CAPITULO 4

DISEÑO DEL IDS

En este capítulo se describe el diseño del IDS presentado para este trabajo de Tesis. Se explican las consideraciones que se tomaron para realizar el diseño del mismo sistema de seguridad tales como la topología de red sobre la que se llevó acabo la simulación y los ataques que más adelante se implementaron.

4.1 Topología de Red

La implementación de la red para la simulación realizada en este trabajo de tesis se enfoca inicialmente en la topología de la Figura 4.1 sobre la cual se realizó la simulación y en el que los datos o paquetes generados por los elementos externos a la red (Generador 1 y Cliente) deben pasar por ciertos puntos de la misma red.

Posteriormente la red interna se compone de dos subredes con su respectivo dominio o direccionamiento, así mismo en una de las subredes se colocó a un segundo generador de ataques con el propósito de analizar el desempeño de los IDS tal como se hará con el generador de ataques 1. Por otra parte la red tiene una Zona Desmilitarizada *(DMZ*) que contiene a sus respectivos Servidores de Mail, Web y DNS siendo descrita más adelante en este capítulo.

También se cuenta con un administrador de red el cual desempeña la función de analizar el tráfico en la misma a través de los IDS para el desempeño y función de detección de alguna amenaza o ataque y posteriormente registrarlos.

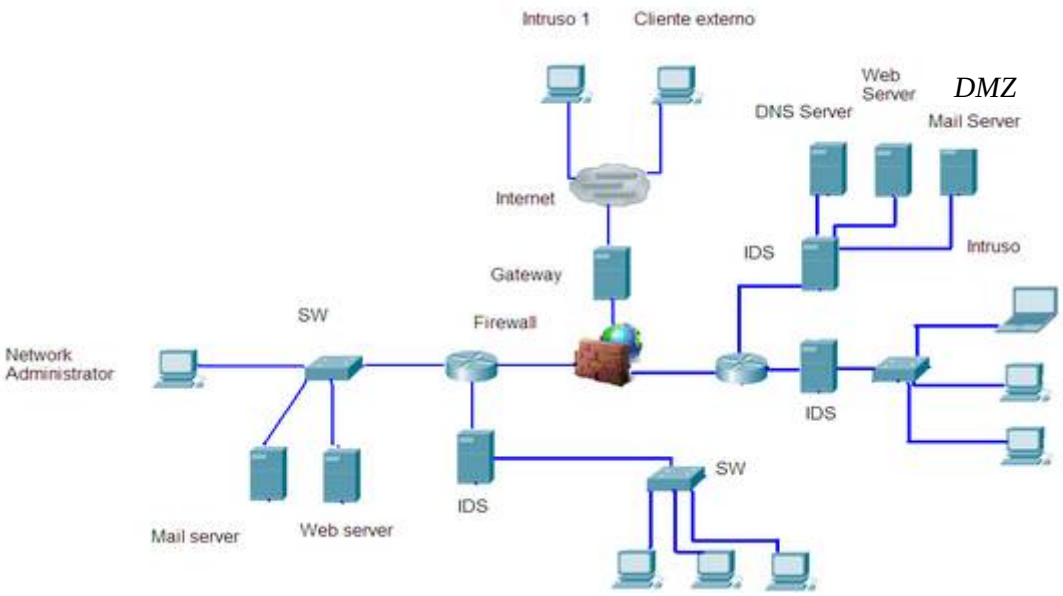

Figura 4.1: Esquema aproximado de la topología de red para la simulación.

Una vez presentado el esquema de la red para realizar la simulación se realizó el diseño final en OMNET++ (véase la Figura 4.2).

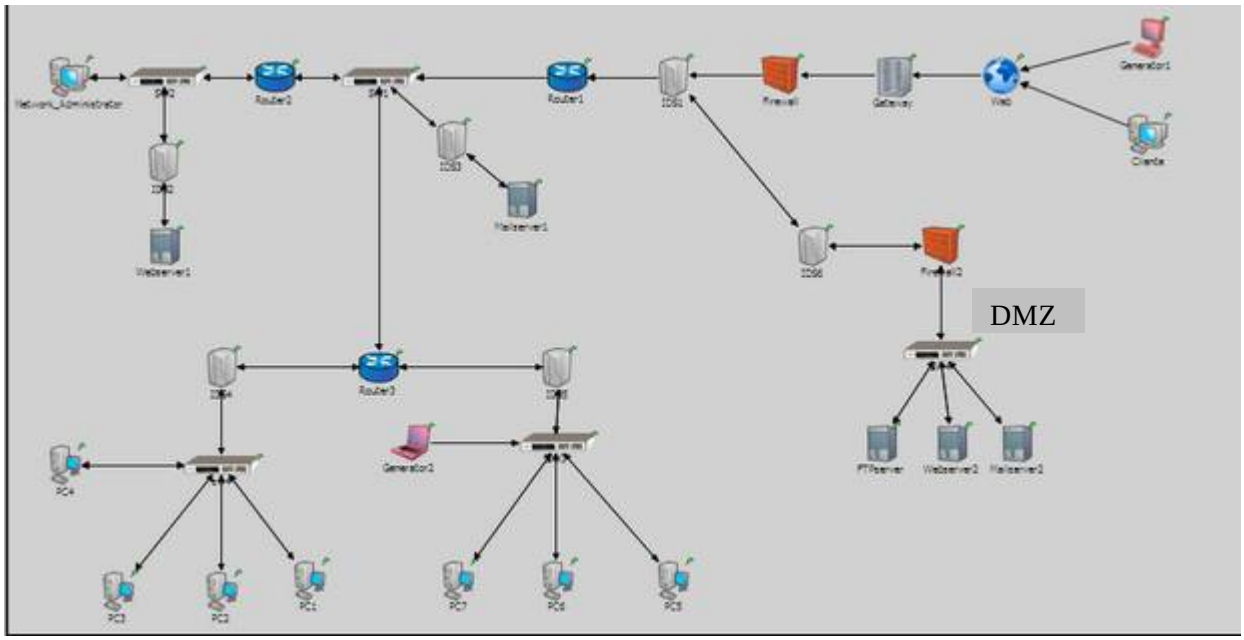

Figura 4.2: Topología de la red para la simulación en OMNET++.

A continuación en la Figura 4.3 se muestra el direccionamiento IP establecido en la topología presentada de la Figura 4.2.

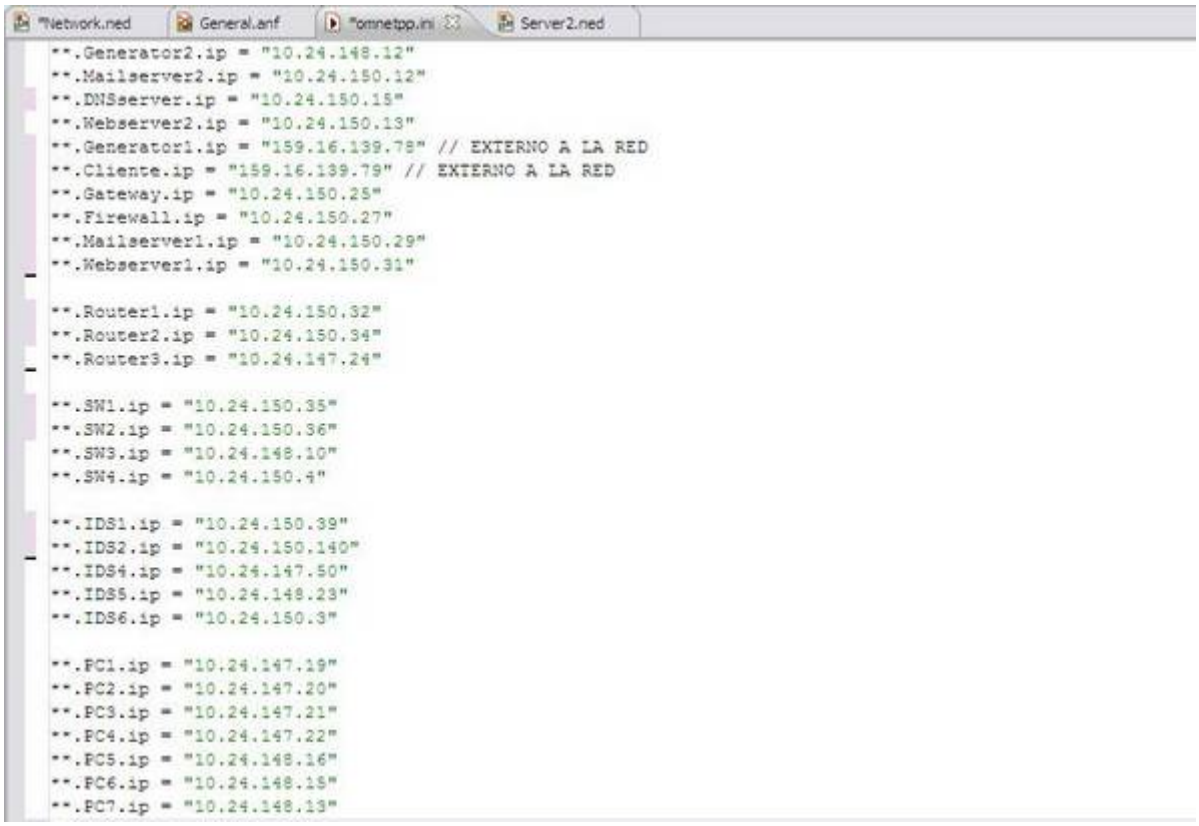

Figura 4.3: Direccionamiento IP para los elementos de la red simulada en OMNET++.

En la Figura 4.3 se presentan las direcciones IP establecidas para el reconocimiento de cada elemento que conforma a la red simulada, cabe mencionar que las características de este direccionamiento es que los dominios *10.24.150, 120.24.148* y *10.24.147* pertenecen a la red interna siendo direcciones clase A, cuyo rango es *1.0.0.0* a *127.255.255.255*, mientras que las direcciones para los elementos externos en la red (Generator 1 y Cliente) pertenecen a la clase B, cuyo rango es del *128.0.0.0* a *191.255.255.255.*

Tal direccionamiento se estableció siguiendo el criterio de definición de redes además de que se emplean estas direcciones como estáticas, el rango del dominio de la red interna permite la conectividad de un mayor número de host, tratándose de un ámbito real, mientras

que el direccionamiento establecido para los elementos externos de la red es para distinguirlos de que provienen de otra red.

Como en toda red existe el retardo en el tráfico a través del medio de transmisión de los datos, este valor puede ser variado dando doble click sobre los enlaces ilustrados como flechas en la Figura 4.2, los cuales conectan a cada uno de los nodos en la red de la simulación. Éste valor debe ser establecido de tal manera que el tráfico de los mensajes pueda llegar a sus nodos destinos y los valores (ya sean ataques o mensajes de datos) sean reflejados en las gráficas correspondientes y la cogestión sea menor.

4.2 Zona Desmilitarizada (DMZ)

Una zona desmilitarizada (*DMZ*) o red perimetral es una red local (una subred) localizada entre la red interna de una organización y una red externa. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas *[2, 6]*. La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos externamente de la red, tales como servidores de e-mail, Web y DNS (véase la Figura 4.2).

Por lo general la política de seguridad para la DMZ es la siguiente:

- El tráfico de la red externa a la DMZ está autorizado
- El tráfico de la red interna a la DMZ está autorizado
- El tráfico de la red interna a la red externa está autorizado
- El tráfico de la DMZ a la red externa está denegado si no se cuenta con una autorización previa para el acceso.

De esta manera la DMZ posee un nivel de seguridad intermedio el cual no es lo suficientemente alto para almacenar datos imprescindibles. Debe tomarse en cuenta que es posible instalar una DMZ en forma interna para aislar la red interna con niveles de protección variados y así evitar intrusiones internas y externas.

4.3 Ataques Implementados para la Simulación

En esta sección del trabajo de tesis se consideraron ciertos ataques, que debido a su desempeño fueron funcionales para el desarrollo de la simulación y el diseño del IDS. Dicho desempeño se consideró de acuerdo a la manera en cómo se afecta el recurso del ancho de banda y que para el caso de la simulación se enfocan estos ataques en atacar el mismo recurso de los nodos PCs o servidores. A continuación se definirá a cada uno de ellos.

4.3.1 DoS (*Denial Of Service*)

Este ataque se basa en la desorganización de un sistema para tener acceso al mismo, bloqueando el acceso de los servicios al cliente "víctima". Es un ataque a un sistema de computadoras que causa que un servicio o recurso sea inaccesible a los usuarios legítimos provocando la pérdida de la conectividad causado por el consumo del ancho de banda del sistema de la víctima o sobrecarga de sus recursos computacionales (véase la Figura 4.4) *[12]*.

De esta forma si un ordenador "mal intencionado" solicita un número suficiente de peticiones simultaneas puede llegar a saturar los puertos del servidor y provocar que éste deje de funcionar correctamente, puesto que el servidor deja de prestar servicio a nuevas peticiones, sean legítimas o no *[20]*.

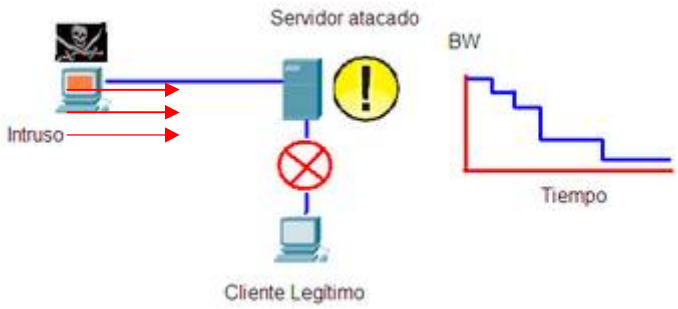

Figura 4.4: Ejecución de un Ataque DoS.

Como se muestra en la Figura 4.4 el intruso afecta al elemento atacado (servidor) provocando un consumo mayor en sus recursos tales como ancho de banda o memoria RAM. De esta forma el atacante consigue que el servidor no logre restablecer las nuevas conexiones, es decir que los siguientes usuarios que intenten acceder, sean atacantes o no, serán rechazados y se les denegará el servicio. Este ataque se encuentra descrito de manera detallada a través del RFC[5] 4732.

[5]RFC: Request for Comments: Conjunto de información que contiene registros y propuestas para mejorar el desempeño del Internet *[15]*.

4.3.2 DDoS (*Distributed Denial Of Service*)

Un ataque DDoS es un tipo de ataque DoS el cual consiste en la ejecución de un ataque conjunto y coordinado entre varios equipos hacia un servidor "víctima". De la misma manera que el ataque anterior, su objetivo es agotar el BW saturando la capacidad de procesamiento de la víctima *[12]*.

En este tipo de ataques suelen emplearse ordenadores "*bots*" que son equipos o nodos en una red infectados por un software que permite a un usuario remoto controlarlos (véase la Figura 4.5). De esta forma es posible coordinar un ataque desde decenas de ordenadores señuelos de forma simultánea. De la misma manera se genera mediante la saturación de los puertos con flujo de información provocando que el servidor se sobrecargue y no pueda seguir prestando servicios *[21]*. Su RFC es el 3552.

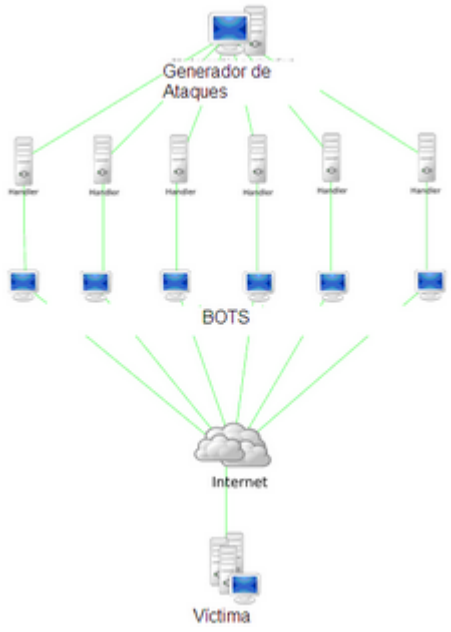

Figura 4.5: Desarrollo del ataque DDoS *[12]*.

4.3.3 PoD (*Ping of Death*)

Un Ping[6] of Death es un ataque enviado a una computadora o servidor, el cual consiste en enviar numerosos paquetes ICMP mayores a 65.535 bytes con el fin de colapsar el BW (Ancho de banda) del sistema atacado. Este ataque consiste en mandar un Ping deformado, puesto que su tamaño real es de 64 bytes y debido a que en algunas computadoras sus sistemas no pueden manejar *PINGS* de tamaño mayor, se provoca que su sistema se caiga de la forma en que se mencionó anteriormente *[13]*.

Se caracteriza por ser uno de los ataques de negación de servicio, teniendo como objetivo saturar los recursos del sistema de la víctima de tal forma que se inhabilitan los servicios brindados por la misma, tal como la comunicación entre un nodo y los demás elementos de una red acumulando buffers con información de las conexiones abiertas, impidiendo así tener conexiones legítimas y el acceso a los respectivos clientes. Dicha información se encuentra contenida en documento RFC 4732 *[22]*.

4.3.4 XSS (*Cross-Site Scripting)*

Es un tipo de intrusión que explota la vulnerabilidad del sistema de validación HTML. Es un ataque contra aplicaciones Web en los que un atacante toma el control sobre el navegador de un usuario con el objetivo de ejecutar códigos o scripts maliciosos escritos en lenguaje HTML ó JavaScript (véase la Figura 4.6) *[14]*.

Se realiza una modificación del código HTML de modo que dicha modificación se caracteriza como un ataque cuando se modifica la información relativa a la ubicación de uno o varios contextos dados, permitiendo manipular el sistema de la víctima y sus aplicaciones.

---

[6]Ping: Packet Internet Grouper. Comprueba el estado de la conexión con uno o varios equipos remotos por medio de los paquetes de solicitud de eco y de respuesta de eco (ambos definidos en el protocolo de red ICMP) *[13]*.

```
<HTML>
<title>Hola</title>
<a href=´http://www.trusted.domain/VWA/<script> \
Document location=´´\
http://www.malicious.domain/city.jpg?stolencookies=´´\
+document.coockie;\
</script>´>enlace</a>
</HTML>
```

Figura 4.6*:* Desarrollo de un ataque XSS *[14]*.

En la Figura 4.6 se muestra el código de enlace que dirigirá al usuario hacia un sitio web vulnerable, generando posteriormente una página de error indicando que el recurso solicitado no existe y en el que a continuación se trasladará al usuario a un sitio que domina el atacante para obtener y manipular la información del mismo usuario *[14]*.

4.3.5 Ataque MITM *(Man in the Middle)*

Es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar los mensajes entre dos partes sin que ninguna de ellas conozca que el medio de comunicación entre ellos es controlado por un sistema intruso. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas a través de un *Sniffer*, el cual es un software herramienta que le permite monitorear el tráfico en la red (véase la Figura 4.7) *[28]*.

El desarrollo de este ataque se basa en el protocolo Diffie-Hellman, el cual permite el intercambio secreto de claves entre dos partes que no han tenido contacto previo, utilizando un canal inseguro, y de manera anónima. Este protocolo se emplea generalmente como medio para establecer claves simétricas que serán empleadas para el cifrado de una sesión *[1]*.

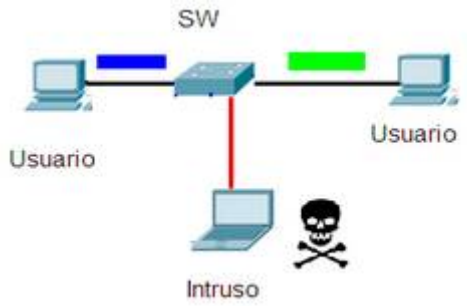

Figura 4.7: Esquema de una red afectada por el ataque MiTM *[28].*

4.4 Snort Rule del IDS diseñado

Para el diseño del IDS en OMNET++ dada la plataforma de programación del simulador *(C++)* se llevó a cabo el establecimiento de las reglas para el diseño del IDS siguiendo los siguientes parámetros y estructura para el buen desempeño y función del sistema. En la Figura 4.8 se muestra el diagrama de flujo que obedece el funcionamiento del IDS diseñado.

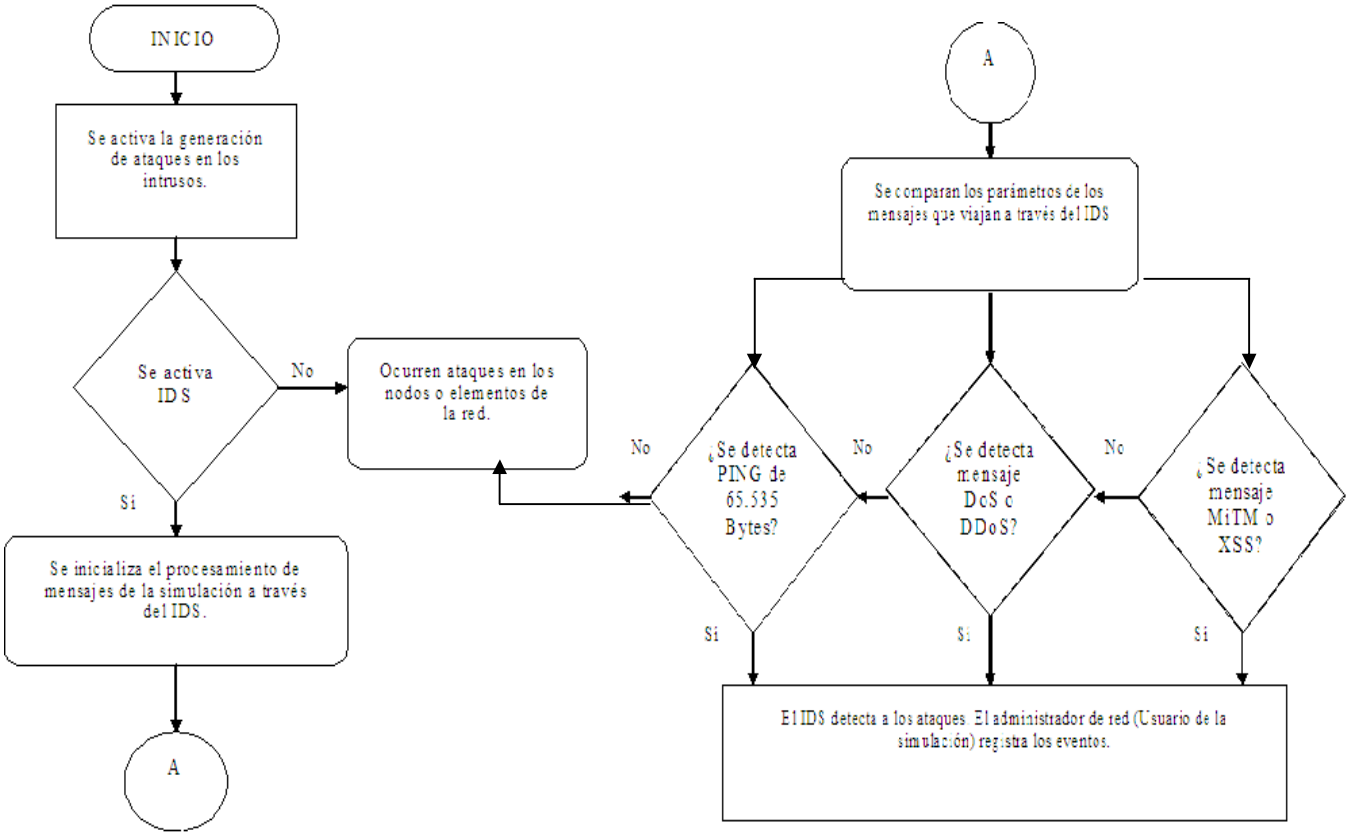

Figura 4.8: Diagrama de flujo del funcionamiento del IDS.

Para realizar el diseño del IDS se estructuró de la siguiente manera la regla de Snort (véase la Figura 4.9).

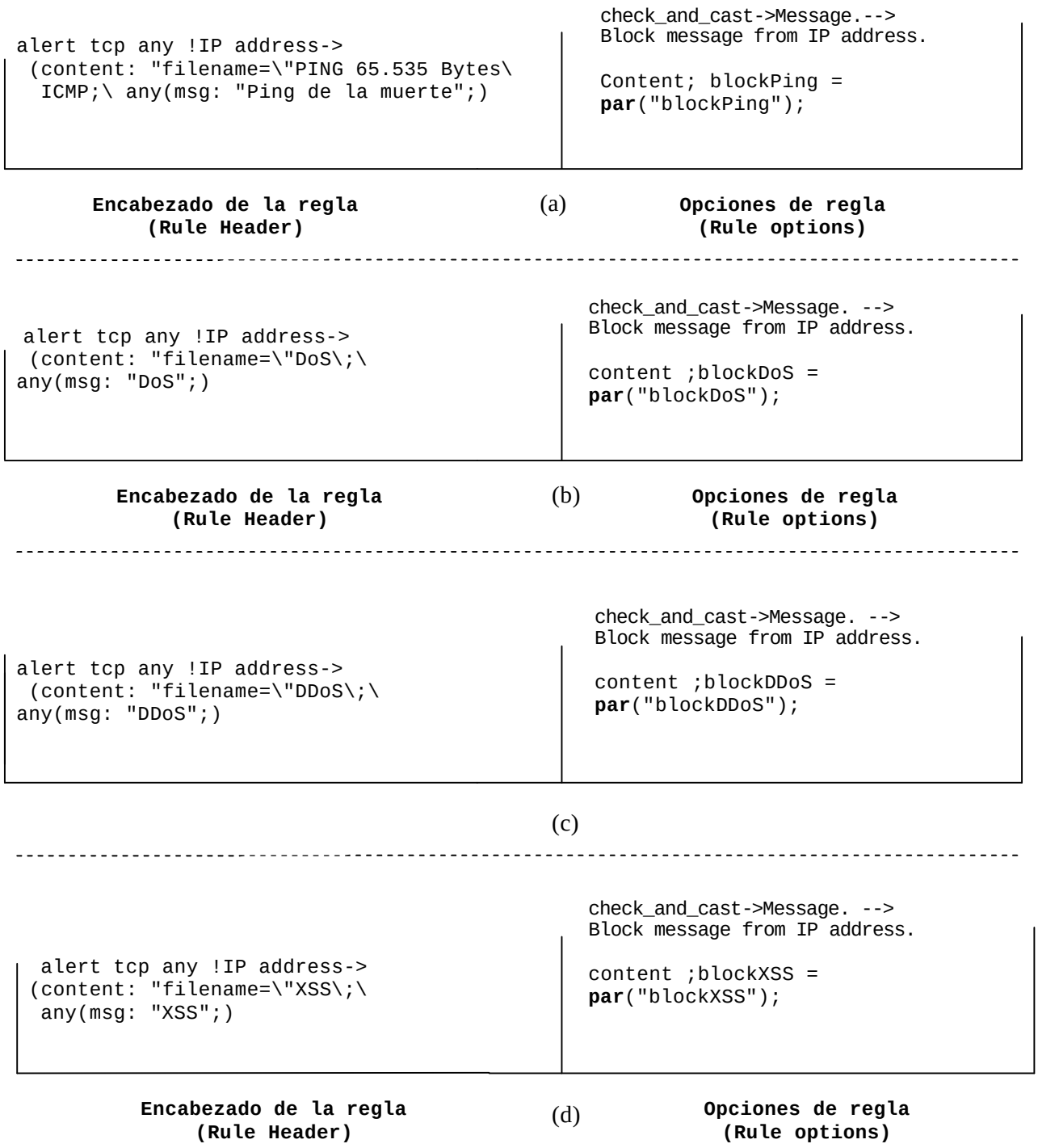

Figura 4.9: Snort Rule para el diseño del IDS. (a) Reglas establecidas para la detección del ataque PoD. (b) DoS. (c) DDoS. (d) XSS

El Snort Rule presentado en la Figura 4.9 es el establecido para el diseño del IDS en este trabajo de Tesis. Tal como se muestra en dicha regla, en el encabezado se indica como alerta la detección de los datos o tipos de mensajes programados como posibles amenazas para los demás elementos en la red, mientras que en el bloque de Opciones de la regla se establece como indicación que primero se compare el mensaje que fue detectado por el IDS, y si fue un mensaje o dato que no sea considerado como amenaza, éste continúe con su trayectoria, de lo contrario este sea bloqueado y registrado.

4.5 Discusión

En este capítulo se ha presentado la topología de red sobre la cual se realizó la simulación y posteriormente el diseño del IDS. Se describieron los ataques que se emplearon para realizar el diseño del sistema de seguridad. Cabe mencionar que estos ataques fueron considerados para este trabajo de tesis por ser amenazas de denegación de servicio y cuyo resultado se puede reflejar en el daño causado al BW (*Band Width*). Respecto al diseño del IDS se describe la regla de *snort* para este sistema en el cual se indican las condiciones y acciones que se deben tomar para intrusos al ser detectados.