Detección de ataques de Denegación de Servicios en la Nube

Seminario de Redes de Computadores IPD-438

Dayana Hernández Rodríguez
Universidad Técnica Federico Santa María
Valparaiso, Chile
dayana.hernandez@usm.sansano.cl

***Resumen*—Los ataques de denegación de servicios persiguen dejar a los usuarios legítimos de un servicio sin este. Los ataques de denegación de servicios de forma distribuida han ido incrementándose cada año, siendo uno de los ataques más rápidos y eficientes que dejan totalmente a las empresas sin acceso a sus activos. La computación en la Nube se ha convertido en una nueva forma de proveer un servicio de infraestructura, plataforma y software a través de Internet. Junto con todas las ventajas que implica tener los servicios en la Nube se levantan grandes retos, como mantener la seguridad de estos servicios. Los ataques de denegación de servicios en la Nube constituyen uno de los ataques más probables y más dañinos, por lo que se han propuesto varias configuraciones para prevenirlos, detectarlos y mitigarlos. Los ataques de seguridad en la Nube tienen la particularidad de dejar a otros clientes sin servicios, además de los clientes que son objetivo del ataque, por lo que los proveedores de la Nube deben tener mecanismos de seguridad robustos que eviten los ataques que ponen en peligro la seguridad de todos sus clientes. En este trabajo tenemos el objetivo de detectar un ataque TCP SYN Flood en un ambiente simulado usando GNS3, haciendo una analogía de un ataque de denegación de servicio contra la Nube.**

***Index Terms*—Nube, Seguridad, Denegación de servicios**

I. Introducción

Con el rápido desarrollo de las tecnologías de procesamiento y almacenamiento y el éxito de Internet, los recursos informáticos se han vuelto más baratos, más potentes y están más disponibles que nunca. Esta tendencia tecnológica ha permitido la realización de un nuevo modelo de computación llamado computación en la nube (*Cloud Computing*), en el que los recursos (por ejemplo, CPU y almacenamiento) se proporcionan como utilidades generales que los usuarios pueden arrendar y liberar a través de Internet en forma de pedido. La computación en la Nube es un avance tecnológico en el suministro de infraestructura, plataforma y software como servicios a través de Internet. La computación en la Nube está siendo adoptada gradualmente por organizaciones como nubes privadas, públicas o híbridas, que ven en esta nueva tecnología una forma de mejorar sus servicios de IT (*Information Technology*) sin necesidad de un gasto excesivo en recursos que lo soporten. La adopción de la computación en la Nube presenta una serie de beneficios sobre los centros de datos tradicionales, como la agilidad mejorada (a pedido, autoservicio, recursos elásticos), la rápida provisión de servicios, la escalabilidad de los servicios, la mejor utilización de los recursos y la reducción de los costos operativos. Las tendencias recientes favorecen la adopción de la computación en la Nube y muestran que las plataformas de computación en la Nube o los centros de datos basados en la Nube procesarán más carga que los centros de datos tradicionales. Cisco predice que para los próximos años los centros de datos basados en la Nube procesarán más de tres cuartos de la carga que procesan los centros de datos tradicionales [1].

Una encuesta realizada por International Data Corporation sugiere que los problemas de seguridad en la computación en la Nube son el desafío principal en la adopción de la misma. Para que las organizaciones hagan la transición a la Nube, es importante para los proveedores garantizar un nivel significativo de seguridad para los clientes. Los clientes pagan por tener sus servicios IT en la Nube, pero además por la seguridad de estos. Junto con los mecanismos de seguridad existentes, como los firewalls y los sistemas de Detección de Intrusión (IDS), los proveedores también pueden tener mecanismos de seguridad integrados en la arquitectura de la Nube para garantizar un alto nivel de seguridad para los clientes. Una empresa que tenga alojados su servicios en la Nube y estos servicios sean atacados, provoca un daño no solo económico sino de prestigio de la empresa que muchas veces puede ser irreversible.

Los ataques de denegación de servicio (*Denial of Service*, DoS) y de denegación de servicio distribuido (*Distributed Denial of Service*, DDoS) son uno de los ataques más comunes en Internet hoy en día. Los ataques DoS tienen como objetivo agotar los recursos de un sistema de manera que comprometa su capacidad para proporcionar el servicio deseado y, por lo tanto, dejarlo indisponible. El informe anual de seguridad 2014 de Cisco clasifica los efectos de los ataques DoS con una magnitud de alta severidad [2]. Los ataques DoS se dirigen principalmente a sitios web aunque también pueden paralizar a los proveedores de servicios de Internet. Por ejemplo, en agosto de 2013, el gobierno de China informó que el mayor ataque DDoS al que se había

enfrentado había cerrado Internet en ese país durante unas cuatro horas [2]. En un entorno de servicios en la Nube, no solo existe el peligro de un ataque desde el exterior a uno de los servicios alquilados por un cliente, sino además existe el peligro de un ataque desde el interior, es decir es posible que el atacante contrate servicios con el proveedor de servicios en la Nube y este desde dentro ataque los servicios de otros clientes en la misma Nube. Además los ataques en la Nube tienen la particularidad de que es posible cuando se ejecuta un ataque contra un cliente determinado, ese ataque afecte a los demás clientes en la Nube. Por lo que los proveedores de servicios tienen que ser capaces de prevenir, detectar y mitigar los ataques de denegación de servicios tanto desde el exterior como desde el interior de la Nube y que puedan afectar a todos los clientes de la Nube. Se han propuesto varias arquitecturas que permiten detectar los diferentes tipos de ataques de denegación de servicios en la Nube, siendo importante realizar un de estudio de los aspectos relacionados con la denegación de servicios y las configuraciones de seguridad que se deben realizar para detectarlos a tiempo. El presente trabajo tiene el objetivo de detectar un ataque TCP SYN Flood en un ambiente simulado usando GNS3, haciendo una analogía de un ataque de denegación de servicio contra la Nube. Debido a la limitación de recursos tecnológicos a nuestra disposición, se decide hacer la analogía entre un ambiente simulado y los servicios reales en una Nube. La presentación del tema en cuestión, a lo largo del artículo, está dividido en cuatro partes fundamentales, en la primera parte se da una visión general de la computación en la Nube, una segunda parte que presenta una visión general de los ataques de denegación de servicios, una tercera parte donde se analizan los ataques de denegación de servicios específicamente en la Nube, y por último se presenta el escenario propuesto y se analizan los resultados alcanzados.

II. Visión general de la computación en la nube

El término de Nube surge desde que el CEO de Google Eric Schmidt en 2006 usó la palabra para describir un nuevo modelo de negocio de proveer servicios a través de Internet. Desde ese momento el término se volvió popular, pero no existía una definición exacta de lo que significaba un servicio en la Nube por lo que el NIST (*U.S. National Institute of Standards and Technology*) se dio la tarea de conceptualizar el término. Para tener una idea más amplia de lo que significa un servicio en la Nube, la siguiente lista resume los cinco criterios que hacen que un servicio se defina como un servicio de computación en la Nube basado en la definición del NIST [3].

1) **Autoservicio a pedido**: el consumidor de IT elige cuándo iniciar y dejar de usar el servicio, sin ninguna interacción directa con el proveedor del servicio.
2) **Amplio acceso a la red**: el servicio debe estar disponible desde muchos tipos de dispositivos y a través de muchos tipos de redes (incluida Internet).
3) **Agrupación de recursos**: el proveedor crea una agrupación de recursos (en lugar de dedicar servidores específicos para uso exclusivo de ciertos consumidores) y asigna dinámicamente recursos de esa agrupación para cada nueva solicitud de un consumidor.
4) **Elasticidad rápida**: para el consumidor, el grupo de recursos parece ser ilimitado (es decir, se expande rápidamente, por lo que se denomina elasticidad), y las solicitudes de un nuevo servicio se completan rápidamente.
5) **Servicio medido**: el proveedor puede medir el uso y reportar dicho uso al consumidor, tanto por transparencia como por facturación.

II-A. Arquitectura de Niveles de la Nube

Según [4] la arquitectura de un entorno de computación en la Nube se puede dividir en 4 capas: la capa de hardware/centro de datos, la capa de infraestructura, la capa de plataforma y la capa de aplicación, como se muestra en la Figura 1. Se describe cada una de ellas en detalle:

La capa de hardware: esta capa es responsable de administrar los recursos físicos de la nube, incluidos los servidores físicos, enrutadores, conmutadores, sistemas de alimentación y refrigeración. En la práctica, la capa de hardware normalmente se implementa en centros de datos. Un centro de datos generalmente contiene miles de servidores que están organizados en racks e interconectados a través de switches y routers. Los problemas típicos en la capa de hardware incluyen la configuración del hardware, la tolerancia a fallos, la gestión del tráfico, la administración de las fuentes de alimentación y las fuentes de refrigeración.

La capa de infraestructura: también conocida como la capa de virtualización, la capa de infraestructura crea un conjunto de recursos de almacenamiento y computación mediante la partición de los recursos físicos utilizando tecnologías de virtualización como Xen, KVM y VMware. La capa de infraestructura es un componente esencial de la computación en la Nube, ya que muchas características clave, como la asignación dinámica de recursos, solo están disponibles a través de las tecnologías de virtualización.

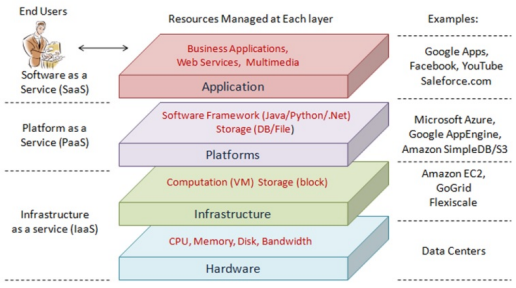

Figura 1. Arquitectura de Niveles en la Nube [4]

La capa de plataforma: Construida sobre la capa de infraestructura, la capa de plataforma consta de sistemas operativos y marcos de aplicaciones. El propósito de la capa de plataforma es minimizar la carga de implementar aplicaciones directamente en contenedores de máquinas virtuales. Por ejemplo, Google App Engine opera en la capa de la

plataforma para proporcionar soporte de API o implementar la lógica de almacenamiento, base de datos y negocios de las aplicaciones web típicas.

La capa de aplicación: Es el nivel más alto de la jerarquía, que consta de las aplicaciones reales de Nube . A diferencia de las aplicaciones tradicionales, las aplicaciones en la Nube pueden aprovechar la función de escalado automático para lograr un mejor rendimiento, disponibilidad y menores costos operativos.

La arquitectura de niveles de la Nube es similar al Modelo OSI para protocolos de red. La modularidad de la arquitectura permite que la Nube sea compatible con una amplia gama de requerimientos de aplicaciones y a la vez reduce la administración y los gastos generales de mantenimiento.

II-B. La Nube y el modelo "como servicio"

El mundo de la computación en la Nube trabaja en un "modelo de servicios". Las empresas en lugar de comprar hardware, licencias de software y realizar gastos en la instalación de estos, deciden convertirse en clientes de un proveedor de servicios de Nube. La idea de recibir un servicio, es más abstracta que la idea de comprar un servidor e instalar un paquete de software en particular. Así que con la computación en la Nube, en lugar de mantener la discusión tan genérica, la industria usa una variedad de términos que finalizan en: "como un Servicio" (*as a Service*, aaS). Cada término "-aaS" tiene un significado diferente [3].

1) **Infraestructura como servicio (IaaS):** IaaS se refiere a la demanda de aprovisionamiento de recursos infraestructurales, generalmente en términos de máquinas virtuales(VM). El propietario de la Nube que ofrece IaaS se llama Proveedor de IaaS. El cliente decide la cantidad de rendimiento / capacidad de hardware para asignar a la VM (número de CPU virtuales, cantidad de RAM, etc.). Como ejemplo de este tipo de servicio es Amazon Web Services (AWS), un proveedor de nube pública, desde el cual se puede crear una máquina virtual como parte de su servicio IaaS.
2) **Plataforma como servicio (PaaS):** PaaS se refiere a proporcionar recursos de capa de plataforma, incluido el soporte del sistema operativo y los frameworks de desarrollo de software. Un servicio de PaaS es como IaaS en algunos aspectos. Ambos suministran al consumidor una (o más) máquinas virtuales, con una cantidad configurable de CPU, RAM y otros recursos. La diferencia clave entre PaaS y IaaS es que PaaS incluye muchas más herramientas de software más allá del sistema operativo básico. Esas herramientas son útiles para un desarrollador de software durante el proceso de desarrollo. Como ejemplos podemos encontrar el App Engine PaaS de Google y el entorno de desarrollo integrado de Eclipse.
3) **Software como servicio (SaaS)**: SaaS se refiere al suministro de aplicaciones bajo demanda a través de Internet. El proveedor de la Nube puede usar muchas máquinas virtuales para crear el servicio, pero estos requerimientos de hardware están ocultos para el consumidor. El proveedor de la Nube otorga licencias, instala y le da el soporte necesario al software. Los servicios de almacenamiento de archivos como Apple iCloud, Google Drive, Dropbox y Box son ofertas de SaaS.

II-C. Topologías de la Nube

Hay muchos aspectos que se deben tener en cuenta al mover una aplicación empresarial al entorno de Nube. Por ejemplo, algunos proveedores de servicios están interesados principalmente en reducir los costos de operación, mientras que otros pueden preferir alta confiabilidad y seguridad. En consecuencia, hay diferentes tipos de nubes, cada una con sus propios beneficios e inconvenientes [4]:

Nubes públicas: una nube en la que los proveedores de servicios ofrecen sus recursos como servicios al público en general. Las nubes públicas ofrecen varios beneficios claves, incluida la ausencia de inversión de capital inicial en infraestructura y el desplazamiento de los riesgos a los proveedores de infraestructura. Sin embargo, las nubes públicas carecen de un control preciso sobre los datos, la red y la configuración de seguridad, lo que dificulta su eficacia en muchos escenarios empresariales.

Nubes privadas: también conocidas como nubes internas, las nubes privadas están diseñadas para uso exclusivo de una sola organización. Una nube privada puede ser construida y administrada por la organización o por proveedores externos. Una nube privada ofrece el mayor grado de control sobre el rendimiento, la confiabilidad y la seguridad. Sin embargo, a menudo se les critica por ser similares a las granjas de servidores propietarios tradicionales y no proporcionan beneficios, como no tener costos de capital iniciales.

Nubes híbridas: una nube híbrida es una combinación de modelos de nube pública y privada que trata de abordar las limitaciones de cada enfoque. En una nube híbrida, parte de la infraestructura del servicio se ejecuta en nubes privadas, mientras que la parte restante se ejecuta en nubes públicas. Las nubes híbridas ofrecen más flexibilidad que las nubes públicas y privadas. Específicamente, brindan un control y seguridad más estrictos sobre los datos de la aplicación en comparación con las nubes públicas, al tiempo que facilitan la expansión y la contracción del servicio a pedido. En el lado negativo, el diseño de una nube híbrida requiere determinar cuidadosamente la mejor división entre los componentes de la nube pública y privada.

La definición del NIST para la computación en la Nube enumera el "*acceso amplio a la red*" como uno de los cinco criterios principales. El uso de Internet para comunicarse entre una empresa y un proveedor de nube pública es fácil y conveniente pero introduce problemas como Seguridad, Capacidad y Calidad de Servicios. Otra forma de conexión soportada es el uso de conexiones WAN dedicadas. En las Figuras 2 y 3 se aprecian las diferentes topologías que podemos usar para acceder a los servicios contratados en una Nube Pública y en la Tabla I se hace una comparación donde se establecen las ventajas y desventajas de cada una de

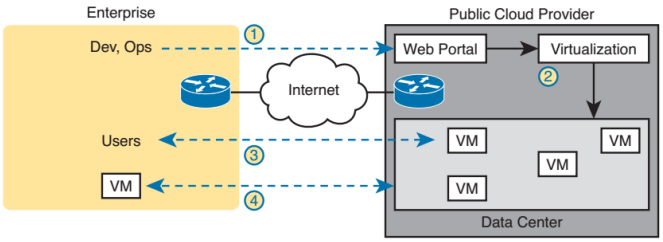

Figura 2. Acceso a la Nube a través de Internet [3]

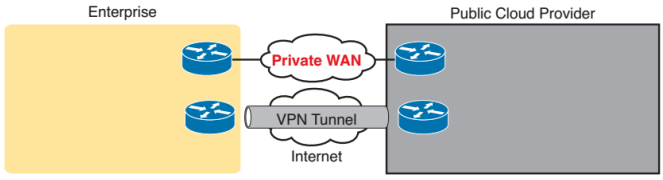

Figura 3. Acceso a la Nube a través de WAN [3]

las opciones de acceso a la Nube Pública. En función de las necesidades de la empresa que decida contratar un servicio, y de las opciones que maneje el proveedor de servicios de la Nube, se decide cual es la mejor opción para implementar.

	Internet	Internet VPN	MPLS VPN	Ethernet WAN	Intercloud Exchange
Secure	No	Yes	Yes	Yes	Yes
QoS	No	No	Yes	Yes	Yes
Requires capacity planning	Yes	Yes	Yes	Yes	Yes
Easier migration to new provider	Yes	Yes	No	No	Yes
Can begin using public cloud quickly	Yes	Yes	No	No	No

Tabla I
COMPARACIÓN DE LOS DISTINTOS TIPOS DE CONEXIÓN A LA NUBE [3]

III. VISIÓN GENERAL DE ATAQUES DE DENEGACIÓN DE SERVICIOS

Los ataques de denegación de servicio (**DoS**) y de denegación de servicio distribuido (**DDoS**) son uno de los ataques más comunes en Internet hoy en día. Un ataque de denegación de servicio (DoS) es un ataque que impide que un usuario legítimo acceda a un recurso de la red. Un ataque de denegación de servicio distribuido (DDoS) es uno que usa múltiples recursos de red como la fuente del vector de ataque específico. Un ataque DDoS se lanza desde numerosos dispositivos comprometidos, a menudo distribuidos globalmente en lo que se conoce como **botnet**. Es distinto de otros ataques de denegación de servicio (DoS), ya que utiliza un solo dispositivo conectado a Internet (una conexión de red) para inundar un objetivo con tráfico malicioso. En la Figura 4 se muestra un ataque de denegación de servicios distribuido.

Dentro del ambiente de la seguridad de la información, los ataques DDoS se encuentran dentro del pilar "Disponibilidad" de la tríada de la CIA como se puede ver en la Figura 5. DDoS se diferencia de otras áreas de explotación de la seguridad de la información que intentan

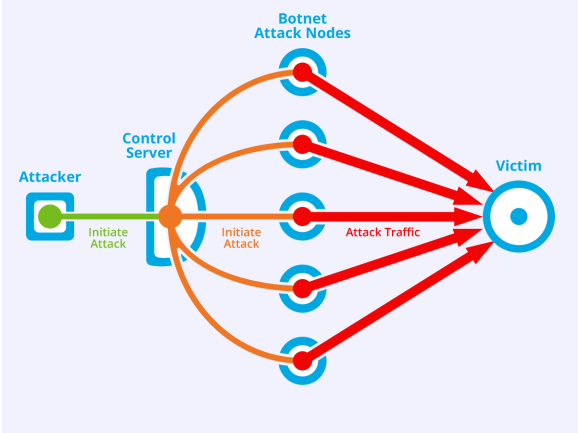

Figura 4. Ataque de denegación de servicios distribuido [6]

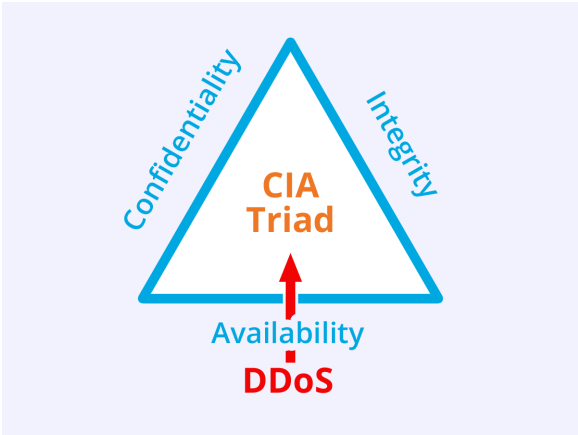

Figura 5. Ataque de denegación de servicios distribuido [6]

alterar u obtener acceso a los datos para causar daños. Los ataques DDoS se basan en la noción de que el acceso de usuarios legítimos a los datos, es lo que posee valor para una organización, y eliminar ese acceso causa el mayor daño.

Los ataques de DoS se pueden clasificar en tres categorías [5]:

1) **Ataques de DoS basados en el volumen**: afectan a los servidores cuando se dirige un gran volumen de ese tráfico. Algunos ejemplos son el ICMP flood y los ataques de UDP flood.
2) **Ataques DoS basados en protocolo**: utilizan protocolos específicos de Internet para consumir los recursos del servidor. Algunos ejemplos son el ataque de TCP SYN flood y el Ping-of-death.
3) **Ataques DoS basados en aplicaciones**: estos se dirigen a las debilidades de las aplicaciones en Internet. También se conoce como ataques de la capa de aplicación y algunos ejemplos son el ataque de Slowloris y el ataque de amplificación de DNS.

Los ataques DDoS se están convirtiendo rápidamente en el tipo más frecuente de amenaza cibernética, creciendo rápidamente en el último año, tanto en número como en

volumen. La tendencia es hacia una duración de ataque más corta, pero un volumen de ataque de paquete por segundo más grande [5].

Los atacantes están motivados principalmente por [6]:

Ideología: los llamados 'hacktivistas' usan los ataques DDoS como un medio para atacar sitios web con los que no están de acuerdo ideológicamente.

Peleas en los negocios : las empresas pueden usar los ataques DDoS para eliminar estratégicamente los sitios web de los competidores, por ejemplo para evitar que participen en un evento importante como el Cyber Monday.

Aburrimiento: los vándalos cibernéticos, 'script-kiddies' usan scripts preescritos para lanzar ataques DDoS. Los perpetradores de estos ataques suelen estar aburridos, los posibles hackers que buscan una descarga de adrenalina.

Extorsión: los perpetradores usan ataques DDoS o la amenaza de ataques DDoS como medio de extorsionar el dinero de sus objetivos.

Guerra cibernética: los ataques DDoS autorizados por el gobierno se pueden usar para paralizar sitios web de la oposición y la infraestructura de un país enemigo.

Existen varios tipos de ataques de DDos entre los más utilizados por los ciber-atacantes tenemos [9]:

UDP Flood: El ataque UDP flood, por definición, es cualquier ataque DDoS que inunda un objetivo con paquetes del Protocolo de Datagramas de Usuario (UDP). El objetivo del ataque es inundar puertos aleatorios en un host remoto. El host receptor verifica las aplicaciones asociadas con estos datagramas y, al no encontrar ninguno, envía un paquete de "Destino inalcanzable". A medida que se reciben y contestan más y más paquetes UDP, el sistema se ve abrumado y no responde a otros clientes. El protocolo UDP no requiere el saludo *Three-Way Handshake* que usa TCP, por lo que se ejecuta con menor sobrecarga y es usado para las aplicaciones que son sensibles al retardo en la red. Sin embargo estas propiedades hacen que UDP sea más vulnerable al uso por parte de atacantes. Debido a la ausencia del establecimiento de la conexión acordada por las dos partes, para establecer una conexión válida, se puede enviar un gran volumen de tráfico de "mejor esfuerzo" a través de los canales UDP a cualquier host, sin protección incorporada para limitar la tasa de flood DoS de UDP. Esto significa que no solo los ataques de UDP flood son altamente efectivos, sino que también pueden ejecutarse con relativamente pocos recursos.

ICMP Flood (Ping): Similar en principio al ataque de UDP flood, un ICMP flood agota los recursos del destino con paquetes *ICMP Echo Request* (ping), generalmente enviando paquetes lo más rápido posible sin esperar respuestas. Este tipo de ataque puede consumir ancho de banda entrante y saliente, ya que los servidores víctimas del ataque, intentarán responder con los paquetes *ICMP Echo Reply*, lo que resultará en una importante desaceleración general del sistema.

Ping of Death: Un ataque de ping of death ("POD") implica que el atacante envíe múltiples pings malformados o maliciosos a una computadora. La longitud máxima de paquete de un paquete IP (incluido el encabezado) es de 65.535 bytes. Sin embargo, la capa de enlace de datos generalmente establece límites para el tamaño máximo de trama, por ejemplo, 1500 bytes a través de una red Ethernet. En un escenario de Ping of Death, luego de una manipulación maliciosa del contenido del fragmento, el destinatario termina con un paquete IP que es más grande que 65,535 bytes cuando se vuelve a ensamblar. Esto puede desbordar los buffers de memoria asignados para el paquete, causando la denegación de servicio para paquetes legítimos.

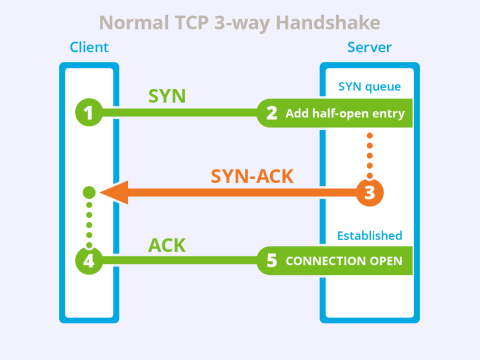

Figura 6. TCP three-way handshake [6]

TCP SYN Flood: El three-way handshake normal de TCP hace que el cliente envíe un paquete SYN inicial al servidor. El servidor agrega la conexión medio abierta a su tabla de estado de conexión interna (cola de sincronización) y luego responde con un SYN-ACK. En una conexión normal, el cliente responde con un ACK. En este punto se establece la conexión y la comunicación puede ocurrir, esto se puede apreciar en la Figura 6. En un ataque SYN flood, el atacante envía paquetes SYN repetidos a todos los puertos del servidor de destino, a menudo utilizando una dirección IP falsa. El servidor, inconsciente del ataque, recibe múltiples solicitudes aparentemente legítimas para establecer comunicación, respondiendo a cada intento con un paquete SYN-ACK de cada puerto abierto. El cliente malintencionado no envía el ACK esperado o, si la dirección IP está falsificada, nunca recibe el SYN-ACK en primer lugar. De cualquier manera, el servidor atacado esperará el reconocimiento de su paquete SYN-ACK durante algún tiempo. Durante este tiempo, el servidor no puede cerrar la conexión enviando un paquete RST, y la conexión permanece abierta. Antes de que la conexión se agote, llegará otro paquete SYN. Esto deja un número cada vez mayor de conexiones medio abiertas. Eventualmente, a medida que se llenan las tablas de desbordamiento de conexión del servidor, se negará el servicio a los clientes legítimos y el servidor puede incluso fallar. En la Figura 7 se muestra la secuencia de los mensajes durante un ataque SYN Flood.

Los ataques TCP SYN flood han ido desarrollándose y ganando en efectividad, la principal diferencia entre los ataques modernos TCP SYN flood y los clásicos es el número de paquetes por segundo enviados por el atacante. El ataque TCP SYN flood moderno genera paquetes SYN medidos en millones de paquetes por segundo (PPS). Este

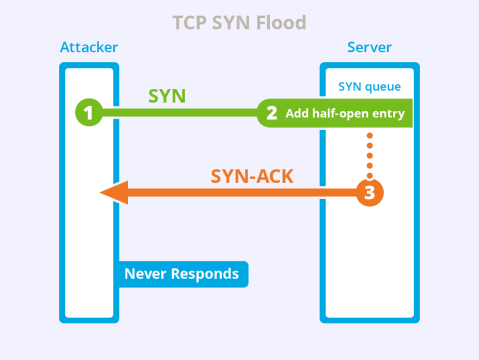

Figura 7. Ataque SYN Flood [6]

gran volumen de paquetes SYN crea dos efectos. El primero es que los balanceadores de carga, los cortafuegos y los otros dispositivos que gestionan el estado de conexión, utilizarán una CPU excesiva y pueden desbordar las tablas de estado de su red. El segundo, que constituye el comportamiento más dañino, ocurre cuando las redes no están adecuadamente dimensionadas para recibir un gran volumen de paquetes SYN pequeños.

IV. Visión general Ataques de Denegación de Servicios en la Nube

Los ataques de denegación de servicios siempre han sido un peligro contra la disponibilidad de los servicios de una empresa; con el nuevo paradigma de los servicios en la Nube, en la mayoría de los casos, este tipo de ataques ve una puerta abierta que les permite aumentar en efectividad. Las ventajas proporcionadas por la computación en la Nube están disponibles tanto para las víctimas como para los atacantes. Es decir, en un entorno de Nube, un atacante puede arrendar recursos de la Nube para lanzar ataques DoS en las máquinas virtuales de otros clientes [5]. La virtualización está en el núcleo de la computación en la Nube, esto implica que los recursos físicos de un proveedor de servicios de Nube son repartidos dinámicamente a varios clientes, por lo que un ataque de denegación de servicios que vaya contra la infraestructura de virtualización que sustenta los servicios en la Nube puede dejar sin servicios a varios clientes, lo que representa una pérdida multiplicada por la cantidad de empresa que han sido afectadas. La computación en la Nube es una agrupación de varias tecnologías como la virtualización, el acceso de banda ancha, la gestión autónoma y la orientación a servicios, por lo que los controles de seguridad aplicados en cada una de estas tecnologías deben converger para proteger a los usuarios en la Nube [10]. Con el desarrollo de los servicios en la Nube cada año son más las empresas que trasladan sus servicios hacia esta, por lo que los atacantes han girado sus esfuerzos a vulnerar los servicios en la Nube. Los ataques de DoS han sido un tema siempre de gran interés en la comunidad dedicada a la cyber-seguridad, pero en los últimos años ha ganado gran importancia las investigaciones dirigidas a salvaguardar los servicios de una empresa alojados en la Nube.

La Figura 8 detalla los principales mecanismos y el posible impacto de los ataques en servicios e infraestructura en la Nube, comparándolo con los ataques de DDoS tradicionales. Entre las principales diferencias mostradas, está que los ataques a la Nube presentan pérdidas económicas que pueden afectar tanto a los clientes como a los proveedores de servicios y presentar daños colaterales a clientes alojados en los mismos recursos físicos que han sido atacados. Las principales diferencias entres los ataques de denegación de servicio en la Nube y los tradicionales no radican en el ataque en sí, sino en las consecuencias y los mecanismos de mitigación empleados. La escala de los ataques DDoS en la Nube es principalmente dada por la relación volumen/masividad, con anchos de banda de ataque mayor a 100 Gbps. La Figura 9 muestra un resumen de las principales contribuciones relacionadas con la prevención, detección, mitigación y recuperación de ataques DDoS en la Nube [9].

Basados en los recientes ataques DDoS en los servicios en la Nube, [9] brinda un grupo de elementos que deben ser tomados en cuenta por los proveedores de servicios de la Nube y las empresas que poseen Nubes privadas que soportan sus servicios:

Flujo de tráfico: Está bien establecido que la detección basada únicamente en el análisis de tráfico no es suficiente ni infalible. Los ataques modernos evolucionan variando sus características para que no sean detectados por los filtros de tráfico.

Costos de administración: los ataques DDoS están comprometiendo las finanzas de los propietarios de los servicios brindados a las víctimas. Al diseñar soluciones de mitigación, el factor de costo es importante al administrar los aspectos de sostenibilidad.

Disponibilidad de servicios: mientras se mitigan los ataques DDoS, debe existir un mecanismo para ejecutar servicios para usuarios benignos con un tiempo de inactividad mínimo o nulo.

Colaboración: los ataques de gran volumen y masivos, no son completamente detectables por la víctima. Hay muchos otros puntos de información / alerta en la Nube e Internet que pueden ayudar a obtener información importante sobre la probabilidad de ataques. Estas alertas y las acciones posteriores basadas en estas, pueden resultar prometedoras para combatir ataques.

Minimización de daños: la mitigación de DDoS también debe permitir minimizar los daños colaterales. Esto se puede asegurar aislando y monitoreando los esfuerzos en otros componentes como hipervisores y redes.

Administración de recursos: los ataques DDoS en la Nube han sido evaluados como un problema de administración de recursos en el servicio de la víctima. La idea principal detrás de estas soluciones es proporcionar una garantía de recursos libre de conflictos que puedan ayudar en la mitigación de un ataque cuando este está ocurriendo. Estos métodos basados en la gestión de recursos son útiles y rentables.

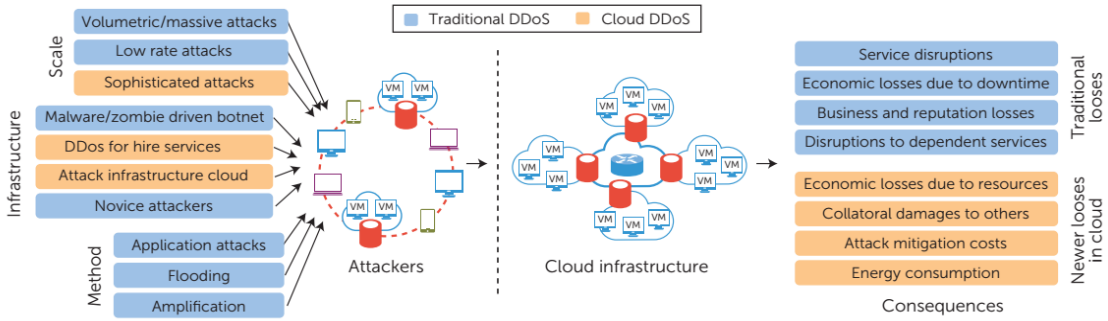

Figura 8. Ataques de Denegación de Servicios y pérdidas en los servicios en la Nube [9]

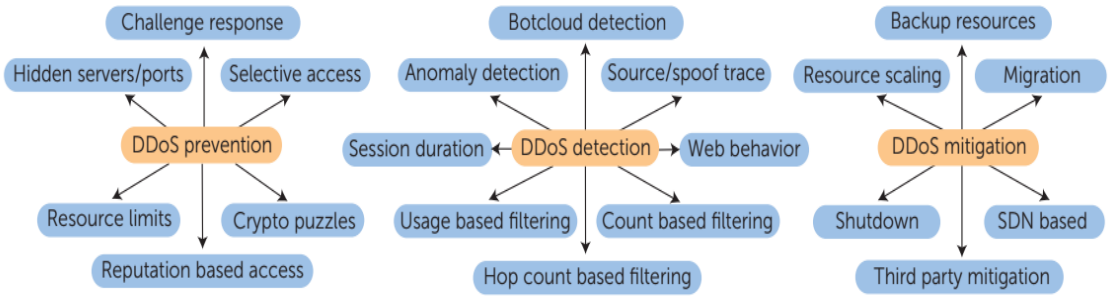

Figura 9. Varios métodos para combatir los ataques DDoS en cloud computing [9]

IV-A. Mecanismos de Seguridad propuestos para Detectar los Ataques de Denegación de Servicios en la Nube

Para detectar ataques DoS en una red, normalmente se utilizan firewall y sistemas de detección de intrusos (IDS). Los IDS se clasifican en IDS basados en firmas y basados en anomalías; los primeros tienen la limitación que si el ataque no está registrado en su base de datos son incapaces de detectarlo, por lo que en los entornos de servicios en la Nube se ha recomendado usar los IDS basados en detección de anomalías que utiliza métodos estadísticos o de aprendizaje automático para detectar nuevo ataques.

Para proteger el entorno de la Nube se ha propuesto el Sistema de prevención de intrusiones en la red (*Network Intrusion Prevention System*, NIPS) basado en perfil. El NIPS, que es administrado por un administrador de la Nube, examina los paquetes que se originan y están destinados a las interfaces virtuales de las máquinas virtuales(VM) dentro de la Nube y lo compara contra un perfil de la máquina virtual ya creado. Un perfil de VM inicial se crea al monitorear todo el tráfico que pasa hacia y desde la VM. Este tráfico se compara con una base de datos de firmas de ataque y utilizando los ataques y los comportamientos normales del tráfico se crea un perfil, el cual es actualizado posteriormente por el administrador del NIPS.

En [6] se presenta una revisión exhaustiva de las técnicas de detección de intrusos para entornos de Nube. Destacan el uso de técnicas de minería de datos y de aprendizaje automático para un sistema de detección de intrusiones basado en anomalías, como redes neuronales artificiales, lógica difusa, reglas asociativas, máquina de vectores de soporte, algoritmos genéticos e híbridos de estos. Debido a que el presente trabajo no hace uso de IDS basados en anomalías, este tema no es profundizado. Se recomienda usar firewall e IDS en conjunto para la protección contra ataques de DoS. Los Firewall actuales poseen funcionalidad de IPS e IDS [7]. Como por ejemplo, el Cisco ASA es un dispositivo de seguridad que combina capacidades de firewall, antivirus, prevención de intrusiones y redes privadas virtuales (VPN), lo que proporciona una defensa proactiva contra amenazas que detiene los ataques antes de que se propaguen a través de la red [8].

V. Arquitectura Implementada

El objetivo de este trabajo es detectar un ataque de Denegación de Servicios, específicamente un ataque TCP SYN flood en un ambiente simulado. En [5] se presenta la arquitectura de la Figura 10, como una posible configuración de seguridad que pudieran usar los proveedores de servicios de la Nube. Esta arquitectura es montada físicamente y son detectados varios tipos de ataques de Denegación de Servicios, pero debido a limitaciones de recursos reales, en el presente trabajo se hace una analogía de la configuración de seguridad presentada anteriormente y se implementa la arquitectura en un ambiente simulado y solamente se detecta el ataque TCP SYN flood. La arquitectura implementada se muestra en la Figura 11, donde se aprecia que cada uno de los servicios de infraestructura (IaaS) solicitados por un

cliente se protegen con un Firewall, el cual es configurado para detectar y proteger contra ataques TCP SYN flood. Las herramientas usadas para montar la arquitectura implementada se listan a continuación.

1) GNS3 2.1.11 (Cisco ASA 9.8, Router Cisco 7200)
2) Kali Linux 2018.1-i386 (hping3 y Metasploit Framework)
3) Wireshark 2.6.1
4) ASDM(Adaptive Security Device Manager) 7.8
5) PC (Corei7 RAM 8GB)

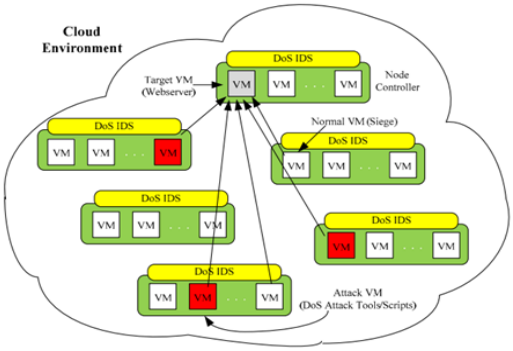

Figura 10. Arquitectura de Nube propuesta en [5]

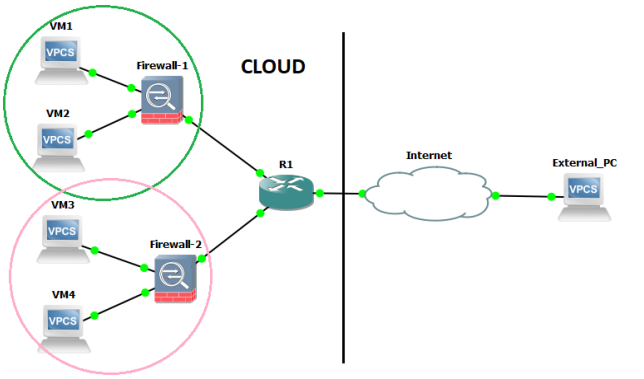

Figura 11. Arquitectura de Nube implementada

En la Figura 12 se muestra la arquitectura implementada en más detalle, el servidor Web con IP 10.1.0.2 fue la victima de los ataques de denegación de servicios ejecutados con las herramientas hping3 y el Módulo TCP SYN Flooder del Framework Metasploit que forman parte de Kali Linux usado. El hping3 es un ensamblador y analizador de paquetes TCP/IP orientado a la línea de comandos. La interfaz está inspirada en el comando ping de Unix, pero hping3 no solo es capaz de enviar solicitudes de eco ICMP sino que además admite los protocolos TCP, UDP y ICMP. La herramienta usada Metasploit, es una plataforma de pruebas de penetración que permite encontrar, explotar y validar vulnerabilidades. Además, proporciona la infraestructura, el contenido y las herramientas para realizar pruebas de penetración y auditorías de seguridad integrales. El Firewall de Cisco ASA detecta lo que se conoce como conexiones embrionarias que no es más que una solicitud de conexión que no ha completado el protocolo de enlace necesario entre el origen y el destino (*three-way handshake of TCP*). El Firewall Cisco ASA permite limitar el número de conexiones embrionarias lo cual previene los ataques TCP SYN flood. Cuando es sobrepasado el umbral de conexiones embrionarias, el Cisco ASA actúa como un proxy para el servidor que está posiblemente bajo un intento de ataque, y genera una respuesta SYN-ACK a la solicitud SYN del cliente o posible atacante. Cuando el Cisco ASA recibe un ACK del cliente, puede autenticar que el cliente es real y no es un atacante y permitir la conexión al servidor. El componente del Cisco ASA que se comporta como proxy se conoce como TCP Intercept. La configuración del Cisco ASA evita que un servidor reserve recursos innecesariamente en espera de un mensaje ACK que nunca llegará, y permite que solamente accedan al servidor las conexiones que completen el *three-way handshake*. En las Figuras 13, 14, 15 se muestran las configuraciones más importantes realizadas en el Firewall

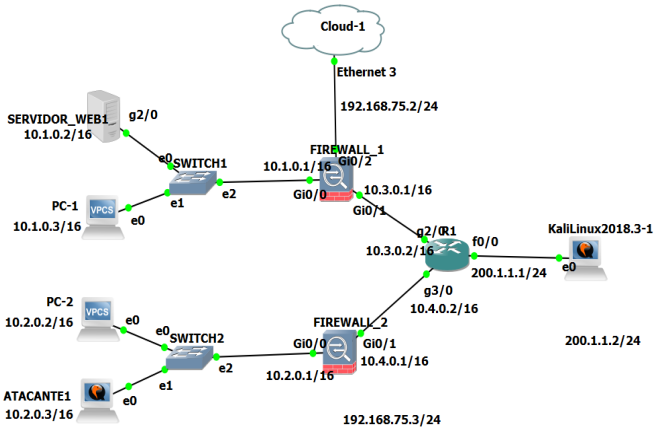

Figura 12. Arquitectura de Nube implementada en detalles

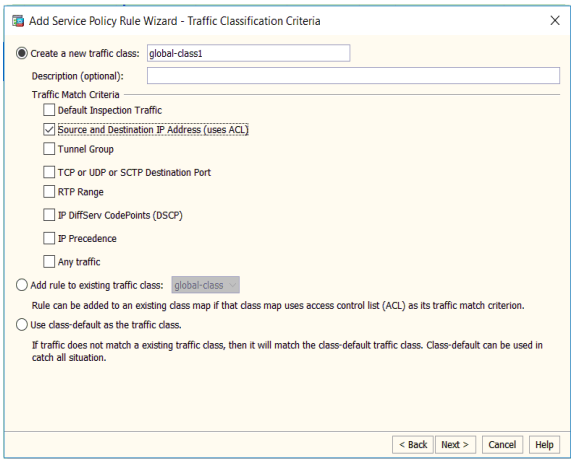

Figura 13. Configuración Firewall Cisco ASA

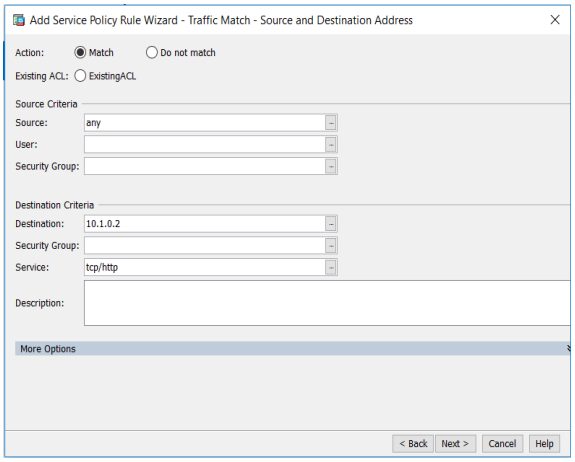

Figura 14. Configuración Firewall Cisco ASA

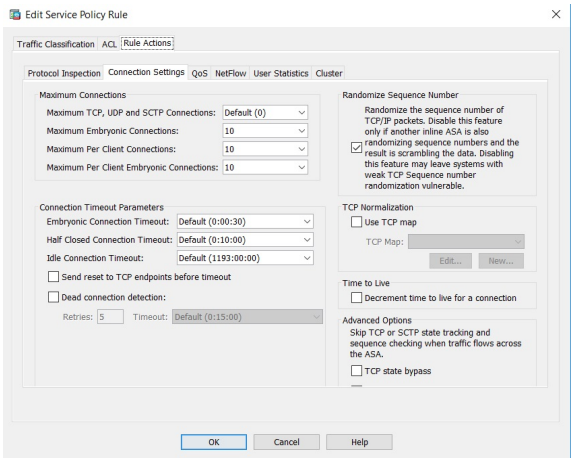

Figura 15. Configuración Firewall Cisco ASA

Las pruebas realizadas siguiendo el objetivo del trabajo se dividen en los siguientes puntos:

1) Ataque al servidor Web con IP 10.2.0.1 usando hping3 desde una Atacante Externo al ambiente de la Nube con IP 200.1.1.2 sin y con protección del Firewall Cisco ASA.
2) Ataque al servidor Web con IP 10.2.0.1 usando módulo TCP SYN Flooder del Framework Metasploit desde un Atacante Interno al ambiente de la Nube con IP 10.2.0.3 sin y con protección del Firewall Cisco ASA.

V-A. Ataque TCP SYN Flood usando hping3

En la Figura 16 se muestra la configuración del ataque ejecutado por el Atacante Externo usando hping3. Entre los parámetros configurados se encuentra la IP que va a ser atacada y el puerto que se va a usar para dicho ataque.

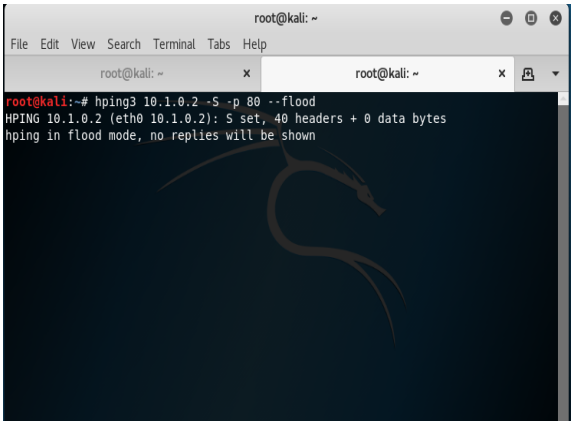

Figura 16. Ataque usando la herramienta hping3

En la Figura 17 se puede ver la inundación SYN desde la PC atacante hacia el servidor Web víctima. Pasados seis minutos aproximadamente del comienzo del ataque, la conexión con el servidor es perdida, lo cual se demuestra en la Figura 18, se estima que en entornos reales, donde los servidores en la Nube tienen mayor cantidad de recursos de cómputo contratados, que una maquina virtual creada sobre los recursos limitados de una PC, el tiempo en el que se pierde la conexión con el servidor víctima debido al ataque sea mayor.

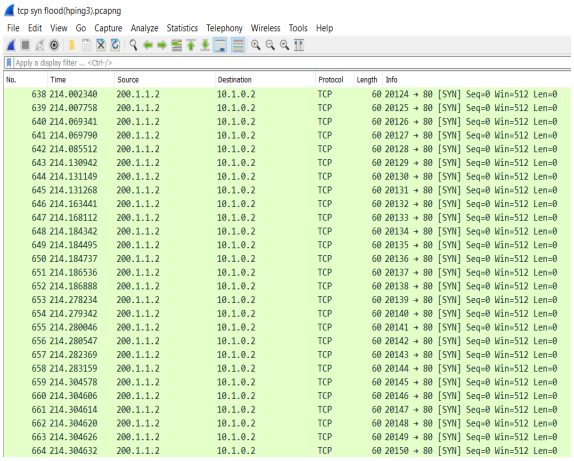

Figura 17. Ataque SYN Flood sin protección del Firewall Cisco ASA

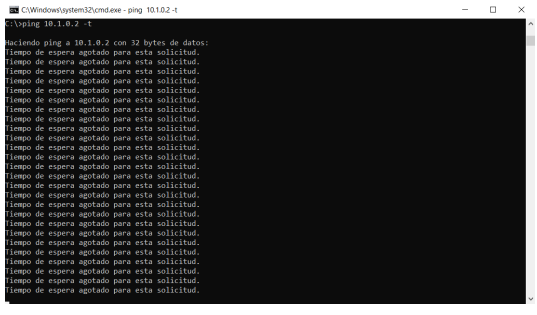

Figura 18. Conexión fallida con el servidor víctima del ataque

Una vez activadas las políticas de seguridad configuradas en el Firewall Cisco ASA, se procede a realizar un nuevo ataque TCP SYN Flood con la herramienta hping3. Como se aprecia en la Figura 19, con las políticas activadas, cuando el ataque sobrepasa la cantidad de conexiones embrionarias configuradas en el Firewall, este comienza a filtrar esas conexiones y evita que el ataque logre su objetivo. En la Figura se muestra que la comunicación con el servidor Web nunca se pierde debido a que el Firewall evita que sea víctima del ataque TCP SYN Flood y no pueda responder de forma efectiva a las solicitudes de los usuarios legítimos.

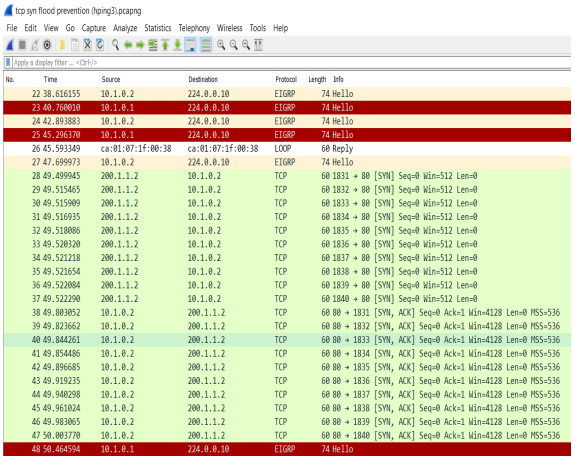

Figura 19. Ataque SYN Flood con protección del Firewall Cisco ASA

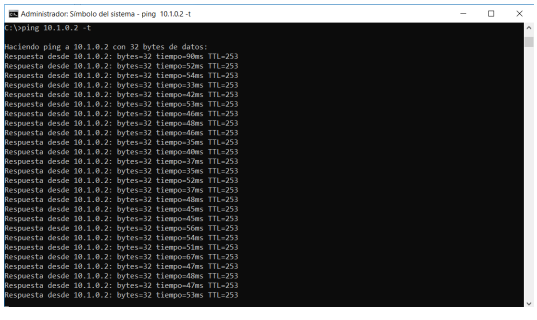

Figura 20. Conexión satisfactoria con el servidor víctima del ataque debido a la protección del Firewall

El Firewall Cisco ASA es capaz de detectar y bloquear el ataque TCP SYN Flood y además envía notificaciones de esta detección que pueden ser revisadas por el administrador de la Nube. En la Figura se muestran los reportes (*log*) del Firewall, donde se indica que el límite de conexiones embrionarias se ha sobrepasado, por lo que la IP fuente es considerada un atacante y es bloqueada.

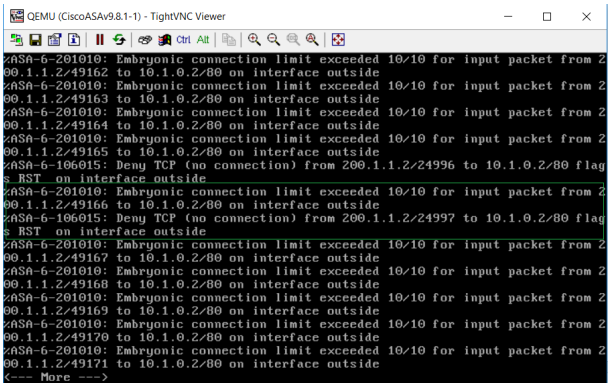

Figura 21. Reportes del Firewall Cisco ASA durante el ataque TCP SYN Flood

V-B. Ataque TCP SYN Flood usando módulo TCP SYN Flooder del Framework Metasploit

En la Figura 16 se muestra la configuración del ataque ejecutado por el Atacante Interno usando el módulo TCP SYN Flooder del Framework Metasploit. Entre los parámetros configurados se encuentra la IP que va a ser atacada y el puerto que se va a usar para dicho ataque.

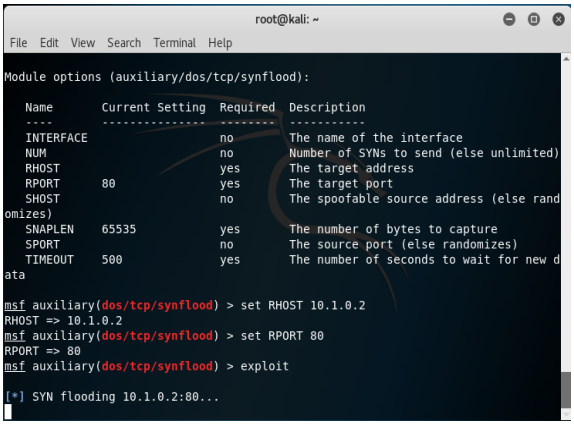

Figura 22. Ataque usando el módulo TCP SYN Flooder del Framework Metasploit

En la Figura 23 se muestra la inundación SYN desde la PC atacante hacia el servidor Web víctima. Como se aprecia la IP del Atacante Interno es enmascarada, lo cual hace el ataque TCP SYN Flood usando el módulo del Framework Metasploit más peligroso, debido a que no se conoce de donde se está perpetrando el ataque.

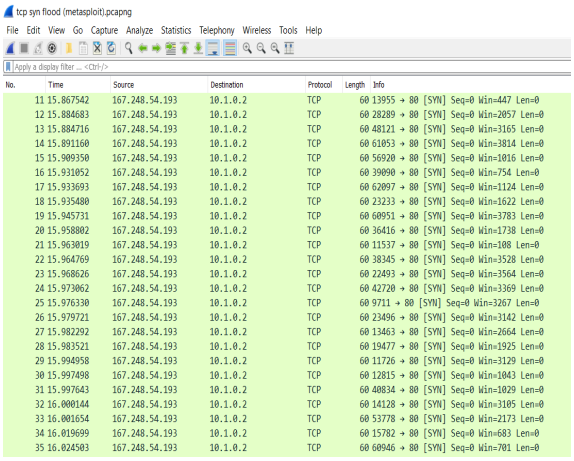

Figura 23. Ataque TCP SYN Flood sin protección del Firewall Cisco ASA

Una vez activadas las políticas de seguridad configuradas en el Firewall Cisco ASA, se procede a realizar un nuevo ataque TCP SYN Flood con la herramienta TCP SYN Flooder. Como se aprecia en la Figura 24, con las políticas activadas, cuando el ataque sobrepasa la cantidad de conexiones embrionarias configuradas en el Firewall, este comienza a filtrar esas conexiones y evita que el ataque logre su objetivo.

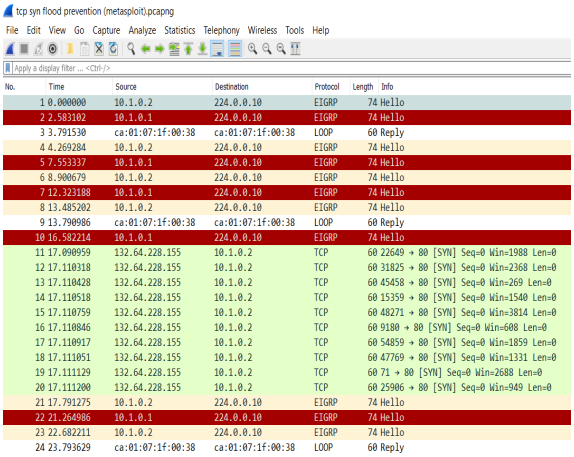

Figura 24. Ataque TCP SYN Flood con protección del Firewall Cisco ASA

VI. Conclusiones

Los ataques DoS son fáciles de comenzar usando scripts automatizados o herramientas como hping3, Net-tools, Metasploit. Los síntomas y efectos de un ataque DDoS, pueden ser simulados, permitiendo reconocer estos y actuar lo más rápido posible ante ataques reales. Los mecanismos de seguridad configurados son métodos eficaces para prevenir un posible ataque TCP SYN Flood y, por lo tanto, evitan el consumo no deseado de recursos del sistema y que el servidor sea inaccesible para los hosts legítimos durante un ataque. Las herramientas usadas para la detección de ataques DoS en la redes físicas de una empresa pueden ser usadas para la protección de los servicios contratados en la Nube. La principal diferencia entre los ataques de DoS tradicionales con los ejecutados contra la Nube no radica en el ataque en sí, sino en las pérdidas económicas tanto para el proveedor como para los clientes y los daños colaterales a terceros, producto a que los clientes se encuentran alojados en la misma infraestructura física.

Referencias

[1] Cisco Systems Inc., "Cisco Global Cloud Index: Forecast and Methodology, 2013–2018", Cisco Systems Inc. Americas Headquarters,San Jose, CA, USA. 2014.

[2] Cisco Systems Inc., "Cisco 2014 Annual Security Report", Cisco Systems Inc. Americas Headquarters, San Jose, CA, USA. 2014

[3] CISCO, *CCNA Routing and Switching ICND2 200-105 Official Cert Guide*, 2016 Published by Cisco Press.

[4] Q. Zhang, L. Cheng, R. Boutaba *Cloud computing: state-of-the-art and research challenges*, J Internet Serv Appl (2010) 1: 7–18 DOI 10.1007/s13174-010-0007-6.

[5] R. Kumar, S. Pranit, A. Sharma *Detecting Denial of Service Attacks in the Cloud*, 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing.

[6] *DDoS Attacks, Incapsula* , Available:https://www.incapsula.com/ddos/ddos-attacks.html

[7] *The DDoS myth about the firewall and the IPS* Available:https://www.corero.com/blog/609-the-ddos-myth-about-the-firewall-and-the-ips.html

[8] *What is the Cisco ASA?* , Available:https://www.cxtec.com/resources/blog/what-is-cisco-asa-security-appliance/,2018

[9] G. Somani, M. Singh Gaur,D. Sanghi, M. Conti, M. Rajarajan, R. Buyya, *Combating DDoS Attacks in the Cloud: Requirements, Trends,and Future Directions*, 2017 IEEE Cloud Computing, published by the IEEE Computer Society.

[10] P. Mell *What's Special about Cloud Security?*,US National Institute of Standards and Technology, 2012.

[11] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, *A survey of intrusion detection techniques in Cloud*, Journal of Network and Computer Applications, vol. 42, pp. 42-57, 2012.

[12] K. Hajdarevic, A. Kozic, I.Avdagic, Z. Masetic, N. Dogru *Training Network Managers in Ethical Hacking Techniques to Manage Resource Starvation Attacks using GNS3 Simulator*, 2017 IEEE.