México, Ciudad de México

¿ASEGURAR AWS CON SONICWALL VIRTUAL O UNA VPN PUNTO A PUNTO?

José Maria Salas/Hugo Ariel Mateos
Praxis, Gerencia Cloud

RESUMEN

La información es quizás el bien más importante dentro de un centro de datos, es de gran importancia para la toma de decisiones, por lo cual no se puede desestimar la seguridad, es de vital relevancia prestar atención a cómo vamos a cuidar dicha información.

En el modelo de Centro de Datos Físico además de la seguridad lógica, se debe de poner especial atención en la seguridad física, en aspectos como:

- Perímetro de seguridad física
- Controles físicos en la entrada
- Protección contra amenazas externas y ambientales
- Ubicación y protección del equipo
- Suministros de apoyo
- Mantenimiento de equipo
- Monitoreo y revisión de los servicios del proveedor
- Planificación en la continuidad de la seguridad de la información
- Disponibilidad de instalaciones de procesamiento de la información

Aun cuando en el modelo de Infraestructura en la nube, no debemos de preocuparnos por el tema de la seguridad física, ya que ésta debe estar cubierta por el proveedor de nube que elijamos, si deberemos de considerar la seguridad lógica, en este tipo de seguridad, esto ya no depende completamente del proveedor de nube sino de quien hace uso de los servicios. Entre los peligros a los que estamos expuestos en la parte lógica de la seguridad están:

- Vulnerabilidades de software
- Intrusión en la red
- Denegación de Servicio Distribuido, DDoS (*Distributed Denial of Service*)

Aun cuando físicamente no tengamos acceso a un centro de datos en la nube, no se puede desestimar la seguridad, ya que la información que está contenida en nuestros recursos

virtuales siempre estará expuesta a posible robo o pérdida.

PALABRAS CLAVE:

SEGURIDAD, VPN, FIREWALL, AWS.

INTRODUCCIÓN

Existen diversos métodos de brindar seguridad a la información que se encuentra alojada en un centro de datos, así como también la información que viaja por Internet. En este documento se analizarán a grandes rasgos la puesta en operación de dos tipos de soluciones, así como pros y contras desde el punto de vista del integrador.

Se va a integrar la seguridad de una infraestructura creada para proveer funcionalidades Web en la nube pública de *Amazon Web Services* (AWS) y la infraestructura física de un cliente la cual incluye *firewall*. Se integrarán ambas infraestructuras para que la comunicación entre ellas fluya como si estuvieran en la misma red física.
Analizaremos las siguientes opciones:

La infraestructura en la nube con una solución de firewall virtual con un AMI (*Amazon Machine Image*) de un tercero marca Sonicwall que se obtiene desde el *Marketplace* de AWS, misma marca que el *Firewall* Físico.

La infraestructura en la nube que se conectará a la infraestructura física a través de una *Virtual Private Network* (VPN) punto a punto, con dos túneles por cada VPN.

DESARROLLO

LA INFRAESTRUCTURA EN LA NUBE

Cada entorno consiste en “n” *Virtual Private Cloud* (VPC), con “n” subredes públicas, dentro de ésta se encuentran dos instancias montadas en *Windows Server* con *Internet Information Service* (IIS) habilitado como servidor web.

La comunicación entre las instancias en la nube y los equipos físicos deberá ser a través de las IP’s privadas cuidando que la infraestructura en la nube y la física tengan un CIDR (*Classless Inter Domain Routing* «Enrutamiento entre Dominios sin Clase») diferente.

FIREWALL EN LA NUBE

Para la implementación del *firewall* virtual en la nube se deberá de seguir los pasos utilizados comúnmente para crear una instancia con cualquier

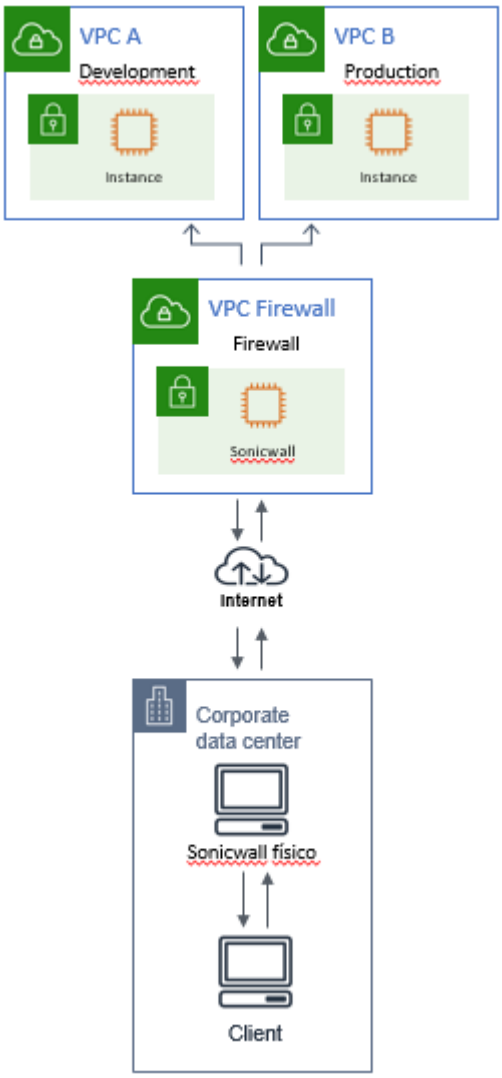
distribución de *Amazon Machine Image* (AMI).

- Firmarse en la consola AWS
- Crear un nueva VPC con una Subred Privada (Lan) y una Pública (Wan)
- Desde el menú de instancias de *Elastic Cloud Computing* (EC2)
- Lanzar una nueva instancia
- En la pestaña de AWS Marketplace buscar Sonicwall
- Elegir el tipo de instalación
- Seleccionar el tipo de instancia
- En los detalles de configuración de la instancia
- Seleccionar la VPC y la Subred correspondiente
- Añadir una interfaz de red (son necesarias al menos 2 interfaces de red para que pueda funcionar)
- Aceptar el almacenamiento por default
- Añadir los tags necesarios
- Configurar el grupo de seguridad con al menos Secure Shell (SSH) y Hypertext Transfer Protocol Secure (HTTPS)
- Una vez creada la instancia, deshabilitar "*source/destination check*"
- Asignar una IP Elástica a la instancia
- Conectarse a través de la nueva IP Elástica
- Modificar la tabla de ruteo de la Lan, añadiendo el destino 0.0.0.0/0 hacia la interface Lan.
- Modificar la tabla de ruteo de la Wan, añadiendo el destino 0.0.0.0/0 hacia el *Internet Gateway*.

El proceso detallado se puede encontrar en el sitio oficial de Sonicwall.[1]

Aunque el proceso de cómo crear una instancia con el AMI de Sonicwall puede parecer lo suficientemente detallado, existen huecos que no permiten que con el sólo hecho de seguir las instrucciones se logre completar un perímetro, lo único que se consigue es tener un "n" número de VPC's y una instancia con Sonicwall en otra VPC completamente aislada y que básicamente funciona como una simple consola.

[1] https://www.sonicwall.com/techdocs/pdf/nsv-series-on-aws-getting-started-guide.pdf



"Elaboración propia del autor"

COMUNICACIÓN

Para que exista una comunicación entre el *Sonicwall* de la nube y las instancias de AWS que se deseen proteger, la conectividad se debe realizar a través de un "*Peering Connection*". Esto no es más que una interconexión entre dos VPC's, que permite enrutar el tráfico entre ambas a través de sus IP's privadas. Al utilizar la misma infraestructura de AWS, no funciona como un Gateway ni requiere de un recurso de hardware.

Una vez completado el proceso de creación del *Peering Connection* se deberán de configurar las Tablas de Ruteo de cada VPC, de modo que el destino de cada una de ellas deberá ser el CIDR de la VPC a la cual deseamos comunicar, este procedimiento se realizará las tablas de ruteo de cada VPC que se desee comunicar.

Completado lo anterior, contaremos con la comunicación entre ambas VPC's, pero no será posible comunicar con el Sonicwall, por las mismas propiedades del firewall.

REGLAS

Por defecto la comunicación hacia la interfaz *Lan* de la Instancia *Sonicwall* existirá hasta que se creen las configuraciones necesarias en el *Sonicwall*. Se necesita que el tráfico pase de una VPC a otra a través del *firewall*, para lo cual es indispensable crear una regla para cada VPC que tengamos que conectar.

La nueva regla de ruteo en el *firewall* deberá de tener lo siguiente:

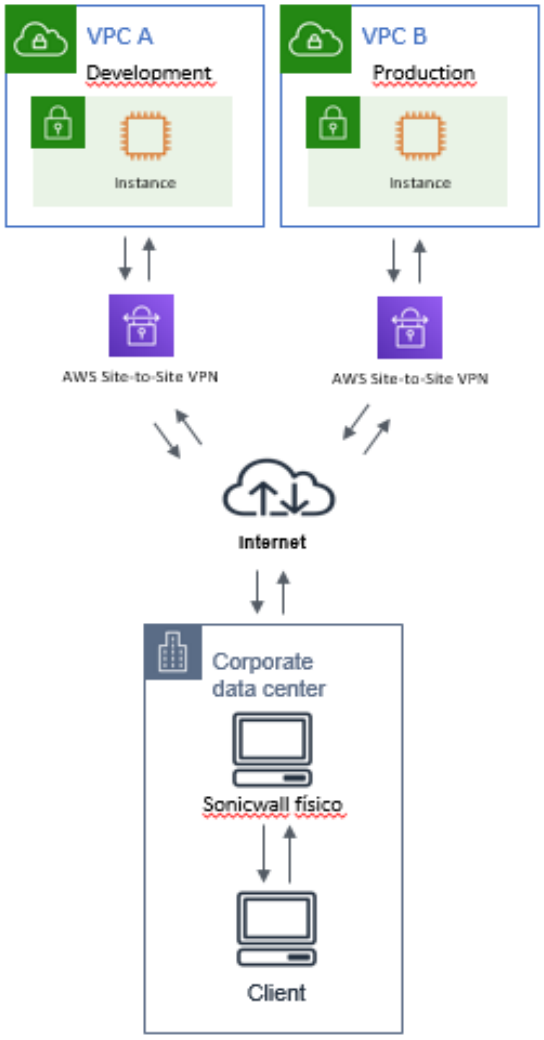
- *Source*, es la instancia, dispositivo, interfaz de red.
- *Destination*, es el CIDR de la VPC al que deseamos comunicar.
- *Service*, son los protocolos que se van a permitir.
- *Interface*, es la interfaz a través de la cual se va a comunicar con la VPC.
- *Gateway*, es la puerta de enlace por donde va a pasar todo el tráfico entre las VPC's.

Una vez completada la configuración de la nueva regla de ruteo en el *Sonicwall*, se tendrá la conectividad y protección propia del *firewall*.

VPN PUNTO A PUNTO DE AWS

Para crear la VPN punto a punto, básicamente se requieren de 3 componentes:

1. *Customer Gateway*, que representa el destino hacia donde deseamos hacer la conexión, aquí se especifica la IP del firewall físico.
2. *Private Virtual Gateway*, representa el *endpoint* de la conexión de AWS, en este caso el id de la VPN que deseamos comunicar.
3. *VPN Connection*, es la unión de los dos componentes previamente creados y que brindara la configuración que se utilizara para el *firewall* físico, deberemos proporcionar el CIDR de la red física para poder comunicar, al finalizar este paso, tendremos un archivo de configuración el cual utilizaremos para configurar el *firewall* físico con los valores que se nos proporcionan en dicho archivo.



"Elaboración propia del autor"

CONCLUSIÓN

A pesar de contar con el respaldo, la experiencia de una marca especialista en seguridad, en este caso *Sonicwall*, tiene una complejidad adicional el agregar una instancia con un software de seguridad como lo fue en este caso, además de la dificultad para realizar la configuración.

AWS está incorporando cada vez más funcionalidades, así como mejorando las que ya tiene, por lo anterior, resulta mucho más fácil la configuración y operación de una solución propia de Amazon que incluir el soporte de un tercero, al utilizar las soluciones propias minimiza el riesgo de falla en alguno de los componentes o problemas en la configuración.

REFERENCIAS

SIN AUTOR. How do I create a secure connection between my office network and Amazon Virtual Private Cloud? De AWS Sitio web: https://aws.amazon.com/es/premiumsupport/knowledge-center/create-connection-vpc/.

SIN AUTOR. What is VPC Peering? De AWS. Sitio web: https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.ht

México, Ciudad de México

José María Salas Fontana
Gerente de Especialidad Cloud.

55 5080 0048 Ext. 1121
sxfm@praxis.com.mx
https://www.linkedin.com/in/josemariasalas