CAPITULO 5

IMPLEMENTACIÓN DEL IDS EN OMNET++

En este capítulo se describe la implementación del IDS una vez diseñado para obtener resultados que permitan medir su desempeño y eficiencia en base a los ataques empleados en la simulación, los cuales han sido descritos en el capítulo anterior. Dicho análisis se basará en el tráfico que se presentó en la red así como los ataques implementados en la simulación.

5.1 Presentación del tráfico y Ataques en la Red

Una vez establecida la red descrita en el capítulo 4, se realizó la simulación del tráfico y de los ataques generados sobre ella con el propósito de medir el desempeño del IDS diseñado. A continuación se presentan diagramas de flujo que describen el funcionamiento de la simulación en la red. Cabe recordar que la programación completa se encuentra adjunta en el disco del programa de la simulación del apéndice A.

5.1.1 Mensajes en el tráfico de Red

Inicialmente se declaran las librerías para establecer los mensajes como entradas y salidas de los nodos en la red, así como las cadenas de comando y mensajes que se generarán en la ejecución de la simulación (véase la Figura 5.1).

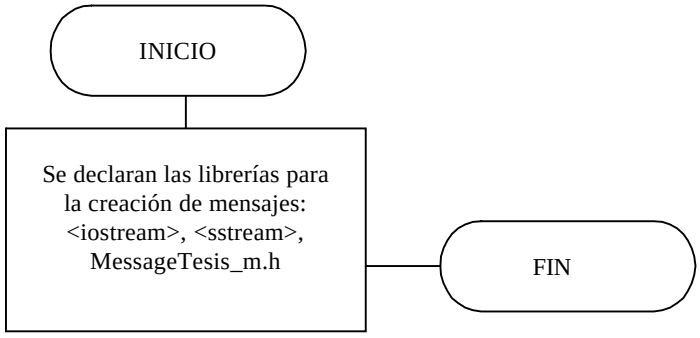

Figura 5.1: Diagrama de flujo para el proceso de creación de los mensajes en el tráfico.

En la programación se crea la clase ***MessageTesis*** para la creación de los mensajes y parte del tráfico en la red. Por otra parte tal como ocurre en un ambiente real sobre una red se realiza el conteo de los nodos por los que pasa un paquete hasta llegar a su destino. A los cambios de puntos de ruteo que haga el paquete antes de llegar a su destino se les conocen como *hops*.

Se estableció en la simulación un valor máximo de 255 *hops* o saltos de acuerdo a la *IETF (Internet Engineering Task Force)*, ya que es el máximo tiempo de vida *(TTL, Time To Live)* de un paquete al viajar por la red para que no sea descartado y así el paquete generado pueda llegar a su destino (véase la Figura 5.2).

.

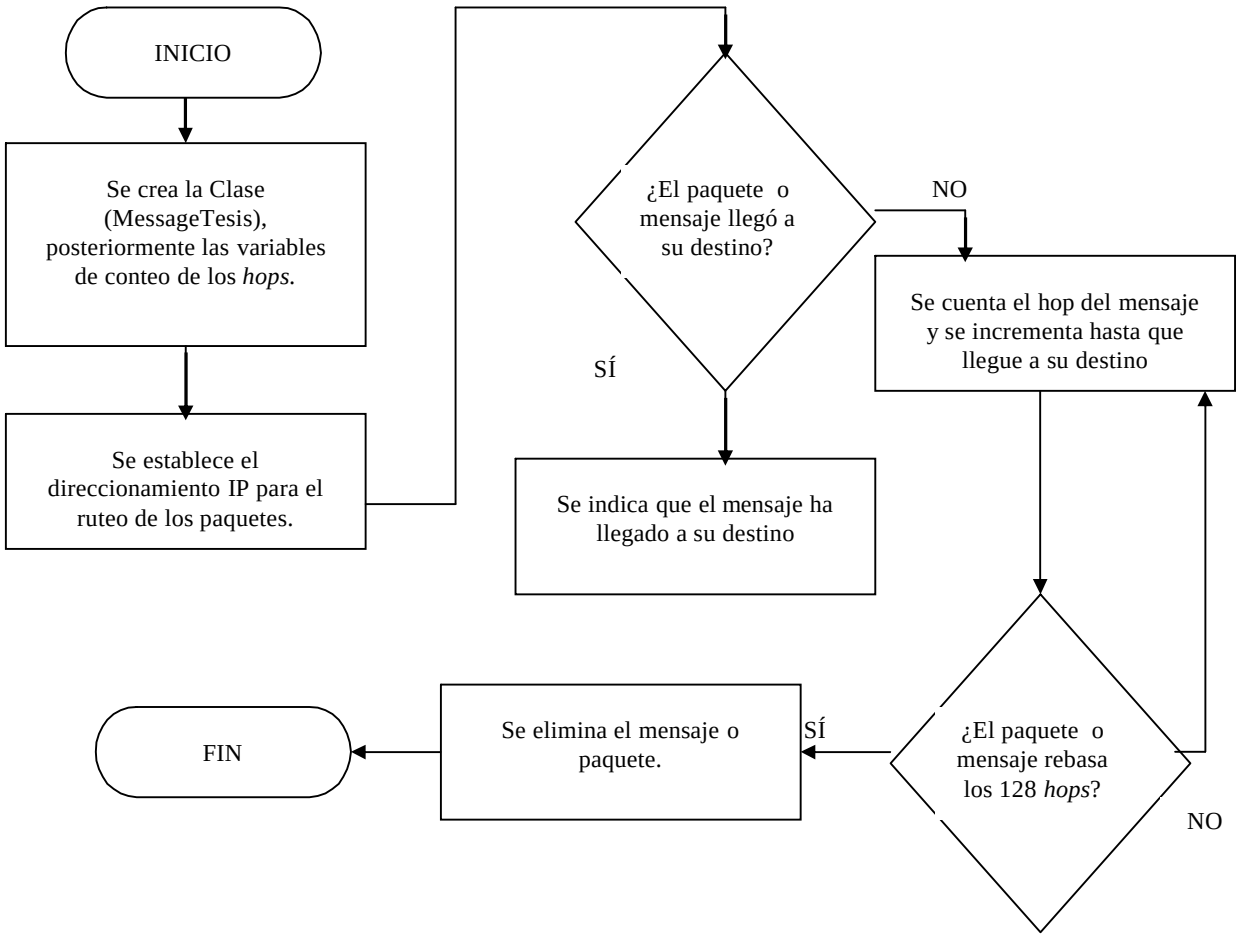

Figura 5.2: Diagrama de flujo para tráfico de los mensajes y el conteo de su TTL.

En este bloque de programación se establece el direccionamiento para los mensajes creados en la red declarando como variables las direcciones IP fuente y destino.

A continuación para que en la simulación se registren los mensajes que han transitado por la red, en el código de programación estos deben ser ordenados en un arreglo para poder ser visualizados a través de la herramienta *TKENV* de OMNET++, descrita en el capítulo 3.

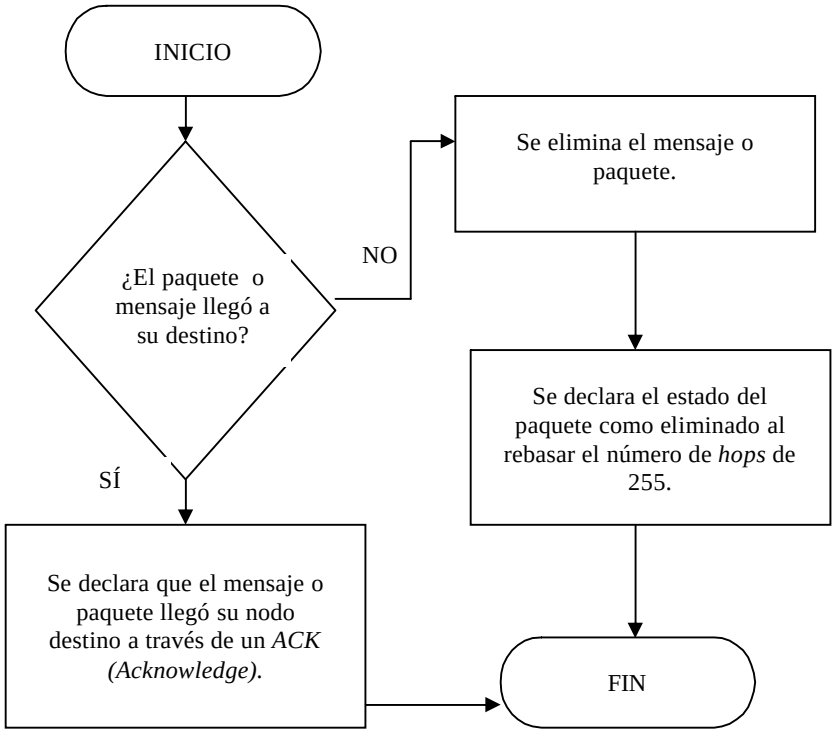

Figura 5.3: Diagrama de flujo para el registro del tráfico durante la simulación.

Ya establecida la programación para el comportamiento del tráfico se ejecuta la simulación (véase la Figura 5.4) en la que se pueden observar los paquetes o mensajes que viajan a través de la red.

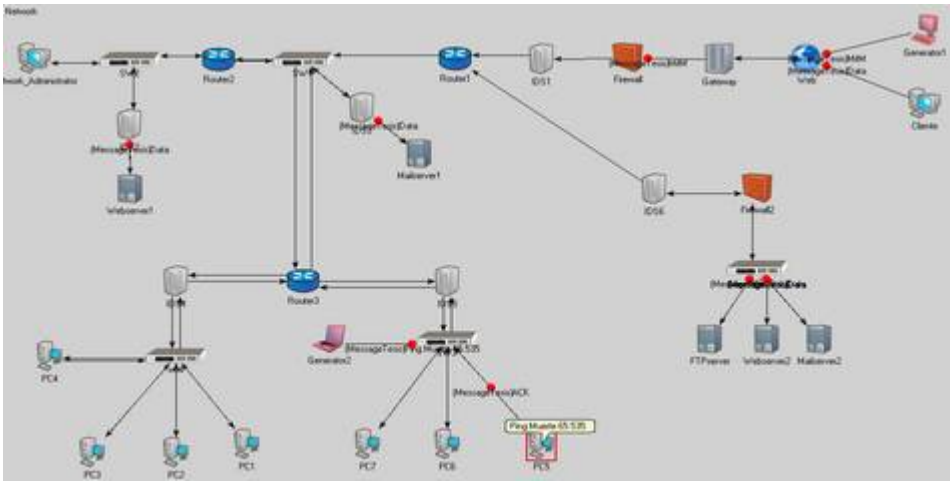

Figura 5.4: Tráfico de los mensajes sobre la red simulada en OMNET++.

5.1.2 Generación de Ataques sobre la Red

Una vez presentada la descripción de cómo fue implementado de manera general el tráfico de mensajes en la red, se describirá brevemente la estructura de datos que se siguió para la generación de los ataques (véase la Figura 5.5). Dicha estructura es la misma para ambos Generadores de ataques (Generador de ataques 1 y 2), tanto el externo como interno de la red.

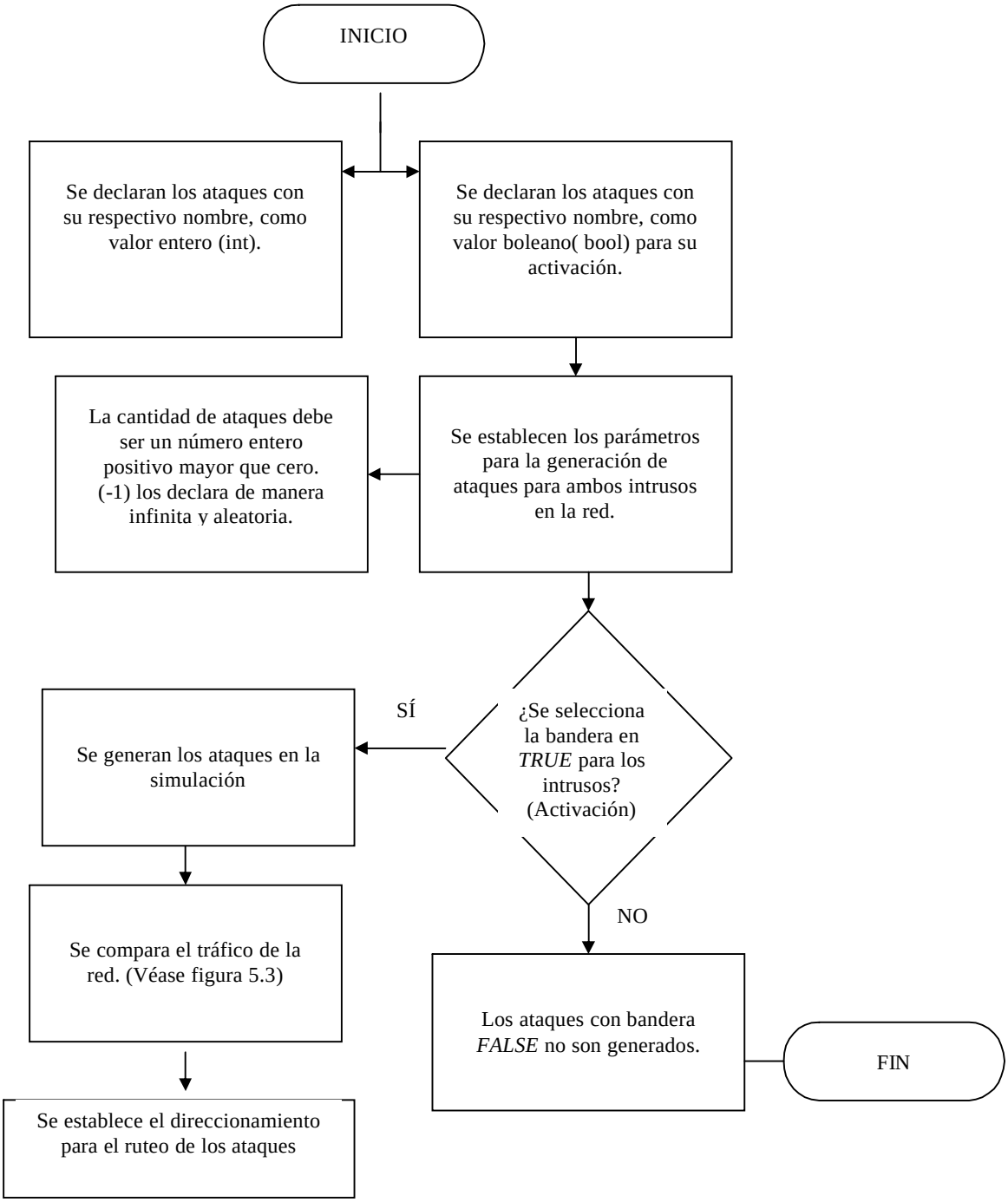

Figura 5.5: Diagrama de flujo para la generación de ataques.

Al ser establecidos los parámetros para que los intrusos generen los ataques en la red, en la simulación se indican la llegada de estas amenazas a los destinos o equipos "víctima" (véase la Figura 5.6).

Cuando el ataque llega a su destino se expande un mensaje sobre el nodo que fue afectado. Por otra parte el ataque logró su objetivo de consumir el ancho de banda del nodo víctima, se expande un mensaje como *offline*.

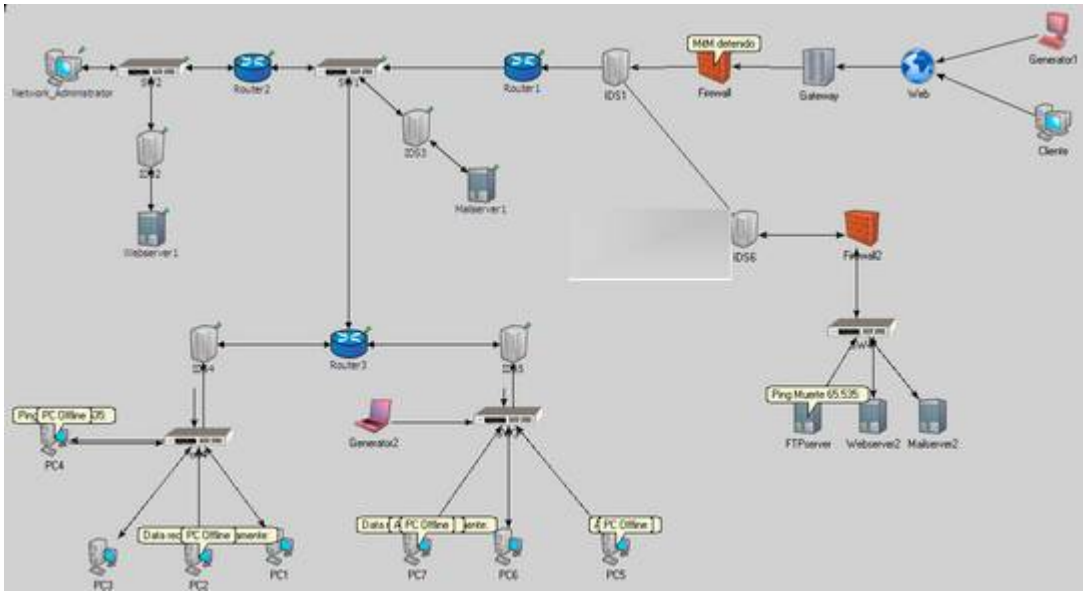

Figura 5.6: Ataques presentes en la simulación de la red con OMNET++. En esta figura se puede apreciar la presencia de un ataque *PoD* y el intento de un *MiTM.*

5.2 Diseño e Implementación del IDS

Una vez probado el desempeño del tráfico en la red simulada se continuó con el diseño del IDS para obtener un análisis del mismo tráfico y de los ataques que viajan a través de la red. Cabe mencionar que la detección de intrusos se realiza siempre y cuando ciertos mensajes o amenazas pasaron a través del sistema de seguridad. De la misma manera el IDS es reglamentado con la regla de detección de los ataques como parámetros y cuyo conteo iniciará en 0 hasta que cada uno de los ataques sea detectado y posteriormente registrado por el sistema de seguridad (véase la Figura 5.7).

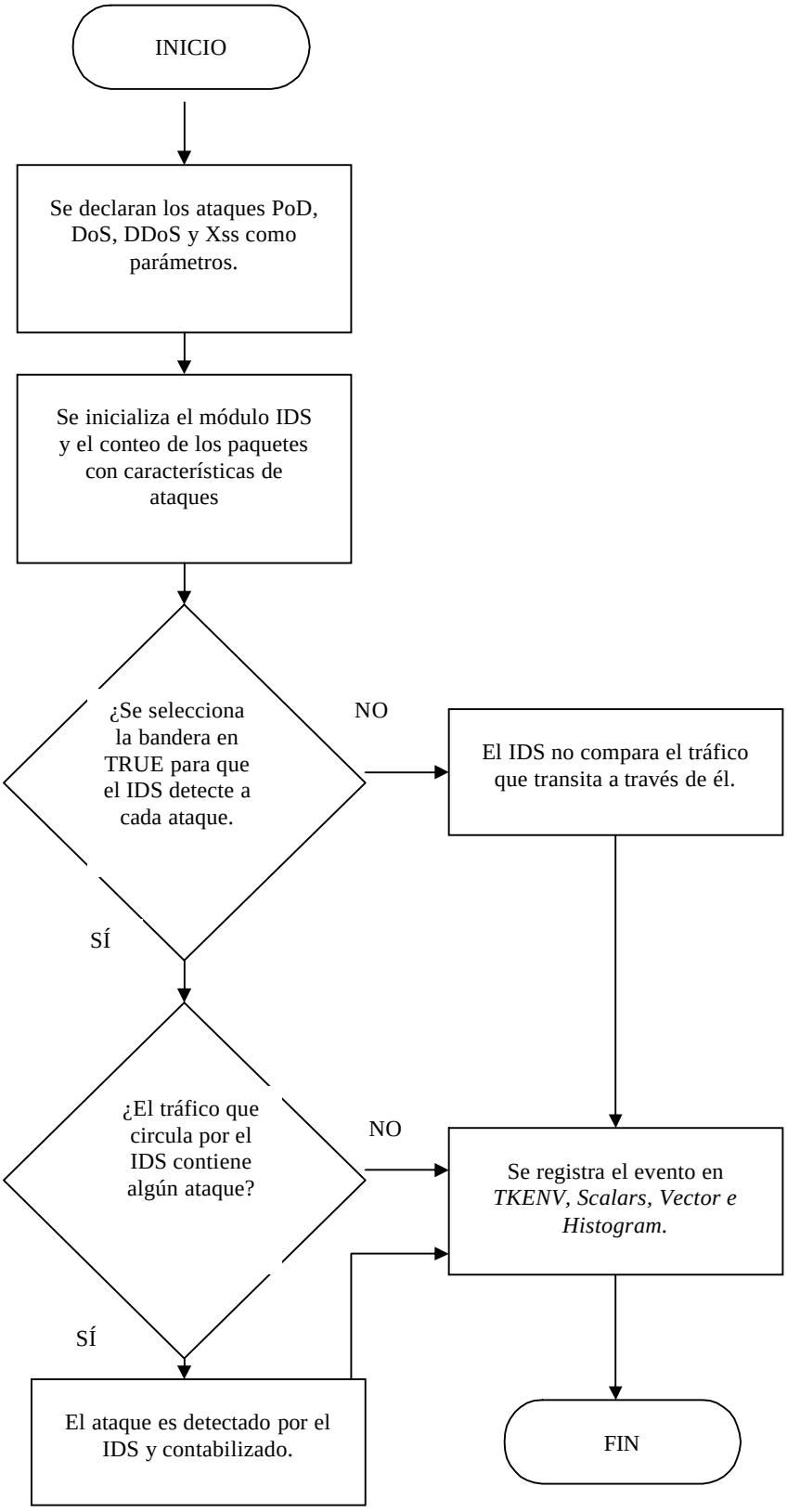

Figura 5.7: Diagrama de flujo para el desempeño y función del IDS diseñado.

5.2.1 Diseño e Implementación del Firewall

Además de contar con la presencia de un IDS, un Firewall también funciona como un sistema de seguridad pues al ser un filtro inicial del tráfico y de datos para acceder a una subred ayuda a un IDS a llevar acabo su desempeño, pues el tráfico a procesar puede ser menor y más fácil para el mismo sistema detector llevar a cabo su función. Dicha labor se describe en la sección *Implantación de las Barreras de Protección* del capítulo 2.

En la topología de la red para la simulación se establecen dos Firewall, el primero para funcionar como un filtro de seguridad en la entrada de la red y el segundo Firewall para la protección de la Zona Desmilitarizada (*DMZ)* ya que en la red interna o LAN (*Local Area Network*) se encuentra un segundo intruso. Ambos Firewall poseen la misma estructura de datos.

El Firewall diseñado se establece como un filtro que principalmente se enfoca en la detección del ataque MiTM (véanse las Figuras 5.6 y 5.8), pues debido a que su desempeño es monitorear el tráfico y capturar datos entre los nodos de la red. En un esquema real de red, este ataque sería detenido puesto que en un Firewall se puede establecer una lista de acceso, dicha lista se puede basar en direcciones IP de clientes legítimos.

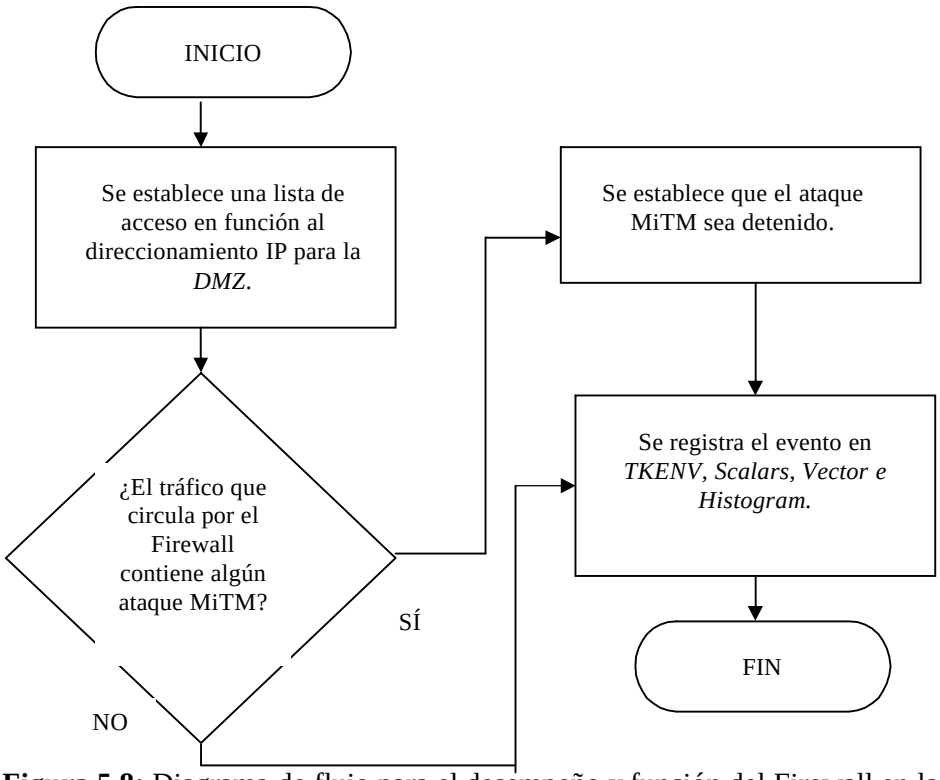

Figura 5.8: Diagrama de flujo para el desempeño y función del Firewall en la red.

5.3 Discusión

En este capítulo se ha presentado de manera breve a través de diagramas de flujo la implementación del tráfico generado, ataques, desempeño del IDS diseñado y de los Firewall establecidos en la red. Inicialmente durante la programación se estableció que el tráfico estuviera compuesto de datos o mensajes que no afecten el desempeño de los elementos de la red reflejando la comunicación entre ellos. Por otra parte se estableció una estructura de datos en la misma programación para la generación de los ataques PoD, DoS, DDoS y XSS, los cuales funcionan como ataques que provocan la denegación de servicio a las víctimas afectando su BW.

Una vez que se generó el tráfico sobre la red se lleva acabo el registro de los eventos los cuales muestran el comportamiento del tráfico y de los equipos conectados a la red ante la presencia de ataques analizando posteriormente el funcionamiento del IDS diseñado.