiene abierto.