Proveer de seguridad a redes empresariales de ataques.

Pedro Arce 202056597-k, Benjamin Espinoza 202030547-1, Pablo Etcheberry 201904517-2, Vicente Olmos 202030529-3

I. Introduccion

Este proyecto busca brindar seguridad a las redes empresariales, específicamente contra ataques de denegación de servicio (DDoS). Estos ataques se encuentran entre las amenazas más persistentes a nivel mundial y continúan evolucionando en complejidad y escala, lo que hace cada vez más difícil mitigarlos de manera efectiva. Estadísticas recientes muestran un aumento significativo en la frecuencia y gravedad de estos ataques; Según Cloudflare, hubo un aumento interanual del 117% y sus sistemas mitigaron automáticamente más de 5,2 millones de ataques HTTP DDoS, por un total de más de 26 mil millones de solicitudes en el último año. Aunque esto representó una disminución del 20% en comparación con los niveles de 2022, los ataques DDoS a la capa de red aumentaron un 85%, totalizando 8,7 millones de incidentes en 2023.
El impacto de estos ataques va más allá de la mera interrupción del servicio; afecta la confianza del cliente, la reputación de la empresa y puede tener graves consecuencias financieras. Por lo tanto, es crucial proteger las redes empresariales no sólo para la continuidad del negocio, sino también para salvaguardar la información confidencial y los activos críticos. Si bien servicios como los que ofrece Cloudflare son efectivos, pueden resultar prohibitivamente costosos a largo plazo, especialmente para las pequeñas y medianas empresas.
Por lo tanto, este proyecto tiene como objetivo desarrollar una solución de simulación que permita a las empresas probar y evaluar varias estrategias de mitigación de ataques DDoS de manera rentable. Al simular ataques en un entorno controlado, las empresas pueden identificar vulnerabilidades dentro de sus redes y mejorar sus capacidades de respuesta sin riesgo de interrumpir sus operaciones reales. Además, este enfoque promueve una mejor comprensión de los ataques DDoS y fortalece la preparación para incidentes futuros, contribuyendo así a una postura de seguridad más sólida y adaptable.

II. Descripción del problema a resolver

Una de las principales dificultades en la gestión de la seguridad de redes frente a ataques DDoS es la necesidad de soluciones de mitigación que no solo sean efectivas sino también accesibles, especialmente para pequeñas y medianas empresas que operan con presupuestos más ajustados. Las soluciones existentes, aunque robustas, a menudo implican costos elevados y pueden no ser prácticas para todas las empresas. Además, el ritmo acelerado del desarrollo tecnológico en técnicas de ataque requiere que las estrategias de defensa sean igualmente dinámicas y adaptativas, una característica que no siempre es posible con soluciones estáticas o genéricas.

El problema que este proyecto busca resolver es: Probar y optimizar estrategias de mitigación de ataques DDoS de manera costo-efectiva. Esto permite a las empresas ajustar sus defensas en un entorno simulado sin el riesgo de afectar sus operaciones en vivo, asegurando que las configuraciones de seguridad no solo sean robustas sino también flexibles y escalables según las necesidades cambiantes de la empresa.

Para abordar este problema de manera efectiva, se propone el desarrollo de una simulador que permita modelar ataques DDoS en un entorno controlado, analizar la respuesta de redes ante estos ataques y ajustar las configuraciones de seguridad. Esta herramienta no solo ayudará a prevenir interrupciones del servicio durante ataques sino que también facilitará una mejora continua en las prácticas de seguridad de la red, permitiendo a las organizaciones aprender de cada simulación y adaptarse a las nuevas amenazas de manera proactiva.

- Para las **pequeñas empresas**, la simulación asume un router por switch, enfocándose en soluciones simples y costeables que pueden implementarse rápidamente y sin necesidad de recursos adicionales significativos.

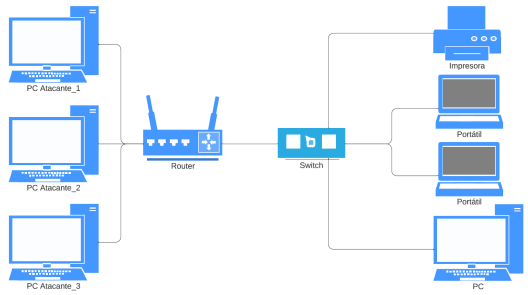

Fig. 1. Red para pequeñas empresas

- Para las **medianas empresas**, se considera una infraestructura más compleja con switches gestionados a través de VLANs, lo que requiere estrategias de seguridad más sofisticadas.

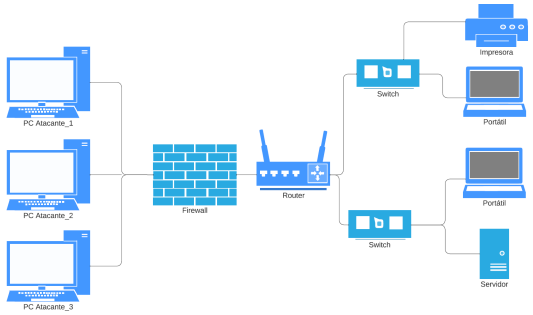

Fig. 2. Red para medianas empresas

Adicionalmente si se indica la presencia de un firewall el diagrama de red seria el siguiente:

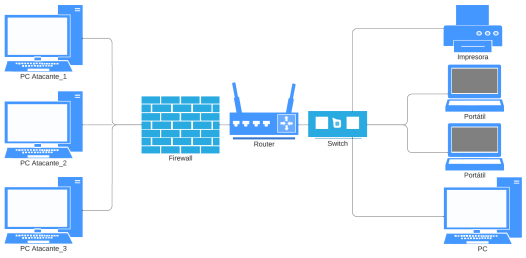

Fig. 3. Red con firewall

III. Objetivo del proyecto

Evaluar y optimizar la resistencia de redes de PyMEs ante ataques DDoS, minimizando la interrupción de servicios, aplicando medidas de seguridad especifica para esa red y garantizando la menor interrupción de servicio.

IV. Método para resolver el problema

Inicialmente, el proyecto se enfocó en manejar el funcionamiento interno de la red, incluyendo el enrutamiento de paquetes y la segmentación del tráfico mediante VLANs. Sin embargo, después se enfocó más hacia la simulación de ataques DDoS y la mitigación de estos ataques, ya que esto proporciona una evaluación más directa y práctica de la resistencia de la red y la efectividad de las medidas de seguridad implementadas.

Para resolver el problema, se diseñó y desarrolló una simulación de red que incluye varios dispositivos, como routers, switches, computadoras y firewalls. Se implementó una clase de ataque DDoS que genera múltiples solicitudes a la red, y el impacto de estas solicitudes se evalúa en función de varias métricas. La red y los ataques se implementaron en Python, utilizando ThreadPoolExecutor para manejar multiples atacantes. Los componentes utilizados son:

- **Router**: Este dispositivo se encarga del enrutamiento de paquetes entre diferentes subredes. Mantiene una tabla de enrutamiento para determinar la mejor ruta para enviar los paquetes.
- **Switch**: Gestiona el tráfico de red dentro de una subred. Permite la configuración de VLANs para segmentar el tráfico y mejorar la seguridad de la red.
- **Computer**: Tiene dirección IP y MAC. Puede contiene datos con información sensible.
- **Firewall**: Implementa reglas de filtrado de paquetes para bloquear tráfico no autorizado. Monitorea la capacidad y recupera su estado automáticamente después de ser sobrepasado.
- **Network**: Esta clase se encarga de gestionar los dispositivos de red, la topología y de procesar las peticiones. Permite la adición de switches y computadoras, la configuración del router y el firewall, y la visualización del estado de la red.

A. Medidas de Seguridad Implementadas

Se implementaron varias medidas de seguridad para mitigar los ataques DDoS y mejorar la resistencia de la red. Estas medidas son:

- **Bloqueo por IP**: Se bloquean las IPs que envían un número excesivo de solicitudes. Si una IP supera un umbral de 50 solicitudes, se agrega a una lista de IPs bloqueadas.
- **Bloqueo por Segmento**: Se bloquean segmentos de red completos si se detecta un número excesivo de solicitudes provenientes de ese segmento. Si un segmento supera un umbral de 80 solicitudes, se bloquea todo el segmento.
- **Bloqueo por Capacidad**: Se monitoriza la capacidad del firewall y se bloquean nuevas solicitudes si el uso de la capacidad supera un umbral del 60%. Esto evita que el firewall se sobrecargue y deje de funcionar.
- **Recuperación Automática del Firewall**: Después de ser sobrepasado, el firewall entra en un estado de recuperación durante un período específico (10 segundos) antes de reactivarse automáticamente.

B. Proceso de Simulación

- **Inicialización de la Red**: Se configuran los dispositivos de red y se establece la topología.
- **Ejecución del Ataque DDoS**: Se lanzan ataques DDoS en múltiples rondas, aumentando gradualmente la cantidad de atacantes y solicitudes por ronda.
- **Procesamiento de Solicitudes**: La clase Network y el Firewall se encargan de procesar las solicitudes, iterando por cada PC en la red para determinar cómo manejar cada solicitud. El Firewall implementa reglas de filtrado y maneja la capacidad, bloqueando solicitudes no autorizadas y recuperando su estado automáticamente.
- **Recopilación de Datos**: Se recopilan datos de cada ronda de ataque para evaluar el rendimiento de la red.
- **Análisis y Visualización**: Se analizan los datos recopilados y se generan gráficos comparativos para visualizar el impacto de los ataques y la efectividad del firewall.

C. Métricas y gráficos generados:

Para simular el ataque se utiliza la clase DDoSAttack, la cual genera múltiples solicitudes a la red para simular un ataque DDoS. Se monitorean las solicitudes permitidas,

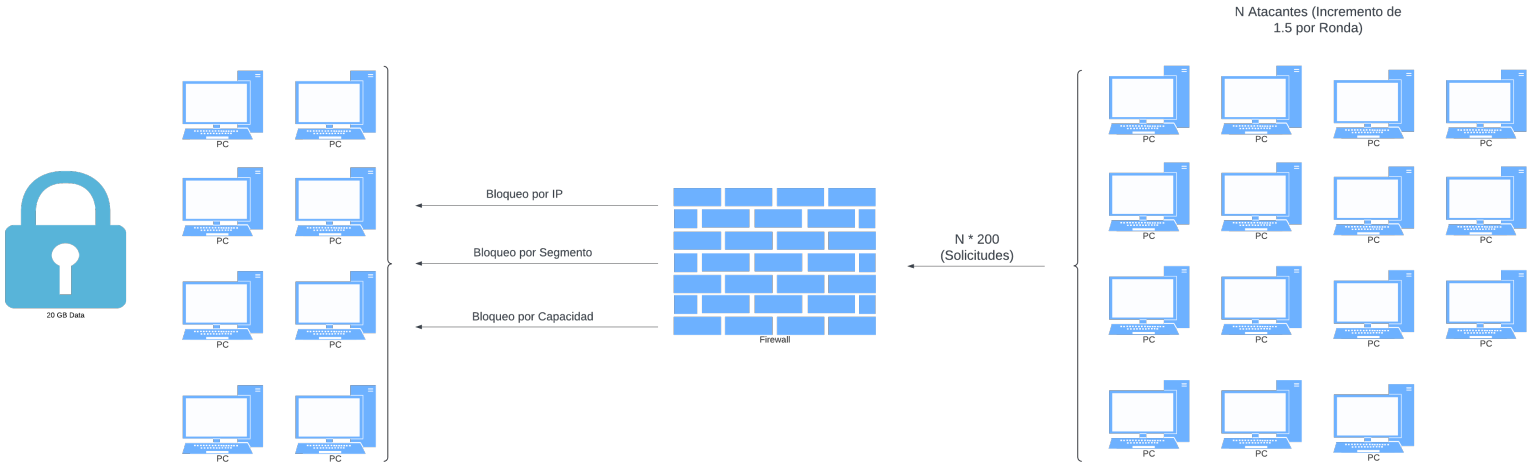

Fig. 4. Diagrama simulador

bloqueadas y se registran eventos durante el ataque. Las métricas a evaluar son:

- **Solicitudes Totales**: Número total de solicitudes recibidas durante cada simulación.
- **Solicitudes Exitosas**: Número de solicitudes que fueron procesadas exitosamente sin ser bloqueadas.
- **Solicitudes Bloqueadas**: Número de solicitudes que fueron bloqueadas por el firewall.
- **Bloqueadas por IP**: Solicitudes bloqueadas específicamente debido al bloqueo de direcciones IP individuales.
- **Bloqueadas por Capacidad**: Solicitudes bloqueadas por medio del bloqueo por umbral de capacidad del firewall.
- **Bloqueadas por Segmento**: Solicitudes bloqueadas debido al bloqueo de segmentos completos de la red.
- **Atacantes Exitosos**: Número de atacantes que lograron realizar solicitudes exitosas(pudieron extraer algun dato).
- **Atacantes Bloqueados**: Número de atacantes que fueron completamente bloqueados por el firewall.
- **Duración del Ataque (segundos)**: Tiempo total que duró cada ataque DDoS en las diferentes rondas de simulación.
- **Porcentaje de Extracción (%)**: Cantidad de datos extraídos durante los ataques, expresada como un porcentaje del total disponible.
- **Tiempo de Recuperación del Firewall (segundos)**: Tiempo total que el firewall pasó en estado de recuperación después de ser sobrepasado.

Estos gráficos permiten una evaluación detallada y comparativa de las métricas clave, proporcionando una comprensión clara de la resiliencia de la red y la efectividad de las medidas de seguridad implementadas.

Esta metodología permite una evaluación exhaustiva de la resiliencia de la red y proporciona información valiosa sobre cómo mejorar la seguridad y la capacidad de recuperación ante ataques DDoS.

V. Resultados obtenidos

La red se configuró para una compañía pequeña con 5 PCs (IP inicial ”192.168.10.1” y VLAN ID 10) y otra con 3 PCs (IP inicial ”192.168.20.1” y VLAN ID 20), los cuales tienen 20GB de información denominada sensible, las cuales los atacantes pueden extraer de 16 MB por conexión.

Configuraciones de firewall:

- **Sin Firewall**: Esta configuración no incluye ninguna medida de seguridad. Se utilizó como línea base para comparar el resultado de los ataques sin protección en la red.
- **Firewall con Bloqueo por IP sin ataque previo**: En esta configuración, se implementó un firewall que bloquea direcciones IP después de detectar un exceso de solicitudes. Esta medida se aplicó sin tener información de ataques previos.
- **Firewall con Bloqueo por IP con ataque previo**: Similar a la configuración anterior, pero en este caso el firewall ya tenía información sobre direcciones IP utilizadas en ataques anteriores, permitiendo bloquear de manera preventiva. Su umbral para bloquear las direcciones IP sera de 50 solicitudes.
- **Firewall con Bloqueo por Segmento sin ataque previo**: Esta configuración bloquea segmentos de red completos cuando se detecta un exceso de solicitudes, en este caso sera de 80 solicitudes, desde cualquier IP del segmento. No utiliza direcciones ip de ataques previos.
- **Firewall con Bloqueo por Segmento con ataque previo**: Se aplica el mismo bloqueo por segmento, pero en este caso, el firewall tiene información sobre direcciones utilizados en ataques previos, permitiendo bloquear el semento.
- **Firewall con Bloqueo por Capacidad**: Esta configuración activa el bloqueo cuando la capacidad del firewall se ve sobrepasada para esta simulación sera de 60%. No se utilizan datos de ataques previos para bloquear IPs o segmentos ya que simplemente bloquea por capacidad.

- **Firewall con Bloqueo por IP, Segmento y Capacidad con ataque previo**: Una configuración más robusta que combina el bloqueo por IP, segmento y capacidad utilizando datos de ataques previos para mejorar la respuesta ante nuevos ataques. Se pone a modo de prueba aunque el bloqueo por segmento tiene preferencia por sobre el resto de medidas de seguridad.

La simulación se realiza con 3 iteraciones por configuración de firewall, donde en hay 30,45 y 67 atacantes, donde cada uno tiene asignado 150 peticiones al servidor, los resultados obtenidos están dados por la tabla 5

Análisis de resultados En general, se observa que el tiempo de recuperación del firewall deja de existir a partir de la implementación del bloqueo por IP. Esto indica que el firewall se vuelve eficiente en mitigar los ataques DDoS una vez que empieza a usar el bloqueo por segmento.Se puede ver en el gráfico 14

La duración de los ataques 15 se mantiene aproximadamente en 50 segundos en todas las configuraciones, lo cual sugiere que la duración del ataque no es significativamente afectada por las distintas estrategias de bloqueo implementadas.

El método más efectivo resulta ser la combinación de todos los mecanismos de bloqueo (IP, segmento y capacidad). Esta estrategia ofrece la mayor protección al combinar diferentes enfoques de defensa, seguido por el bloqueo por segmento, luego el bloqueo por capacidad y finalmente el bloqueo por IP, siendo este último el menos efectivo de todos. Se puede apreciar las solicitudes bloqueadas en el grafico 10, por otro lado los atacantes bloqueados 8

Sorprendentemente, el bloqueo por segmento con ataque previo presenta resultados similares al bloqueo sin ataque previo. Porque aunque el firewall logra bloquear las IPs iniciales, es necesario alcanzar el umbral de solicitudes para bloquear las nuevas IPs que surgen durante el ataque, dejando que los nuevos atacantes generados puedan sacar información. En el gráfico 13 se ve que no hay diferencia en las solicitudes que bloquea.

La efectividad del bloqueo por capacidad es aproximadamente del 90%, mientras que el bloqueo por segmento logra99%. Por otro lado, el bloqueo por IP muestra una efectividad del 75% en escenarios con ataque previo y de 45% sin ataque previo. Estos resultados destacan la importancia de un enfoque diverso para la protección contra ataques DDoS. Se puede ver que en los mejores métodos prácticamente no hay solicitudes exitosas 6

- **Sin Firewall**: Como era de esperarse, no bloquea ninguna solicitud y el porcentaje de extracción aumenta considerablemente a medida que aumentan los atacantes.
- **Firewall con Bloqueo por IP sin ataque previo**: En cada iteración bloquea un mayor porcentaje de direcciones IP, logrando disminuir significativamente el porcentaje de extracción en comparación con la configuración sin firewall.
- **Firewall con Bloqueo por IP con ataque previo**: Aumenta el porcentaje de extracción debido a la mayor cantidad de atacantes que debe bloquear; sin embargo, incrementa su porcentaje de bloqueo a 46%, 88%, y 89% en las iteraciones.
- **Firewall con Bloqueo por Segmento sin ataque previo**: Logra bloquear el 98% de los atacantes, logrando una mitigación prácticamente total del ataque.
- **Firewall con Bloqueo por Segmento con ataque previo**: Similar a su contraparte sin ataque previo, logra un bloqueo del 99% y mantiene la misma extracción de disco de 0.8%.
- **Firewall con Bloqueo por Capacidad**: Aunque es menos efectivo que el bloqueo por segmento, presenta una mejora en la simplicidad de implementación y en hardware real puede ser más eficiente. Bloquea aproximadamente el 90% de las solicitudes.
- **Firewall con Bloqueo por IP, Segmento y Capacidad con ataque previo**: Es el más eficiente, logrando un bloqueo del 100% en su última iteración.

VI. Trabajo Futuro

Como trabajo futuro hay que verificar el uso ThreadPoolExecutor porque deben existen paquetes mas eficientes o puede existir otra forma simple de abordar el problema de múltiples usuarios atacando al mismo tiempo.Otros puntos que se podrían implementar como trabajo futuro son:

- **Uso de medidas de seguridad al mismo tiempo:** Poder implementar las medidas de bloqueo por IP, segmento y capacidad en un mismo firewall,para ver como mejoraria la seguridad de la red.
- **Implementación de Algoritmos de Machine Learning:** Los siguientes pasos seria implementar mecanismos de Reinforcement Learning, los cuales muchos sistemas de simulación enfocado a redes utilizan, por otro lado se podría investigar la efectividad de algoritmos de aprendizaje automático para la detección y mitigación de ataques DDoS. Algoritmos como redes neuronales, SVMs (Support Vector Machines) y clustering podrían ayudar a identificar patrones anómalos en el tráfico de la red en tiempo real.
- **Análisis de Impacto Económico:** Evaluar el rendimiento económico de los ataques DDoS y las medidas de mitigación podría proporcionar una visión más completa del costo-beneficio de implementar múltiples estrategias de seguridad, especialmente comparado con los servicios que ofrece Cloudfare.
- **Simulación de Ataques Distribuidos en Escala Mayor:** Aumentar la escala de las simulaciones, tanto en número de atacantes como en la complejidad de la red interna, lo cual permitiria obtener resultados más representativos de escenarios reales. Además, se podrían incluir variaciones en las forma del ataque.
- **Comparación de Diferentes Tecnologías de Firewall:** Ampliar el estudio para incluir diferentes tecnologías y marcas de Firewall, evaluando su efectividad frente a distintos ataques DDoS.
- **Evaluación de Otros Tipos de Ataques:** Además de los ataques DDoS, sería importante evaluar la resistencia de la red frente a otros tipos de ciberataques, como ataques de phishing, ransomware y ataques de fuerza bruta.
- **Optimización del Consumo de Recursos:** Implementar métodos para optimizar el uso de recursos del firewall y

Configuración	Ronda	Solicitudes Totales	Solicitudes Exitosas	Solicitudes Bloqueadas	Bloqueadas por IP	Bloqueadas por Capacidad	Bloqueadas por Segmento	Atacantes Exitosos	Atacantes Bloqueados	Duración del Ataque (segundos)	Porcentaje de Extracción (%)	Tiempo de Recuperación del Firewall (s)	Porcentaje de Bloqueo(%)
Sin Firewall	1	4500	4500	0	0	0	0	30	0	51.472384	45.0	0.0	0,00
Sin Firewall	2	6750	6750	0	0	0	0	45	0	52.200012	67.5	0.0	0,00
Sin Firewall	3	10016	10016	0	0	0	0	67	0	50.322909	100.0	0.0	0,00
Firewall con Bloqueo por IP sin ataque previo	1	4500	2436	2064	2064	0	0	30	0	49.870814	24.36	30	45,87
Firewall con Bloqueo por IP sin ataque previo	2	6750	2980	3770	3770	0	0	45	0	50.25677	30	80	55,85
Firewall con Bloqueo por IP sin ataque previo	3	10050	6503	3547	3547	0	0	67	0	51.774211	65.03	140	35,29
Firewall con Bloqueo por IP con ataque previo	1	4500	2422	2078	2078	0	0	30	0	50.719713	24.22	30	46,18
Firewall con Bloqueo por IP con ataque previo	2	6750	750	6000	6000	0	0	15	30	49.068807	7.5	80	88,89
Firewall con Bloqueo por IP con ataque previo	3	10050	1100	8950	8950	0	0	22	45	50.798549	11.0	130	89,05
Firewall con Bloqueo por Segmento sin ataque previo	1	4500	80	4420	0	0	4420	30	0	50.596158	0.8	0.0	98,22
Firewall con Bloqueo por Segmento sin ataque previo	2	6750	80	6670	0	0	6670	45	0	49.571836	0.8	0.0	98,81
Firewall con Bloqueo por Segmento sin ataque previo	3	10050	80	9970	0	0	9970	67	0	49.276214	0.8	0.0	99,20
Firewall con Bloqueo por Segmento con ataque previo	1	4500	80	4420	0	0	4420	30	0	48.954479	0.8	0.0	98,22
Firewall con Bloqueo por Segmento con ataque previo	2	6750	80	6670	0	0	6670	15	30	51.222052	0.8	0.0	98,81
Firewall con Bloqueo por Segmento con ataque previo	3	10050	80	9970	0	0	9970	22	45	49.370233	0.8	0.0	99,20
Firewall con Bloqueo por Capacidad	1	4500	601	3899	0	3899	0	30	0	48.988257	6.01	0.0	86,64
Firewall con Bloqueo por Capacidad	2	6750	601	6149	0	6149	0	45	0	50.175889	6.01	0.0	91,10
Firewall con Bloqueo por Capacidad	3	10050	601	9449	0	9449	0	67	0	50.258261	6.01	0.0	94,02
Firewall con Bloqueo por IP, Segmento y Capacidad con ataque previo	1	4500	80	4420	0	0	4420	30	0	49.367603	0.8	0.0	0.0
Firewall con Bloqueo por IP, Segmento y Capacidad con ataque previo	2	6750	80	6670	0	0	6670	45	0	48.907126	0.8	0.0	0.0
Firewall con Bloqueo por IP, Segmento y Capacidad con ataque previo	3	10050	0	10050	0	0	10050	0	67	48.949414	0.0	0.0	0.0

Fig. 5. Tabla de resultados

otros dispositivos de red durante un ataque, minimizando el impacto en el rendimiento general de la red.

- **Integración con Sistemas de Monitoreo en Tiempo Real:** Integrar la simulación con sistemas de monitoreo en tiempo real, actualizados sobre el estado de la red durante un ataque.

VII. Apreciación personal del trabajo realizado,utilidad del trabajo y dificultades

A. Apreciación Personal del Trabajo Realizado

Hemos tenido la oportunidad de poner en práctica conocimientos sobre redes, ciberseguridad y sobre todo de abstracción para poder simularlo todo, logrando un entorno de red simple sujeto a ataques DDoS. Además, la implementación de diferentes configuraciones de firewalls nos ha permitido comparar la efectividad de varias estrategias de defensa, proporcionando una visión clara de sus fortalezas y debilidades.

B. Utilidad del Trabajo

La utilidad de este trabajo radica en varios aspectos:

- **Evaluación de Estrategias de Mitigación**: La simulación permite evaluar de manera efectiva las distintas estrategias de defensa de ataques DDoS.
- **Mejora en la Seguridad de Redes**: Al comprender mejor cómo funcionan los diferentes mecanismos de defensa, se pueden implementar medidas más efectivas en redes reales, mejorando así su seguridad de las redes empresariales.
- **Base para proyecto mas ambiciosos**: Este trabajo puede servir como base para futuros simuladores, donde se podrían probar otras configuraciones de firewalls.

C. Dificultades Encontradas

Durante el desarrollo del proyecto, se encontraron varias dificultades:

- **Complejidad en la Simulación de Redes**: Crear una simulación realista de una red con múltiples dispositivos y su configuración resultó ser un desafió, es por eso que finalmente nos centramos en las estrategias de mitigación frente a los ataques DDoS.
- **Implementación de Múltiples Firewalls**: La implementación de diferentes configuraciones de firewalls y su integración en la simulación requirió un esfuerzo considerable para asegurar su correcto funcionamiento, especialmente el enfoque usando la librería threading en un comienzo la cual proporcionaba un rendimiento pobre comparado con la que se usa actualmente.

- **Interpretación de Resultados**: Analizar y comparar los resultados obtenidos de las distintas simulaciones fue complejo, ya que se debía asegurar la validez y consistencia de los datos, lo cual llevaba a iterar sobre el simulador constantemente.
- **Problemas Técnicos**: Hubo varios problemas técnicos relacionados con la sincronización de los ataques y el procesamiento concurrente de solicitudes, lo que requirió ajustes y depuraciones constantes del código.

REFERENCES

[1] Cloudflare, *DDoS Threat Report 2023 Q4*, Disponible en: https://blog.cloudflare.com/ddos-threat-report-2023-q4,
[2] PixelPrivacy, *DDoS Attack Statistics Report*, Disponible en: https://pixelprivacy.com/resources/ddos-attack-statistics-report/,
[3] BusinessWire, *DDoS Attacks in H1 2023 Up 200% from 2022, According to New Zayo Data*, Disponible en: https://www.businesswire.com/news/home/20230824438114/en/DDoS-Attacks-in-H1-2023-Up-200-from-2022-According-to-New-Zayo-Data,

APPENDIX A
ANEXO

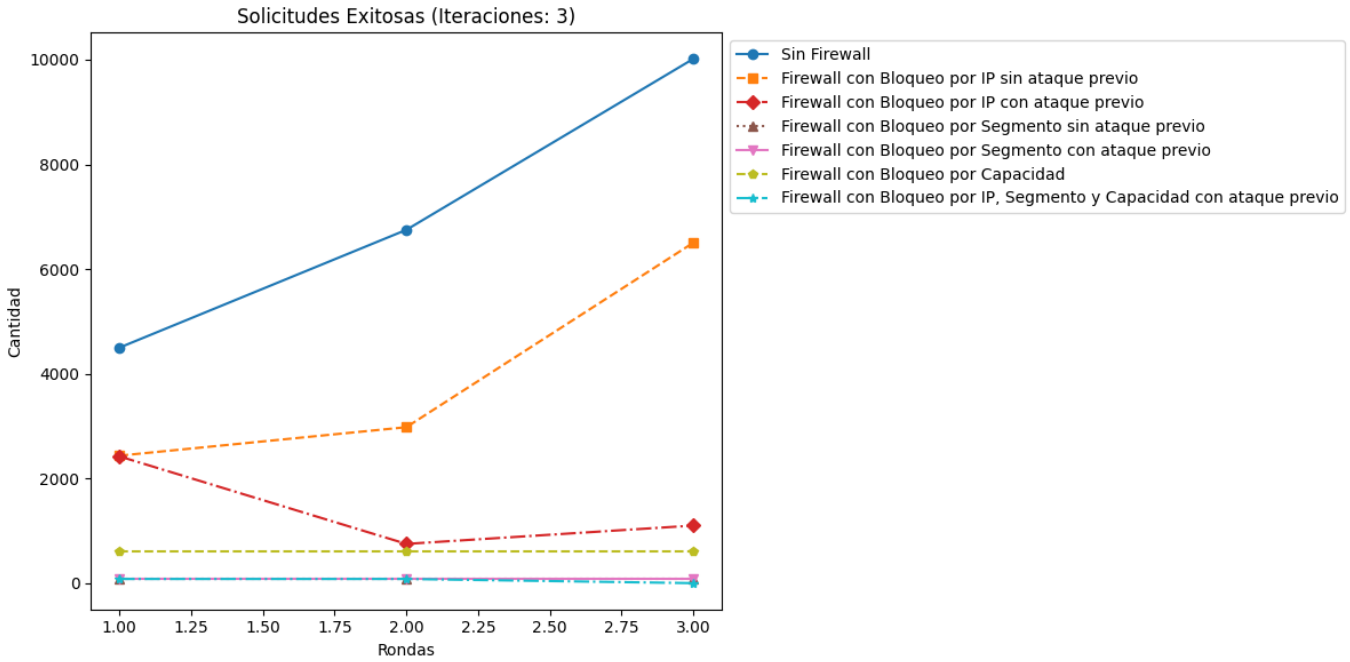

Fig. 6. Solicitudes Exitosas

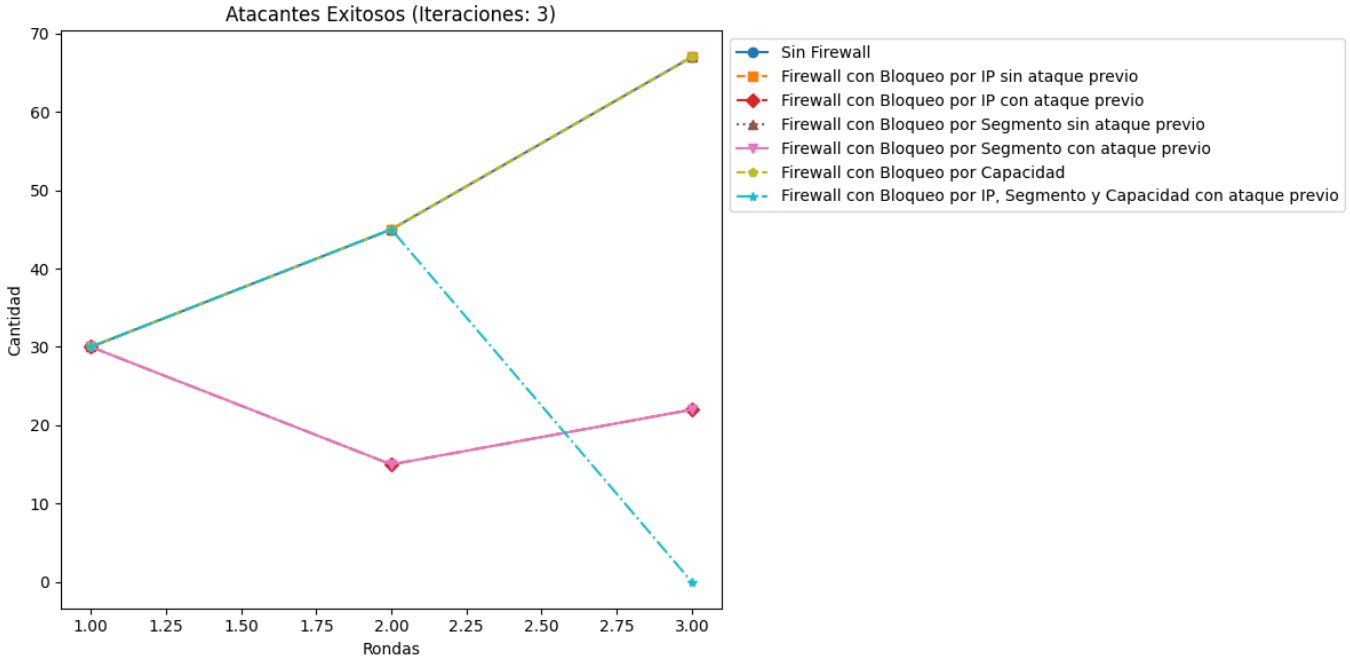

Fig. 7. Atacantes Exitosos

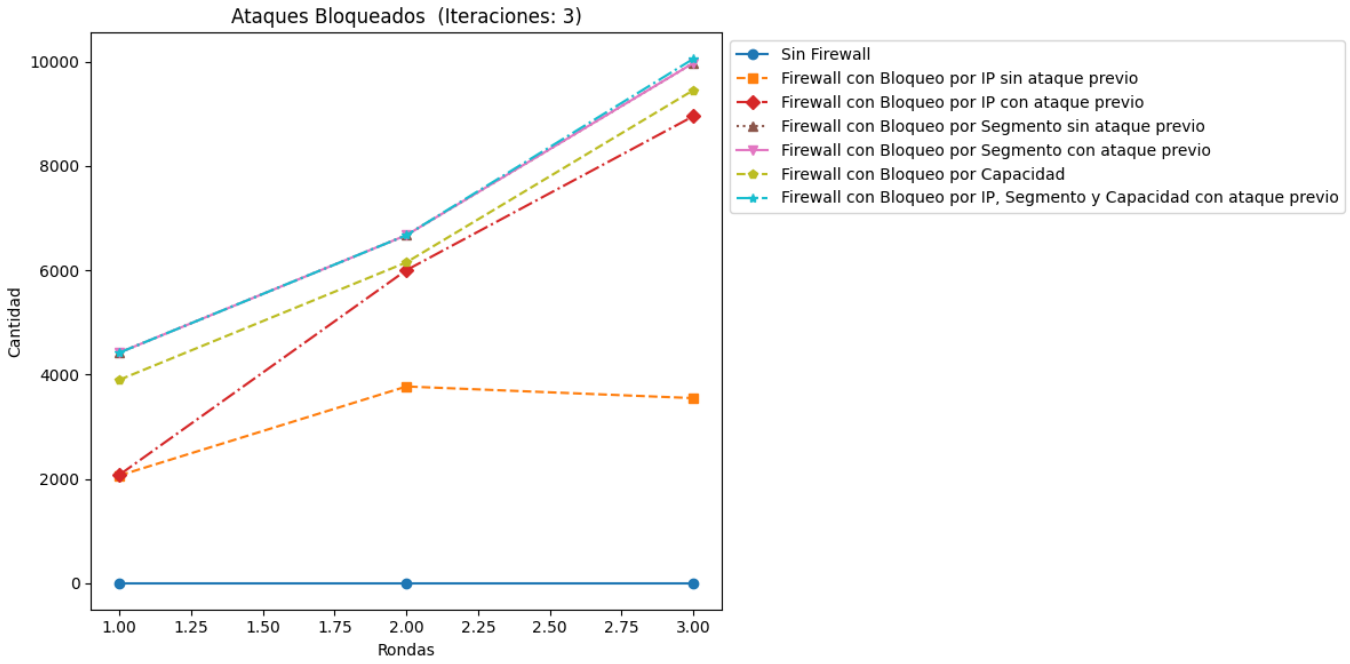

Fig. 8. Ataques Bloqueados

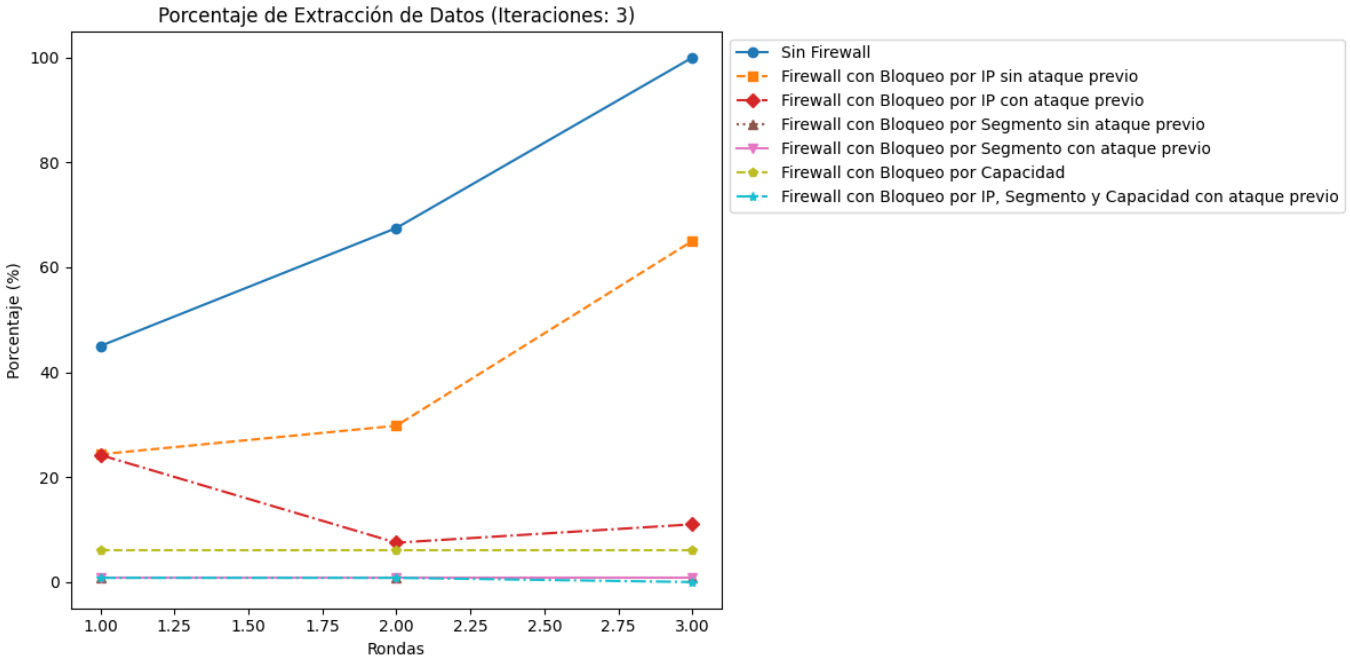

Fig. 9. Porcentaje de Extracción

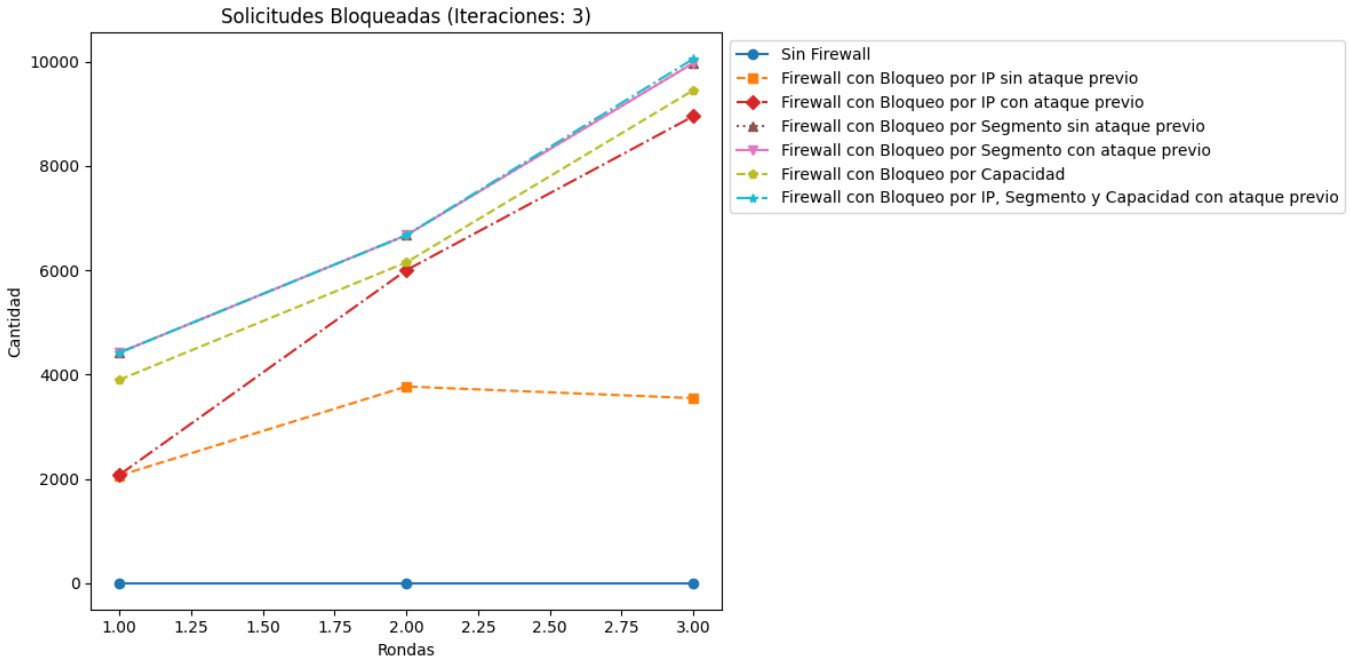

Fig. 10. Solicitudes Bloqueadas

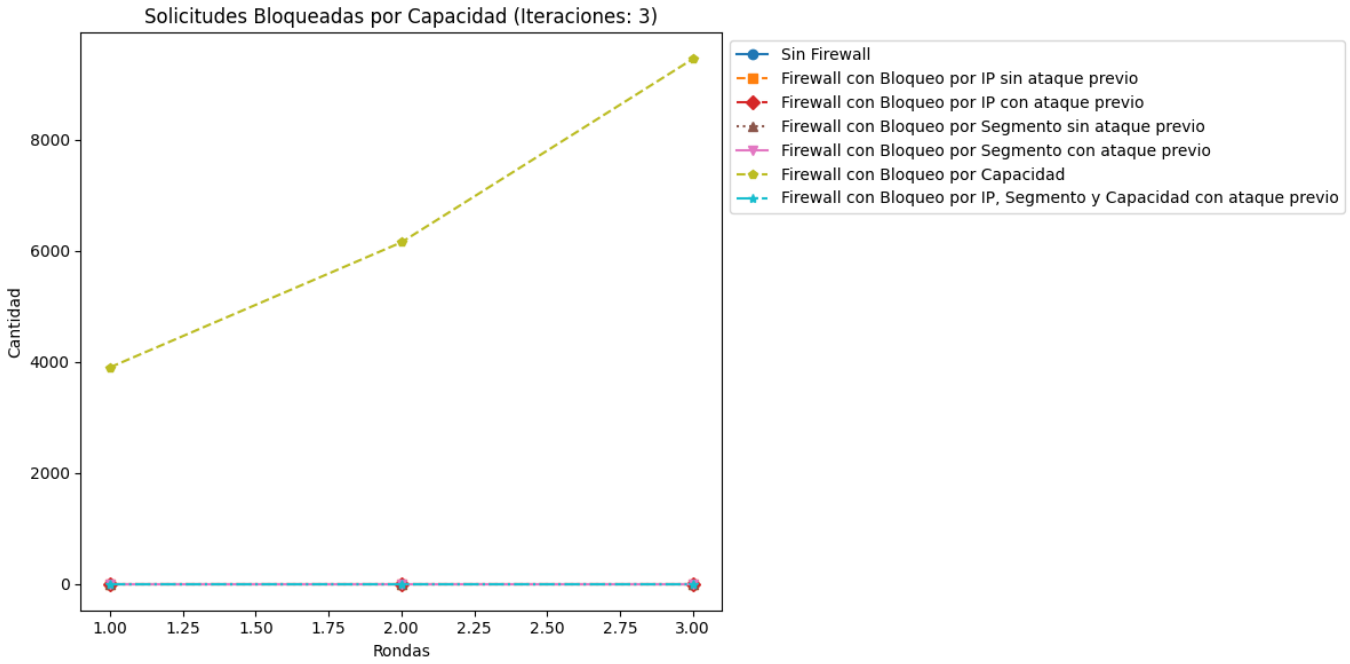

Fig. 11. Solicitudes Bloqueadas por Capacidad

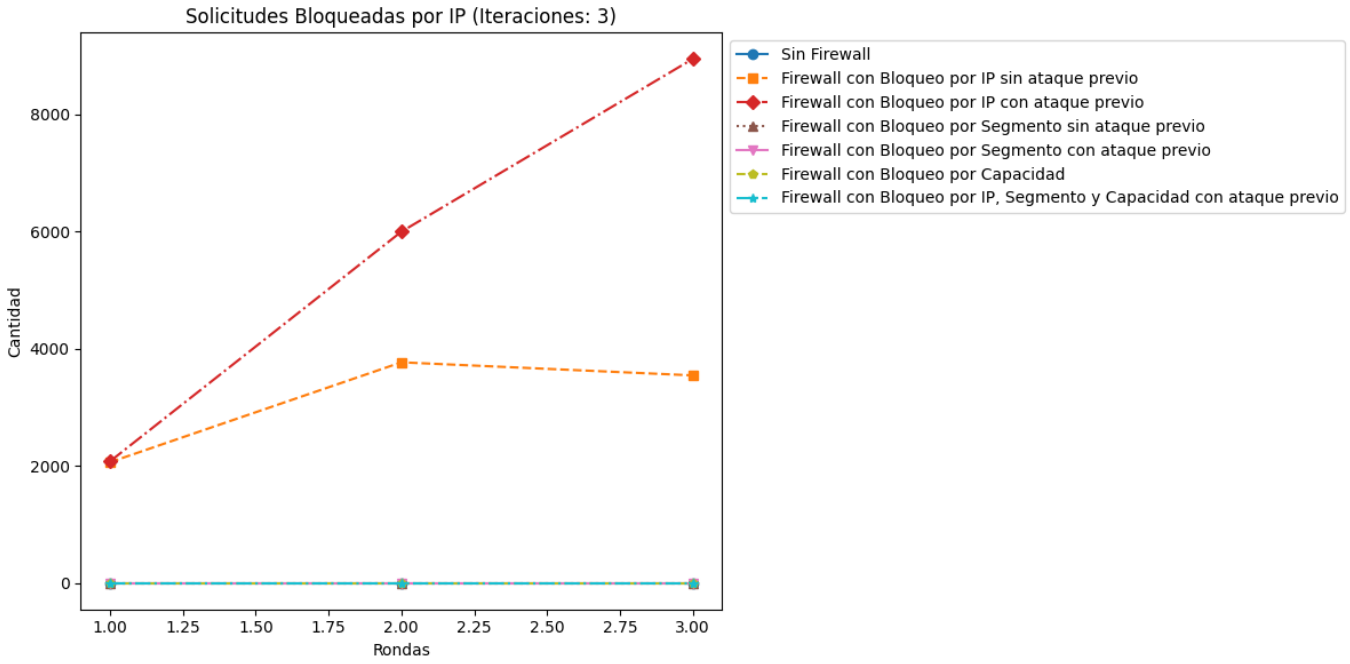

Fig. 12. Solicitudes Bloqueadas por IP

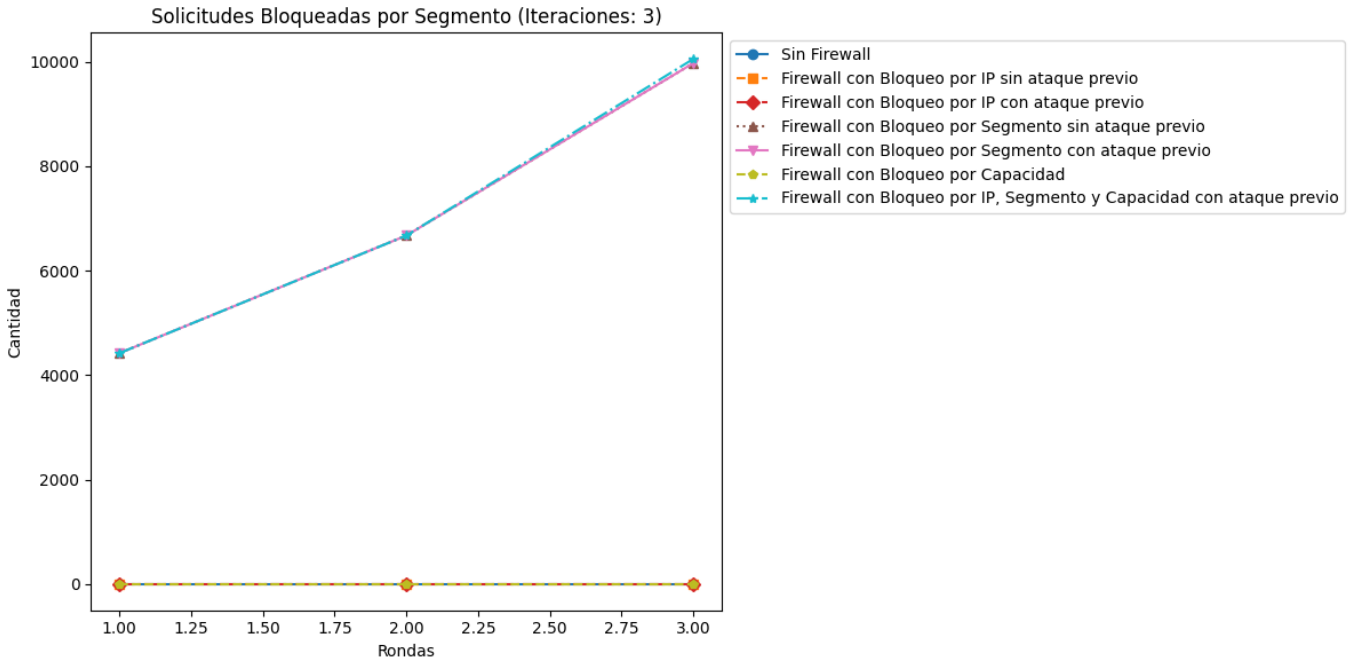

Fig. 13. Solicitudes Bloqueadas por Segmento

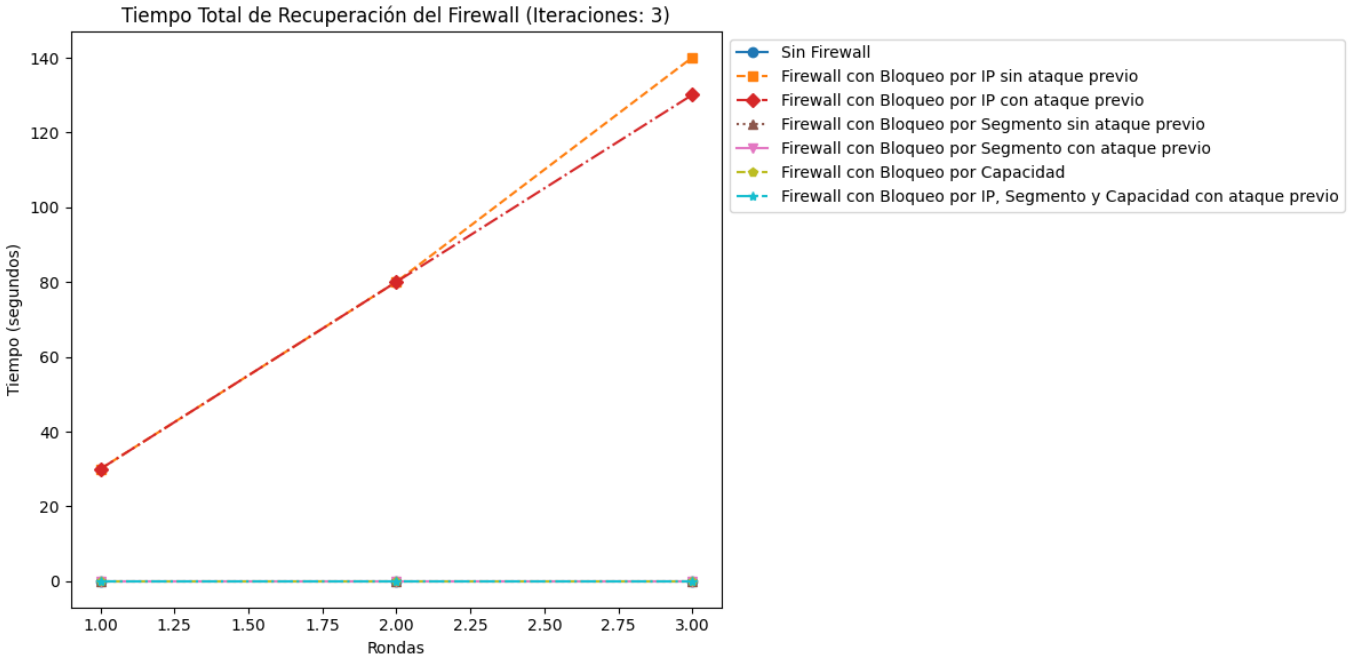

Fig. 14. Tiempo Recuperación

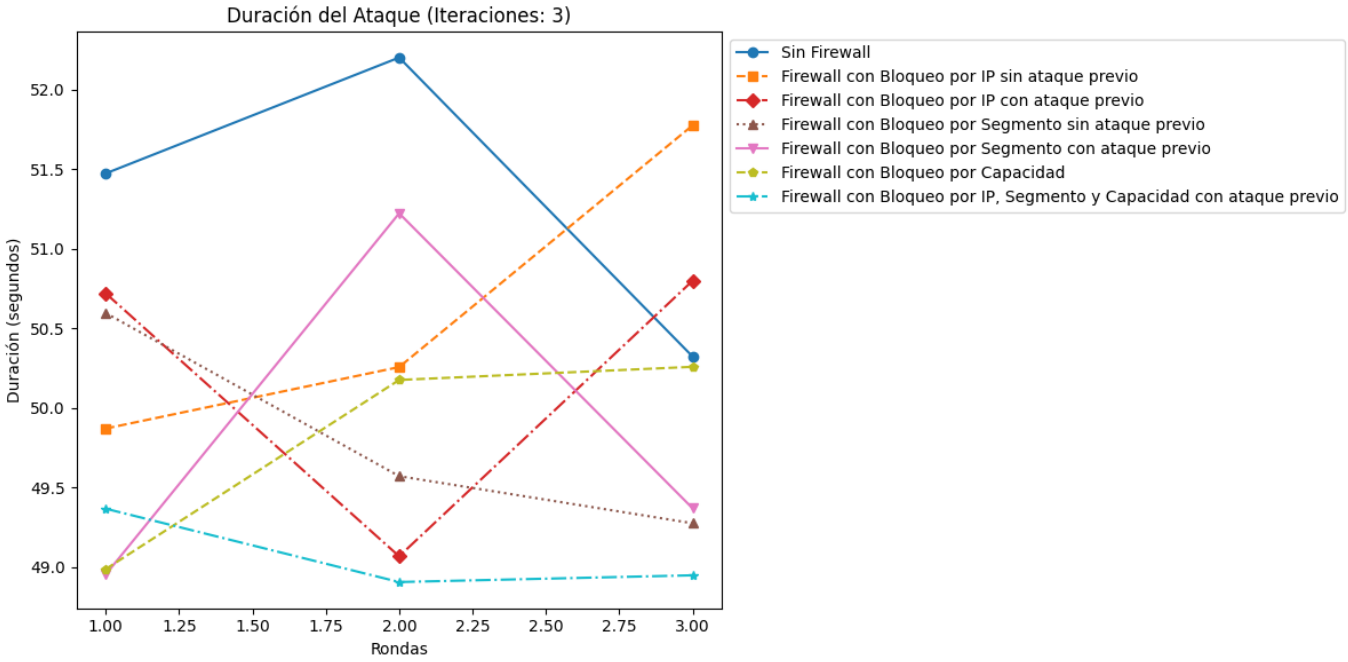

Fig. 15. Duración del Ataque