CAPITULO 2

SISTEMAS PARA DETECCIÓN DE INTRUSOS

En este capítulo se explica la importancia de los sistemas de seguridad que se emplean para las redes de comunicaciones tales como los IDS junto con los Firewall en base al funcionamiento de estos sistemas para preservar una transferencia de datos que asegure la privacidad y arribo de la información al destino deseado. Por otra parte se hace una breve descripción general de los ataques en base a su desempeño en una red.

2.1 Intrusos y Ataques en la Red

La comunicación entre los sistemas que conforman a una red se da en base a los protocolos TCP/IP (*Transmission Control Protocol/Internet Protocol*), los cuales se definen como un conjunto de protocolos de comunicación que permiten direccionar y transportar la información en la red.

Dados estos protocolos de comunicación, usuarios como organizaciones o empresas y clientes individuales se vuelven más dependientes de los servicios de las redes informáticas y en el que si existiera problema alguno sobre ellas, se puede llegar a comprometer la continuidad de sus operaciones.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes con una mejor organización e incluso tecnología, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios y que por consiguiente no deben subestimarse las fallas de seguridad provenientes del interior del sistema del usuario, por lo que se emplean sistemas que detecten y prevengan ataques o intrusiones *[9]*.

Un ataque o intrusión es un evento en una red de comunicación el cual consiste en aprovechar una o más vulnerabilidades de los recursos de un sistema informático tal como un sistema operativo, software u otro sistema del usuario con el fin de causarle un daño, ya sea bloqueando el acceso de clientes legítimos a un servidor o controlar de manera remota algún nodo en una red sin consentimiento del mismo usuario *[9]*.

Los ataques ocurridos en Internet son debido a que el intruso tiene la capacidad y herramientas tales como hardware y software especializado para realizar la intrusión o ataque en algún equipo conectado en la red aprovechando su vulnerabilidad, permitiéndole acceso al intruso. A continuación se explicará la clasificación de los ataques en un contexto general tales como los ataques pasivos y activos, los cuales se definen de acuerdo en la manera en cómo afectan a una red.

Dado el desempeño de las amenazas o ataques en la red, estos se pueden dividir en cuatro categorías de manera general:

- **Interrupción**: Cuando un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad de servicio. Ejemplos de este ataque son la destrucción de un elemento hardware como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión a través del consumo del ancho de banda *(BW, Band Width).*
- **Intercepción**: Ocurre cuando una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. El intruso podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son la intervención en una línea para obtener datos que circulen por la red y la copia ilícita de ficheros o programas.
- **Modificación**: Una entidad no autorizada no sólo consigue acceder a un recurso sino que es capaz de manipularlo. Este es un ataque contra la integridad de algún sistema. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterando un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.
- **Fabricación**: Se da cuando una entidad o usuario en la red no autorizado inserta objetos falsificados en el sistema tales como códigos de acceso y páginas falsas. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo *[23]*.

2.1.1 Ataque Pasivo

Un ataque pasivo es aquél en el que el intruso monitorea el tráfico en la red (*eavesdropping*) para capturar contraseñas u otra información para su uso posterior. Los objetivos esenciales

de este tipo de ataque son la intercepción de datos y el análisis de tráfico para obtener información de la comunicación presente en la red, a fin de conocer la rutina del tráfico en una red de interés para el intruso.

Los ataques pasivos son muy difíciles de detectar ya que no provocan alteración alguna de los datos. Sin embargo es posible evitar su éxito mediante el cifrado de la información. Un claro ejemplo de este tipo de ataque es el uso de un *Sniffer* que es un software especializado en el análisis del tráfico en una red y de este modo poder detectar y conocer qué vulnerabilidades se tienen en la red para recabar la información de mayor interés *[23]*.

2.1.2 Ataque Activo

En un ataque activo el intruso interfiere con el tráfico legítimo o de clientes que fluye a través de la red, explotando las vulnerabilidades de la misma red o de manera específica de alguna víctima. Dado que este ataque puede afectar su desempeño puede subdividirse en cuatro categorías.

- **Suplantación de identidad**: El intruso se hace pasar por un cliente legítimo por secuencias de autenticación capturando distintas direcciones IP. De esta manera se suplanta al usuario, conociéndose este proceso como *IP Spoffing*, en el que a una entidad no autorizada se le permite acceder a una serie de recursos privilegiados en una red representando al cliente que puede hacer uso de ellos.
- **Reactuación**: Evento que ocurre cuando uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.
- **Modificación de mensajes**: Una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, la falsificación de cuentas para que un cliente deposite cantidades de dinero de manera repetida y en cuentas diferentes a la que en verdad debe realizarse la transacción *[24]*.
- **Degradación fraudulenta del servicio**: Se impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicación puesto que el intruso suprime todos los mensajes dirigidos a un determinado elemento en la red. Por otra parte el intruso

puede interrumpir el servicio de una red inundándola con mensajes no auténticos *[24]*. Entre estos ataques se encuentran los de denegación de servicio como el DoS (*Denial of Service*) y DDoS (*Distributed Denial of Service*), que suspenden temporalmente el servicio de un servidor de correo, Web o FTP (*File Transmision Protocol*).

2.2 Sistemas para Detección de Intrusos

Un IDS *(Intruder Detection System)* o Sistema para Detección de Intrusos es una herramienta o sistema de seguridad que monitorea el tráfico en una red y los eventos ocurridos en un determinado sistema informático, para así poder identificar los intentos de ataques o amenazas que puedan comprometer la seguridad y el desempeño de dicho sistema. El desempeño de los IDS se basa en la búsqueda y análisis de patrones previamente definidos que impliquen cualquier tipo de actividad sospechosa o maliciosa sobre una red o host.

Los IDS aportan a la seguridad una capacidad de prevención y de alerta anticipada ante cualquier actividad sospechosa. Los IDS incrementan la seguridad de algún sistema o red vigilando el tráfico, examinando los paquetes en busca de datos sospechosos que puedan afectar a los elementos de la red *[4, 15]*.

Para que un IDS pueda funcionar correctamente en una red establecida detectando posibles amenazas o intrusiones, este sistema de seguridad se compone de los siguientes elementos:

- **Fuentes de recolección de datos:** Su propósito es conseguir de una manera eficiente todos los datos necesarios durante el proceso de detección de intrusos. Estas fuentes pueden ser un *log* o el software de base de datos.
- **Reglas de contenido de datos:** Contienen los patrones para detectar anomalías de seguridad en el sistema.
- **Filtros:** Para analizar y comparar el tráfico monitoreado en la red de acuerdo a las reglas de contenido de datos.
- **Detectores de eventos anormales en el tráfico de red**: Permite al IDS desempeñar su función como detector de intrusos y amenazas para que posteriormente se evite algún ataque a la red.

- **Dispositivo generador de informes y alarmas**: El IDS cuenta con sensores y dispositivos que le permiten avisar al administrador de la red sobre posibles amenazas que puedan afectar el desempeño y funcionamiento de los elementos en la red *[1, 6,2].*

Un *log* es el registro de actividad de un sistema que generalmente se guarda en un fichero o base de datos y al que se le van añadiendo información a medida que se realizan acciones sobre el sistema *[7]*.

2.2.1 Clasificación de los IDS

Dada la función que desempeñan los *IDS* existen dos enfoques que los permiten clasificarse, el primero en ***función de los sistemas que vigilan*** y el segundo en ***función de cómo es que realizan dicha función.*** La primera de estas clasificaciones se enfoca en sistemas que analizan actividades de un host o una máquina en busca de posibles ataques o los que lo hacen en una subred. Por lo que surge una siguiente clasificación dentro de este primer enfoque: Los IDS basados en Red y los IDS basados en Host *[15]*.

IDS basados en Red.

Un ***IDS basado en Red*** monitorea los paquetes o datos que transitan en la red en busca de elementos que se caractericen por ser una posible amenaza contra alguno de los sistemas ubicados en la misma red; el IDS puede situarse en cualquiera de los *hosts* o en un elemento que analice todo el tráfico tal como en un HUB o un enrutador.

Estos sistemas de seguridad actúan sobre una red capturando y analizando paquetes de red a través de un *sniffer* que es un sistema (Hardware o software) que sensa el tráfico de la red, posteriormente el sistema analiza los paquetes capturados buscando patrones que supongan algún tipo de ataque. El análisis del tráfico es en tiempo real, dada esta función los IDS basados en red no sólo trabajan a nivel TCP/IP o transporte si no también a nivel de aplicación *[25, 15]*.

IDS basados en Host

Por otra parte, los ***IDS basados en Host*** realizan su función protegiendo un único sistema buscando patrones que puedan denotar un intento de intrusión, alertando o tomando las

medidas oportunas en caso de que uno de estos intentos sea detectado. Entre más información se le otorgue al administrador de red sobre los ataques o amenazas, mejor será su desempeño para el alertamiento oportuno de posibles ataques en la red *[25] [15]*.

La segunda clasificación de los IDS se realiza en función del desempeño en la detección de ataques, subdividiéndose dos secciones del mismo grupo, siendo los sistemas basados en la ***detección de anomalías*** y ***en la detección de usos indebidos del sistema.***

Detección de anomalías.

La base del funcionamiento de estos sistemas es suponer que una intrusión se puede ver como una anomalía, ya que el sistema de detección de intrusos es capaz de establecer el comportamiento habitual de los sistemas ante una o varias amenazas establecidas, siendo capaz de detectar las intrusiones en base a estadísticas *[25, 15]*.

Detección de usos indebidos.

El funcionamiento de los IDS basados en la detección de usos indebidos presupone que se pueden establecer patrones para los diferentes ataques conocidos y algunas de sus variaciones; mientras que la detección de anomalías conoce lo que sólo fue establecido sin las respectivas variaciones *[25, 15]*.

2.2.2 Colocación de un IDS en la Red

Para tener un funcionamiento adecuado en un sistema de detección de intrusos (*IDS*) se requiere crear en el sistema un registro de firmas (Características de intrusiones o amenazas) y las bases de datos con los posibles ataques. En las redes es necesario considerar el lugar de colocación del IDS ya sea antes o después de un ***cortafuego*** o ***Firewall*** **(**Que se mencionará en la sección de ***Implantación de Barreras de Protección en la Red*****).**

Al colocar un IDS después de un Firewall, (véase la Figura 2.1), el firewall funciona como una barrera que controla el flujo del tráfico entre los host, los sistemas de redes, y los dominios, siendo un filtro que examina cada paquete enviado hacia algún punto o nodo de la

misma red, con el objetivo de analizar si cumple con una serie de criterios establecidos previamente.

Dada esta colocación del IDS se facilita su desempeño puesto que el sistema cuenta con un filtro (***Firewall***) que anticipa posibles amenazas. Por otra parte se reduce así la cantidad de paquetes a procesar para el mismo sistema de detección de intrusos siéndole más fácil identificar y procesar el tráfico que sea no considerado como amenaza (flechas negras) o posibles amenazas o intrusiones (flechas rojas).

Figura 2.1: Ubicación de un IDS después de un Firewall.

Por otra parte si se colocará un IDS antes de un Firewall, el sistema para la detección de intrusos no contará con un filtro primario de paquetes y datos. En un ambiente real, un IDS que no cuente con un firewall previamente ubicado puede ser vulnerable ante ciertas amenazas o ataques debido a la cantidad de tráfico que viaja a través de la red (véase la Figura 2.2) *[15]*.

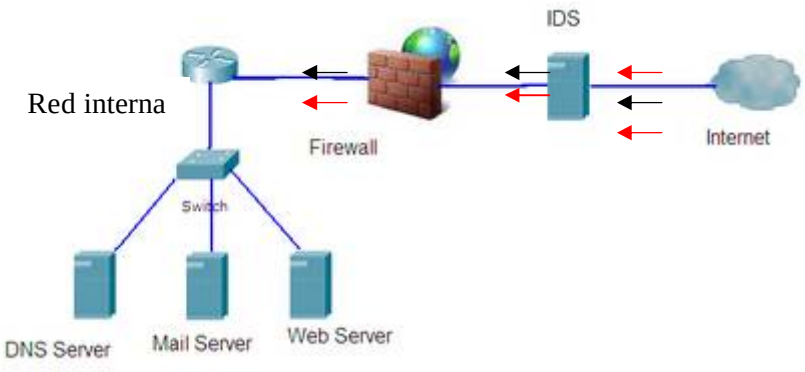

Figura 2.2: Ubicación de un IDS antes de un Firewall.

Debido a la diversidad de datos presentes en el tráfico de la red se deben considerar dos conceptos para el desarrollo e implementación de un sistema de seguridad:

- **Falso positivo:** Es la detección de datos o paquetes como una amenaza o intrusión cuando en realidad no se trata de algún intento de ataque sobre alguna red.
- **Falso negativo:** Este término hace énfasis en los paquetes o datos que son amenazas para una red pero que debido al constante procesamiento del tráfico, el sistema de seguridad no detecta dichas amenazas ocurriendo así las respectivas intrusiones o ataques.

El funcionamiento principal de un IDS es la detección oportuna de intrusos y ataques, este sistema debe ser programado en base a una serie de reglas y firmas conocidas como *Snort Rule*, las cuales contienen las características que le permiten distinguir entre el tráfico normal y aquél que puede ser considerado como posible amenaza para la red.

2.3 Snort Rule de un IDS

Snort Rule es código de seguridad que emplean los sistemas detectores de intrusos en las redes de comunicación, ofreciendo capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas. Logrando así la detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida *[29, 30]*.

Los IDS se implementan con un lenguaje para la creación de reglas flexibles y sencillas a través del *Snort* el cual monitorea en tiempo real lo que ocurre en la red en base al tráfico y en el que si un paquete coincide con algún patrón establecido en las reglas de configuración del IDS se hace un *log*. Así se sabe el momento, origen y cómo se produjo el ataque *[29]*.

El lenguaje usado por *Snort Rule* consiste en un conjunto de reglas establecidas y serán las que funcionen de guía para la escritura de las mismas, dentro de las cuales se tienen:

- La descripción de cada regla
- Cabecera

- Opciones

Cuando las reglas *Snort* (*Snort Rules*) son escritas de preferencia deben estar en una sola línea de lo contrario habrá que usar el carácter de *escape* (\) (véase la Figura 2.3).

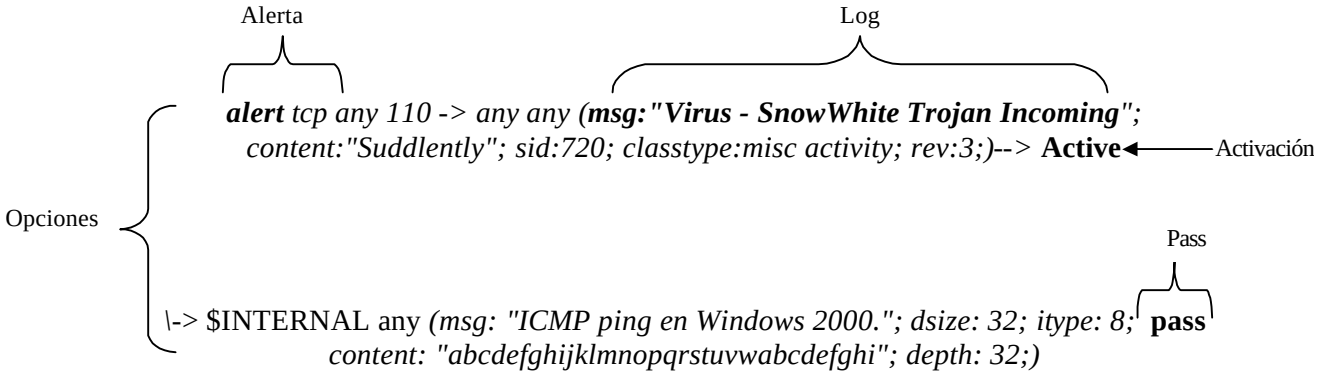

Figura 2.3: Estructura de una regla de Snort *[30]*.

Las reglas Snort se pueden dividir en dos secciones lógicas las cuales componen esencialmente su estructura siendo la cabecera de la regla y opciones:

- **Cabecera:** Contiene la acción de la regla, protocolo, direcciones IPs, máscaras de red, puertos origen y destino del paquete o dirección de la operación. Así mismo el encabezado contiene los siguientes valores.
    - **Alerta:** Este valor instruye a la regla de Snort a crear un campo de alerta y registro de los paquetes. Dicha instrucción se basará en el análisis de su encabezado.
    - **Log:** Este se caracteriza por ser un campo de registro de las amenazas detectadas por el sistema de seguridad. Este campo permite el alertamiento oportuno del IDS.
    - **Pass:** Se caracteriza por ser un campo en el que se describe el acceso a ciertas direcciones IP, como por ejemplo cuando algún usuario legítimo desea hacer uso de un servidor FTP privado.
    - **Activación (Active):** Una vez activadas las reglas de Snort no solo se realiza el alertamiento de la regla exclusiva de al amenaza detectada, si no también de las otras reglas para prevenir a tiempo otros posibles ataques.
    - **Dinámico:** Permite al sistema de seguridad realizar la captura dinámica de paquetes para realizar su análisis y así prevenir ataques o intrusiones.

- **Opciones:** Contiene los mensajes y la información necesaria para la decisión a tomar por parte de la alerta detectada *[29]*.

2.4 Implantación de las Barreras de Protección en la Red

El objetivo principal de una barrera de protección es proteger una red de otras. En general la red que se protege es propiedad de un usuario y la red contra la que se protegería a la red interna es la externa puesto que no puede confiarse en sus elementos y así mismo desde la cual puede violarse la seguridad de la red de interés.

La **Barrera de Protección** se puede definir como el instrumento principal para ejecutar la política de seguridad de red establecida. El término **Barrera de Protección** se define como un concepto para describir un amplio rango de funciones y la arquitectura de los dispositivos que protegen a la red, tales como programas de encriptación, enrutadores de selección, IDS, IPS o Firewalls *[10]*.

El funcionamiento que debe desempeñar una Barrera de Protección basa su operación en el modelo OSI (*Open System Interconnection*) puesto que es el medio para diferenciar la arquitectura de la comunicación y las funciones en una red, además de indicar que esta barrera puede trabajar en cualquiera de las capas del modelo siendo la barrera un punto de monitoreo del tráfico ya sea a nivel de capa de Aplicación o por otra parte operando en la capa de Red y Transporte, analizando los paquetes IP y TCP de los paquetes de entrada y de salida (véase la Figura 2.4).

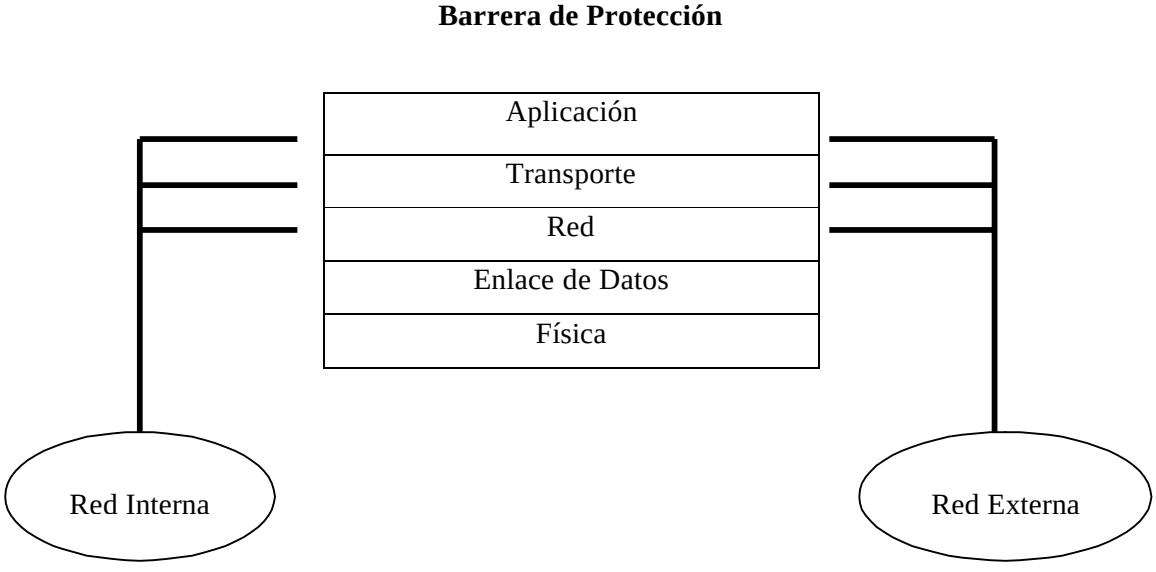

Figura 2.4: Operación de una Barrera de Protección *[10]*.

La Figura 2.4 muestra el modelo OSI en el que se señalan los niveles o capas sobre las cuales puede funcionar una barrera protección comunicándose la Red Interna y la Red Externa.

2.5 Firewall

Además de los IDS, existen otros elementos en una red de comunicación que funcionan como elementos para prevenir alguna intrusión o ataque, funcionando como filtros de datos o paquetes con el objetivo de hacer a un sistema de seguridad más eficiente.

Un Firewall es la parte de un sistema de seguridad en una red, diseñado para bloquear el acceso no autorizado. Se compone de uno o varios dispositivos configurados para permitir, limitar y descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas *[26, 27]*.

Un Firewall se implementa en hardware y software, utilizado para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet. Todos los mensajes que entren o salgan de la intranet pasan a través del Firewall, el cual tiene como función examinar cada mensaje y bloquear aquéllos que no cumplen los criterios de seguridad especificados (véase la Figura 2.5).

También es frecuente conectar el Firewall a una red interna llamada ***Zona desmilitarizada*** o ***DMZ (Desmilitarized Zone)***, en la que se ubican los servidores de la organización que deben permanecer accesibles a usuarios que sí puedan acceder a la red *[26, 27]*.

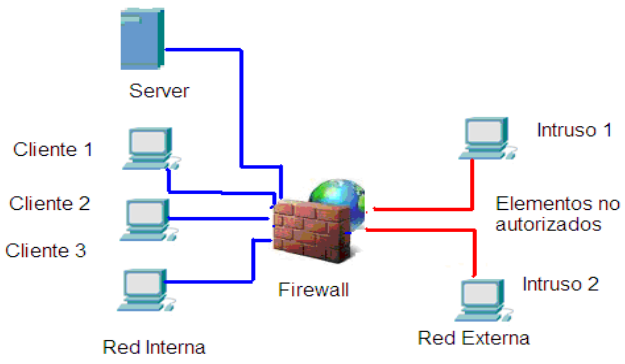

Figura 2.5: Esquema de una red de computadoras empleando un *Firewall* *[26]*.

Básicamente un Firewall se desempeña como un filtro de paquetes en el que se consideran los siguientes parámetros de análisis:

- Dirección IP fuente y destino de los paquetes que transiten por el Firewall.
- Análisis del puerto destino para los paquetes TCP/UDP[1].
- Generación de mensajes ICMP[2].
- Análisis de los paquetes SYN y ACK[3] *[26, 27]*.

Como se menciona anteriormente, el Firewall funciona como un elemento de seguridad que realiza el filtrado de cierto tráfico o paquetes para así proteger a una red de interés. Dada la cantidad de tráfico que transita a lo largo de una red de comunicaciones, pueden existir elementos en el mismo tráfico que pueden ser considerados como posibles amenazas para una red, y del otro lado puede haber elementos que sean amenazas y no ser considerados como tal, si no por el contrario como tráfico de clientes o usuarios legítimos por lo que se debe de considerar las políticas de seguridad que se deben emplear en una red.
Es por eso que el desempeño que tienen los Firewall hace que este bloque de seguridad pueda ser clasificado en dos clases:

- **Firewall de capa de red o de filtrado de paquetes**

Funciona a nivel capa de Red o capa 3 del modelo OSI como filtro de paquetes IP en el que se realizan filtrados según los distintos campos de los paquetes IP (dirección IP origen, dirección IP destino). A menudo en este tipo de cortafuegos (Firewall) se permiten filtrados según campos de nivel de Transporte (nivel 4) como el puerto origen y destino. Esta clase de firewall es uno de los principales tipos de cortafuegos pues se considera bastante eficaz *[27]*.

- **Firewall de capa de aplicación**

Trabaja en el nivel de aplicación o nivel 7 del modelo OSI, de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Un cortafuegos a nivel

[1] TCP/UDP: Transmission Control Protocol/User Datagram Protocol
[2] ICMP*: Internet Control Message Protocol*: Protocolo de control y notificación de errores del Protocolo de Internet (IP) *[13]*.
[3] SYN/ACK: SYN es un bit de control dentro del segmento TCP, se utiliza para sincronizar los números de secuencia iniciales ISN de una conexión. ACK es un mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes han llegado.

7 de tráfico HTTP suele denominarse *Proxy*, y permite que las computadoras u otros equipos de una red accedan a Internet de una forma controlada puesto ya que se oculta de manera eficaz las verdaderas direcciones de red, enmascarándolas *[27]*.

2.6 IPS (*Intruder Prevention System*)

Un IPS se define como un dispositivo que ejerce el control de acceso en una red para proteger a los sistemas o equipos de posibles ataques. Los IPS representan un desarrollo en los sistemas de seguridad ya que cuentan con la capacidad de tomar decisiones de control de acceso basado en los contenidos del tráfico como por ejemplo las direcciones IP fuente y destino o los puertos de acceso *[31]*.

En cuanto a su funcionamiento un IPS al igual que un Sistema para la Detección de Intrusos, funciona ante la detección de intrusos pero la diferencia es que el IDS alerta al administrador de la red ante la detección de un posible intruso, mientras que un Sistema de Prevención de Intrusos establece políticas de seguridad para proteger el equipo o la red de un ataque protegiendo de manera proactiva, es decir que alerta de manera anticipada la detección del ataque y un IDS protege reactivamente, lo que indica que éste último actúa en el momento de detectar el ataque *[31]*.

De la misma manera los IPS se clasifican en relación a la detección del tráfico malicioso:

• Detección Basada en Firmas

• Detección Basada en Políticas

• Detección Basada en Anomalías

- **Detección Basada en Firmas**

Esta detección se basa en una serie de reglas o firma establecida para reconocer a un determinado conjunto de posibles amenazas o ataques. Sin embargo como este tipo de detección funciona parecido a un Antivirus el administrador de la red debe verificar que las firmas estén constantemente actualizadas *[31]*.

- **Detección Basada en Políticas**

En este tipo de detección el IPS requiere que se declaren muy específicamente las políticas de seguridad. Por ejemplo determinar cuáles hosts pueden tener comunicación con determinadas redes. *[31]*

- **Detección Basada en Anomalías**

En este tipo de detección se establecen dos parámetros de funcionamiento:

1. **Detección Estadística de Anormalidades**: El IPS analiza el tráfico de red por un determinado periodo de tiempo y crea una línea base de comparación con el tráfico analizado en el que si el tráfico varía demasiado con respecto a la línea base de comportamiento se genera una alarma de manera automática.
2. **Detección No Estadística de Anormalidades**: En este tipo de detección el administrador de red es el elemento que define el patrón 'normal' de tráfico en función de reglas o políticas establecidas. Sin embargo debido a que con este enfoque no se realiza un análisis dinámico y real del uso de la red el sistema es susceptible a generar falsos positivos *[31]*.

2.7 Políticas de Seguridad en una Red

Las políticas de seguridad se pueden definir como una serie de reglas que reflejen seguridad en una red. Los objetivos de la política de seguridad de red son establecer instancias en un sistema de seguridad tales como en los Firewall o IDS para proteger redes y sistemas ante amenazas o intrusiones que afecten el desempeño de la red.

Los mecanismos de políticas de seguridad de red auxilian en la identificación y la prevención de daños del sistema causados por amenazas o ataques. Para establecer una política de seguridad para una red se deben tomar los siguientes puntos *[10]*.

- Confidencialidad
- Integridad (Mantener seguro los puntos de interés en la red)
- Autenticidad (Verificar la legitimidad de los clientes o usuarios)
- Disponibilidad de los recursos y de la información
- Control de Acceso (Analizar las direcciones de procedencia y destino para mantener un control de conexión de los usuarios)

- Auditoría (Realizar un registro que permita conocer la vulnerabilidad en seguridad con la que cuenta una red) *[15]*.

2.8 Discusión

En este capítulo se presentaron los distintos sistemas de seguridad que pueden ser implementados en una red informática, de la misma manera se definieron y mostraron las clasificaciones de estos sistemas de acuerdo al desempeño que presentan ante el tráfico en la red con el propósito de hacer un comparativo con los IDS. Cabe mencionar que tanto los Firewall, IPS e IDS mantienen una función específica en la red, siendo elementos que se complementan uno al otro enfocados en un objetivo común: mantener a la red lo más seguro posible ante amenazas o ataques que afecten el correcto funcionamiento de ella.