Apéndice C
Mecanismos de seguridad en red

I. Cifrado

1. Cifrado simétrico

Un esquema de cifrado tiene componentes básicos como texto claro, clave de cifrado, algoritmo de cifrado, clave secreta y texto cifrado.

- ***Texto claro*:** es el mensaje o los datos originales que se introducen en el algoritmo de cifrado como entrada.
- ***Algoritmo de cifrado*:** encargado de realizar las sustituciones y transposiciones en el texto claro.
- ***Clave secreta*;** es también una entrada del algoritmo, las sustituciones y transposiciones realizadas por el algoritmo dependen de ella.
- ***Texto cifrado*;** el mensaje ilegible que se produce como salida, depende del texto claro, la clave secreta y el algoritmo empleado, para un mismo texto en claro, dos claves diferentes producirán dos textos cifrados diferentes.

Un aspecto primordial al momento de implementar una solución criptográfica es contemplar el *criptoanálisis*, éste es el proceso por el cual se busca descubrir un texto claro o una clave de cifrado, la estrategia del criptoanalista depende de la naturaleza del esquema de cifrado y de la información disponible. La tabla C.1 resume los diferentes tipos de ataques criptoanalíticos basados en la cantidad de información que posee el criptoanalista.

Tabla C. 1 Comparación de funciones hash seguras.

Tipo de ataque	Información que tiene el criptoanalista
- Sólo texto cifrado.	-Algoritmo de cifrado. -Texto cifrado que se va a descifrar.
- Texto claro conocido.	-Algoritmo de cifrado. -Texto cifrado que se va a descifrar. -Uno o más pares de texto claro- texto cifrado formado con la contraseña secreta.
- Texto claro elegido.	-Algoritmo de cifrado. -Texto de cifrado que se va a decodificar. -Mensaje de texto en claro elegido por el criptoanalista junto con su correspondiente texto cifrado generado con la contraseña secreta.
- Texto cifrado elegido.	-Algoritmo de cifrado. -Texto cifrado que se va a descifrar. -Texto cifrado intencionado elegido por el criptoanalista con su correspondiente texto claro descifrado generado con la contraseña secreta.
-Texto elegido.	- Algoritmo de cifrado. -Texto cifrado que se va a descifrar. -Mensaje de texto claro elegido por el criptoanalista con su correspondiente texto cifrado generado con la contraseña secreta. -Texto cifrado intencionado elegido por el criptoanalista con su correspondiente texto claro generado con la contraseña secreta.

Un esquema de cifrado se dice es computacionalmente seguro, si el texto cifrado generado cumple con los dos o uno de los dos criterios siguientes:

- El costo de romper el cifrado excede el valor de la información cifrada.
- El tiempo necesario para romper el cifrado excede el tiempo de vida útil de la información.

El problema está en que es muy difícil estimar la cantidad de esfuerzos necesarios para realizar satisfactoriamente el criptoanálisis del texto cifrado, sin embargo, si no hay debilidades inherentes en el algoritmo, lo que procede es un enfoque de fuerza bruta.[46]

En el caso del cifrado simétrico en la tabla C.2 se muestran los cifrados más utilizados hasta la fecha, así como las características principales de cada uno de ellos.

Tabla C. 2 Algoritmos de cifrado simétrico convencionales.

Algoritmo	Tamaño de clave (bits)	Tamaño de bloque (bits)	Número de etapas	Aplicaciones
DES (1977)	56	64	16	SET, Kerberos.
3DES (1985)	112 o 168	64	48	Financial Key Management, PGP, S/MIME.
AES (1997)	128, 192, 256	128	10,12, 14	Destinado a sustituir DES y 3DES.
IDEA (1991)	128	64	8	PGP.
RC5 (1994)	Variable hasta 2048	64	Variable hasta 255	Varios paquetes de software.
BLOWFISH (1993)	Variable hasta 448	64	16	Varios paquetes de software.

Para que el cifrado simétrico funcione, las dos partes deben tener la misma clave o contraseña para un intercambio seguro y esa clave debe protegerse del acceso de otros, más aun, es deseable cambiar frecuentemente la clave para limitar la cantidad de datos comprometidos si un atacante la descubre. Por lo tanto, la robustez del sistema criptográfico depende de la técnica de distribución de claves, término que se refiere al mecanismo de entregar una clave a dos partes que deseen intercambiar datos, sin permitir que otros vean dicha clave, la distribución de claves se puede realizar por diferentes maneras para dos partes *A* y *B*.

- Una clave puede ser elegida por *A* y entregada físicamente a *B*.
- Una tercera parte puede elegir la clave, entregarla físicamente a *A* y a *B*.
- Si con anterioridad *A* y *B* han estado usando una clave, una parte podría transmitir la nueva clave a la otra cifrada, utilizando la antigua clave.
- Si *A* y *B* disponen de una conexión cifrada a una tercera parte *C*, *C* podría distribuir mediante los enlaces cifrados, una clave a *A* y a *B*.

[46] William Stallings, Fundamentos de Seguridad en Redes Aplicaciones y Estándares, Prentice Hall, 2da ed., 2005 pág 32

2. Cifrado asimétrico

También llamado criptografía de clave pública, permite brindar cifrado, intercambio de claves y firma digital. De igual importancia que la confidencialidad, como medida de seguridad, es la autenticación, la autenticación de mensaje por medio de firma digital garantiza que el mensaje proviene de las fuentes esperadas, además la autenticación puede incluir protección contra la modificación, el retraso, la repetición y el reordenamiento.

Un esquema de cifrado de clave pública tiene seis componentes básicos:

- ***Texto claro:*** es el mensaje o los datos originales que se introducen en el algoritmo de cifrado como entrada.
- ***Algoritmo de cifrado*****:** realiza diferentes transformaciones en el texto en claro.
- ***Clave pública y privada*****:** es una pareja de claves que han sido seleccionadas, de las cuales una se usa para el cifrado y otra para el descifrado, clave privada y pública respectivamente.
- ***Texto cifrado:*** el mensaje ilegible que se produce como salida depende del texto claro, la clave secreta y el algoritmo empleado, para un mismo texto en claro, dos claves diferentes producirán dos textos cifrados diferentes.
- ***Algoritmo de descifrado*****:** este algoritmo acepta el texto cifrado y la clave correspondientes para producir el texto claro original.
- ***Entidad certificadora*****:** ésta contiene la clave pública de todos los usuarios para que otros las usen con la finalidad de descifrar mensajes, mientras que la clave privada sólo es conocida por el propietario, es importante mencionar que este elemento es opcional pero altamente recomendado contemplarlo.

Los sistemas de clave pública se caracterizan por el uso de algoritmo criptográfico con dos claves, una no se revela y la otra sí, dependiendo de la aplicación, el emisor hace uso de su clave privada o la clave pública del receptor o las dos para realizar algún tipo de función criptográfica, en términos generales, se puede clasificar el uso de criptosistemas de clave pública en tres categorías:

- ***Cifrado/descifrado***: el emisor cifra un mensaje con la clave pública del receptor.
- ***Firma digital***: El emisor *firma* un mensaje con su clave privada, esto se consigue mediante un algoritmo criptográfico aplicado al mensaje o a un pequeño bloque de datos que es una función del mensaje.
- ***Intercambio de claves***: dos partes cooperan para intercambiar una clave de sesión. Hay distintas posibilidades que implican la clave privada de una o de las dos partes.

Algunos algoritmos son adecuados para las tres aplicaciones, mientras otros sólo se pueden emplear para una o dos de ellas. La tabla C.3 muestra algunos de los algoritmos que se emplean en el cifrado asimétrico o de clave pública.

Tabla C. 3 Aplicaciones para criptosistemas de clave pública.

Algoritmo	Cifrado /Descifrado	Firma digital	Intercambio de claves
RSA (1977)	Sí	Sí	Sí
ElGamal (1978)	Sí	Sí	Sí
Diffie-Hellman (1976)	No	No	Sí
DSS (1991)	No	Sí	No
Curva Elíptica-ECC(1985)	Sí	Sí	Sí

a) Firma digital

El cifrado de clave pública se puede utilizar para realizar firmas digitales como lo ilustra la figura C.1, éste se puede utilizar con cifrado o trabajar solo, en este caso A envía el mensaje aplicándole algún algoritmo que soporte firma digital con su clave privada a un usuario B, B podrá verificar el origen del archivo al llevar a cabo el descifrado con la clave pública de A, en este momento el cifrado sirve como firma digital, además de que es imposible alterar el mensaje sin la clave privada de A, así que el mensaje queda autenticado de origen y permite confirmar integridad.

En el caso del descifrado se cifra con la clave pública de la entidad a la que se desea enviar datos y el receptor descifra el mensaje con su clave privada, ya que es el único que conoce dicha clave, sólo él podrá descifrar, de esta manera se genera un canal seguro.

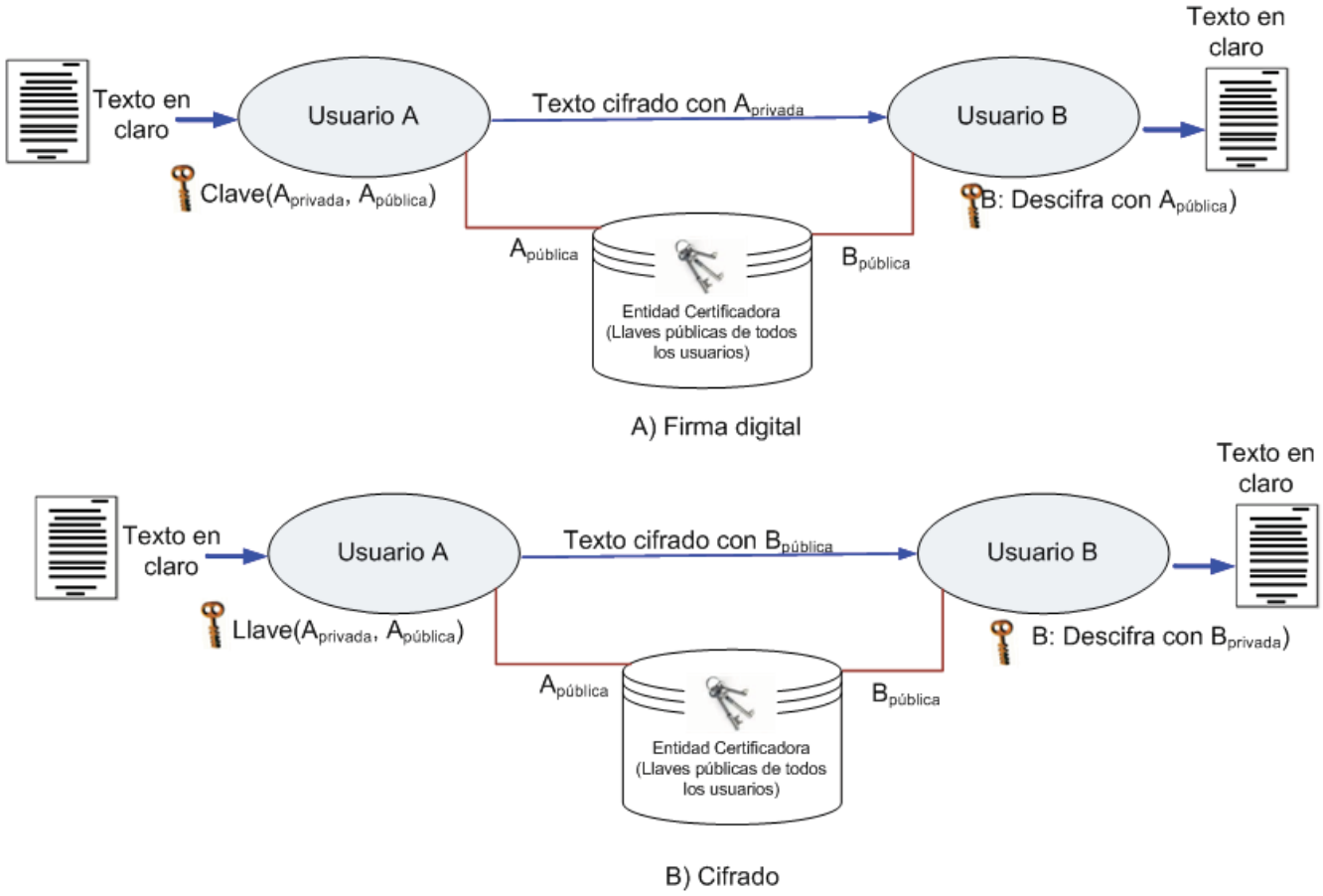

Figura C. 1 Cifrado criptografía de clave pública.

En el mundo real se firma un documento para autenticar que sólo el firmante legítimo puede producirlo, como es el caso de las identificaciones personales, pagos con tarjetas bancarias al utilizar terminales, entre otros, la analogía en el cómputo es la firma digital, en el caso de falsificación, una tercera parte interviene para juzgar la autenticidad en el mundo digital, esta función queda a cargo de las entidades certificadoras. Las características que ofrece una firma digital son autenticación, infalsificable, única para cada documento, inalterable y no repudiada, es decir, el firmante no puede negar la firma.

b) Entidades certificadoras

Adicional a estos dos funcionamientos mostrados en la figura C.1, el cifrado de clave pública trata el problema de distribución de claves y he aquí donde surge un gran problema, ya que la base de este tipo de cifrado establece que la clave pública es de carácter público, así, si hay un algoritmo de clave pública aceptado como RSA, cualquier participante puede enviar su clave pública a otro o difundir su clave a toda la comunidad en general. Aunque este enfoque es conveniente, se tiene la debilidad que cualquiera puede falsificar ese dato público, es decir, un usuario podría hacerse pasar por el usuario *A* y enviar su clave pública a otro participante o difundirla. Hasta el momento en que *A* descubre la falsificación y alerta a los otros participantes, el falsificador puede leer todos los mensajes cifrados enviados a *A* y puede usar las claves falsificadas para la autenticación.

La solución a este problema es el certificado de clave pública, este certificado consiste en una clave pública y un identificador o nombre de usuario del dueño de la clave, además de información como fecha de expiración, número de serie, firma digital del emisor, con todo el bloque firmado por una tercera parte confiable. Comúnmente la tercera parte es una autoridad certificadora (CA- Certificate Authority), en la que confía la comunidad de usuarios. Algunas CA de las más prestigiosas son las siguientes:

- Verysing (comercial). http://www.verisign.com/
- Verizonbusiness (comercial). http://www.verizonbusiness.com
- Darthseven system (comercial). http://darth7.supersite.myorderbox.com/
- PyCA(Solución libre). http://www.pyca.de/
- OpenCA (Solución libre). http://www.openca.org/
- Open source PKI Mozilla. http://www.mozilla.org/projects/security/pki/
- Bibliotecas criptográficas para java y C#. http://www.bouncycastle.org
- Sistema central propio.

El nivel de seguridad en la validación del certificado está limitado a la dificultad del impostor que relacione su clave pública con la identidad de otra persona, se podrá hacer pasar por otra persona y hacer actividades maliciosas, de cualquier manera el usuario deberá almacenar de forma segura su clave privada ya que en ella recae la seguridad.
Las autoridades certificadoras garantizan que sean infalsificables las claves públicas, ya que implementan los servicios de autenticación y no repudio, además de ser una forma segura de distribuir claves públicas en comunidades grandes como lo es Internet.

c) Funciones Hash

Utilizadas para obtener integridad en la transmisión de mensajes o datos almacenados, además de permitir detectar o prevenir alteraciones durante la transmisión, esta función se caracteriza por ser unidireccional, acepta un mensaje de tamaño variable M como entrada y produce un resumen del mensaje de tamaño fijo H(M) como salida, es importante saber que se produce una única cadena diferente a todas las demás para cada M.

La finalidad de una función hash es la de obtener una *huella* de un archivo, mensaje u otro bloque de datos para que resulte útil a la autenticación del mensaje, una función hash H debe poseer las siguientes propiedades:

I. H puede aplicarse a un bloque de datos de cualquier tamaño.
II. H produce una salida de tamaño fijo.
III. H(x) es relativamente fácil de computar para cualquier *x* dado, haciendo que tanto las implementaciones de hardware y software sean prácticas.
IV. Para cualquier valor *h* dado, es imposible desde el punto de vista computacional, encontrar *x* tal que H(x)=h, lo cual con frecuencia, se conoce en la literatura como propiedad unidireccional.
V. Para cualquier bloque dado x, es imposible desde el punto de vista computacional, encontrar con y≠ x que H(y)=H(x), lo que se conoce como colisiones si se presenta el caso.

Las cuatro primeras propiedades son requisito para la aplicación práctica, en el caso de la quinta propiedad existen algoritmos que presentan colisiones ya que diferentes mensajes producen el mismo valor hash. Una función hash que cumple con las primeras cuatro propiedades se conoce como función hash débil, si también posee la sexta propiedad se denomina función hash robusta, a continuación en la tabla C.4 se hace una comparación de las funciones hash seguras.

Tabla C. 4 Comparación de funciones hash seguras.

	MD5	SHA-1 (1994)	RIPEMD-160 (1996)
Longitud del resumen	128 bits	160 bits	160 bits
Unidad básica de procesamiento	512 bits	512 bits	512 bits
Número de pasos	64 (4 etapas de 16)	80 (4 etapas de 20)	160(5 pares de etapas de 16)
Tamaño máximo del mensaje	∞	264 -1 bit	∞

Existe una versión más reciente de SHA-1 denominada SHA2, ésta genera cadenas de 512 bits, existen variantes de SHA-1 con cadenas de resumen con una longitud de 224, 256 y 384, adicional a estos algoritmos existen otros como N-Hash de 128 bits, Snefru 128 y 256 bits, Tiger hasta 192 bits optimizado para máquinas de 64 bits, Haval hasta 256 bits.

La ventaja que tienen estos enfoques es que sólo se cifra un fragmento del mensaje para generar la función hash, lo que significa un costo computacional menor, pero sólo garantiza integridad, por esta razón se contemplaron los algoritmos como MD5, SHA-1 y RIPEMD.

Las funciones hash tienen varios usos dentro de los más comunes se encuentran:

- ***Hash de contraseñas***: como método de almacenamiento de contraseñas.
- ***Integridad de archivos***: utilizando la cadena que produce cada archivo digital con algún algoritmo en particular.
- ***Huella digital:*** de mensajes enviados y eficiencia en firmas digitales.

II. Topologías, Filosofías y tipos de filtrado de Firewalls

Cuando se desea implementar un firewall para protegerse de ciertos tipos de ataques, entra en juego otra decisión muy importante como la ubicación correcta que debería tener un firewall dentro de la red, bajo este principio se han diseñado distintas topologías de acuerdo con las necesidades y el grado de seguridad que se desee tener, se entiende por topología como la ubicación física que éste tendrá dentro de una red, cabe mencionar que las topologías o distribución de firewalls implican costos dentro de la implementación.

Se utilizan tres modelos, aunque éstos son flexibles y pueden ser modificados de acuerdo con las necesidades, además de que es posible combinar las distintas arquitecturas y tipos de filtrado.

a) Multi-homed host: equipo conectado a múltiples redes, el equipo cuenta con más de una tarjeta de red con la cual se puede conectar física y lógicamente con distintos segmentos de red, sin embargo, existe una variante de esta topología conocido como dual host-equipo con dos tarjetas de red.
b) Dual homed firewall: es un firewall con dos tarjetas de red, cada una conectada a distintas redes, por lo general se conecta una red segura (interna) contra otra red insegura (externa), por lo que todo el tráfico proveniente de una red insegura es filtrada antes de pasar a la red segura, en este caso el firewall actúa en la mayoría de los casos como un intermediario entre ambas redes, en la figura C.2 se puede observar dicha topología.

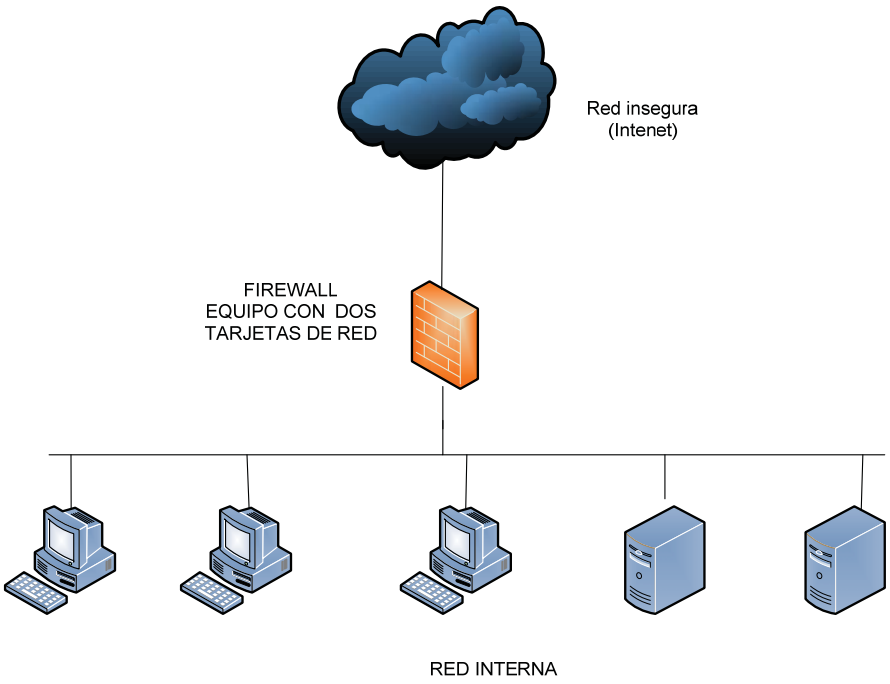

Figura C. 2 Firewall con dos interfaces de red.

La desventaja de esta arquitectura se debe a que si un atacante consigue comprometer cualquiera de los servidores que se encuentre detrás de este punto único, los otros equipos, podrán ser atacados sin ninguna restricción desde el equipo que acaba de ser comprometido.

c) Screened host*:* topología de firewall, hace uso de un equipo llamado bastión host- equipo donde se instala el software necesario para que éste pueda retener los ataques provenientes de internet, en este modelo la conexión de las redes se realiza con el apoyo de un router configurado para bloquear todo el tráfico entre la red externa y los hosts de la red interna excluyendo el equipo bastión host, este tipo de arquitectura permite soportar servicios proxy en bastión host, así como filtrado de paquetes en el router.

En la forma de operar todas las conexiones provenientes de la red insegura son re direccionadas por el router al bastión host y de ahí a los equipos de la red interna, evitando de esta manera una conexión directa con la red externa.

La debilidad de esta configuración es que si el bastión host es comprometido, existe libertad para tener acceso a cualquier host ya que no existe ningún mecanismo entre el bastión host y los equipos de la red interna, esta topología se puede observar en la figura C.3.

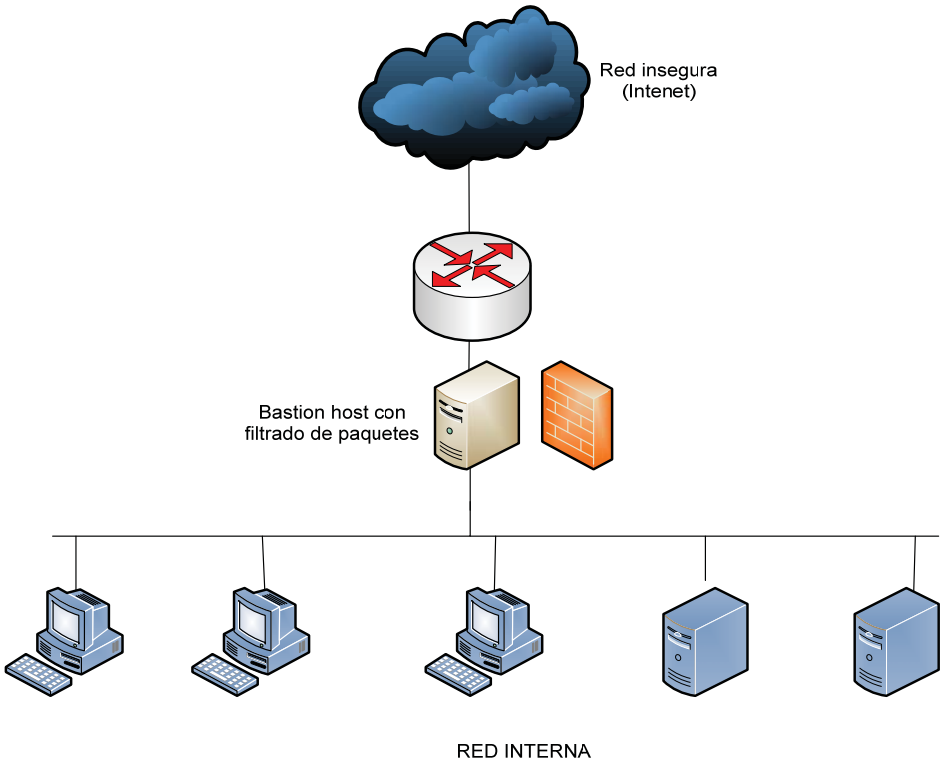

Figura C. 3 Screened host firewall.

d) Screened subset: En una arquitectura screened subnet, se agrega una red en la zona de bastión host, esta red es llamada red perimetral, se encuentra separada de la red interna, también es denominada Demilitarized Zone- Zona desmilitarizada(DMZ).

Los routers se configuran, mediante reglas de filtrado para que tanto los nodos de la red interna como los de la externa sólo puedan comunicarse con nodos de la red del perímetro. Esto permite a la red interna ser invisible a la externa.

En este esquema por lo general se utilizan dos routers: uno exterior y otro interior. El router exterior tiene la misión de bloquear el tráfico no deseado en ambos sentidos: hacia la red interna y hacia la

red externa. El Router interior hace lo mismo con la red interna y la DMZ (zona entre el Router externo y el interno) (figura C.4).

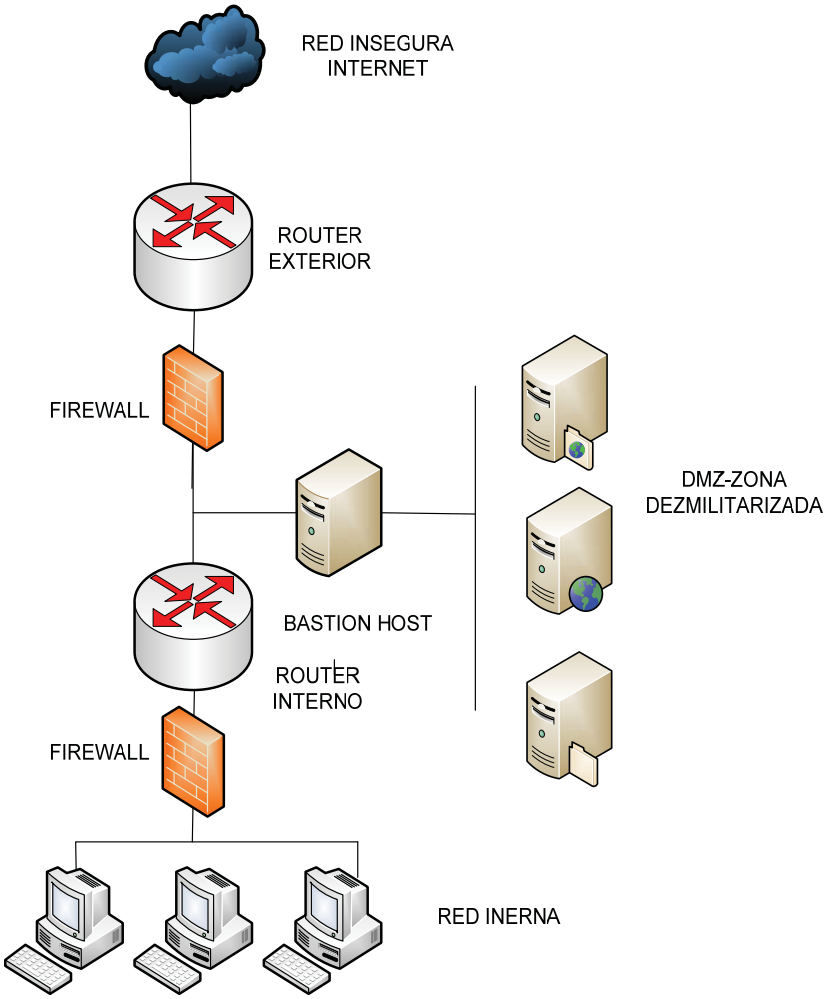

Figura C. 4 Screened subnet firewall.

Filosofía de firewall

El concepto de filosofías de firewall está relacionado directamente con la forma de establecer las reglas dentro del firewall, para permitir o negar el flujo de datos desde una red insegura a otra segura o viceversa. Se manejan dos filosofías.

La primera filosofía es bloquear todo el tráfico que no se desea permitir ingresar a la red o aquel que desea salir, esta filosofía es denominada permisiva, sin embargo, ésta resulta bastante peligrosa, ya que si se consideran los 65535 puertos disponibles para los protocolos TCP, UDP, establecer reglas para las distintas aplicaciones resultaría complicado y con ello el nivel de seguridad disminuye.

Por otro lado, la filosofía prohibitiva consiste en negar todo el tráfico entrante o saliente a excepción de aquel que se encuentra estrictamente permitido, con esta filosofía el control del flujo de datos de una red a otra se torna mucho más sencilla, es la filosofía más utilizada, además de que por default es una regla establecida por la mayoría de firewalls.

Tipos de Filtrado

Implementar un firewall implica un análisis del tipo de tráfico a bloquear, para ello se cuenta con una clasificación de configuración, de acuerdo con el tipo de filtrado que éstos son capaces de realizar, el nivel de seguridad dependerá directamente de los objetivos de la institución.

Se clasifican principalmente en los siguientes tipos:

- Filtrado de paquetes.
  - Estático.
  - Dinámico.
  - Estado.
- Gateways de aplicación.
- Filtrado híbrido.

Cada uno de ellos garantiza un nivel de seguridad, y desde luego cada uno implica un costo, en tabla C.5, se muestra a grandes rasgos el nivel de seguridad, que cada uno ofrece así como instituciones que pueden implementarlos.

Tabla C. 5 Uso y Nivel de Seguridad de Firewall.

Tipo de Firewall	Nivel de Seguridad Alto Ambiente (Hospital)	Nivel de Seguridad Medio Ambiente (Universidad)	Nivel de Seguridad Bajo Ambiente (Negocios pequeños)
Filtrado de paquetes	0	1	4
Gateway de aplicación conocido como proxy	3	4	2
Gateways híbridos	4	3	2

Nota: el número 4 indica que es recomendable utilizarlo, 3 se considera una solución efectiva, 2 aceptable, 1 no recomendable y 0 no aceptable, en la actualidad la implementación de uno u otro tipo de firewall depende directamente de los objetivos de la institución, por lo que la elección requiere de un previo análisis de los recursos a proteger.

a) Filtrado de paquetes

Este tipo de filtrado conocido también como firewalls de primera generación, son los más simples y sencillos comparados con los firewalls actuales, sin embargo, esto no quiere decir que son obsoletos, las reglas que permiten o niegan el paso de paquetes basadas en la dirección destino u origen y puertos ofrecen un nivel de seguridad mínimo, son un tipo de firewall apropiado si la seguridad que se requiere es mínima.

El firewall de filtrado de paquetes realiza la transmisión con base en el contenido de la cabecera IP, UDP o TCP. Aplicando reglas a la entrada o salida de las interfaces de red. Las reglas de filtrado se encargan de determinar si a un paquete le está permitido pasar de la parte interna de la red a la parte externa y viceversa, verificando el tráfico de paquetes legítimo entre ambas partes.

Este tipo de firewall se basa en la información que el paquete IP contiene en su cabecera para permitir o negar el tráfico de datos a través de la red, el tipo de información contenida en la cabecera es dirección destino, dirección origen, así como el estado de fragmentación del paquete. La cabecera TCP contiene información acerca del estado de la conexión, puerto origen y destino, dicha información permite determinar el tipo de aplicación que envía información, así como el host destino. En la figura C.5 se muestra un esquema de este tipo.

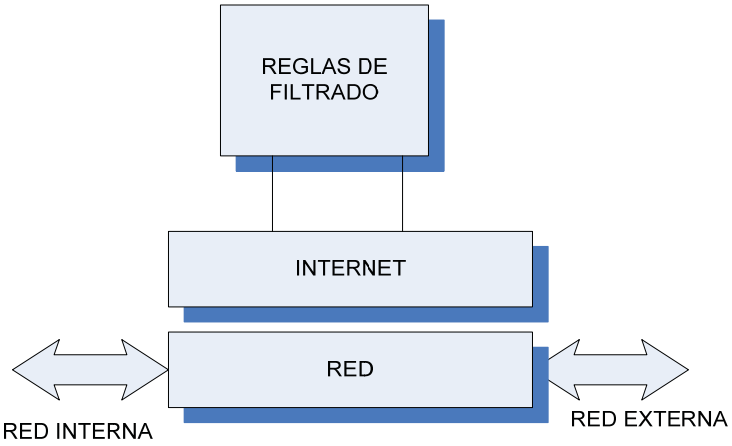

Figura C. 5 Filtrado de paquetes.

Cabe mencionar que las reglas establecidas pueden ser de manera jerárquica bajo una política por defecto de negar todo o aceptarlo todo, se debe tener especial cuidado en el diseño de las mismas ya que una mala configuración estaría dejando una puerta de entrada para el intruso.

Algunos tipos de filtrado comunes son:

- Con base en la dirección destino o fuente.
- Tipos de indicadores con algunas banderas.
- Contenido del paquete.
- Tamaño del paquete.
- Puertos de origen y de destino.

El hecho de negar todo generalmente se recomienda establecer como la última regla, después de colocar arriba de ella sólo las permitidas, este tipo de firewalls sólo es considerado una primera línea de defensa ya que por naturaleza del mismo no es posible prevenir ataques del tipo IP spoofing, DNS spoofing. La autenticación robusta no es soportada por algunos gateways que utilizan el filtrado de paquetes.

Entre las ventajas que ofrece este tipo de firewalls es de gran utilidad para redes con una carga de tráfico elevada, esta tecnología permite la implantación de la mayor parte de las políticas de seguridad necesarias.

b) Filtrado de paquetes por estado

El filtrado por estado es un tipo de firewall más avanzado, ya que analiza los paquetes con mayor detalle, provee un alto grado seguridad en comparación con los firewalls de primera generación

(filtrado de paquetes), en este tipo de firewalls los protocolos de Internet TCP, UDP son analizados con mayor profundidad, así como los servicios FTP, mail, web, telnet, entre otros, además de aplicaciones de negocios como RPC, SQL a través de un constante monitoreo y evaluación del estado y progreso para cada conexión o transacción, entre las ventajas que este tipo de firewalls ofrece, se encuentra la mayor precisión en el filtrado ya que analiza el payload –carga útil de un paquete, permite determinar cuántas conexiones simultáneas puede aceptar, inspección de filtrado por estado, sin embargo, también presenta desventajas ya que requiere mayor procesamiento.

Los estados de conexión son vigilados de principio a fin, cuando un paquete llega al firewall se verifica que éste sea parte de la conexión para permitir el paso o de lo contrario se descarta.

En la tabla C.6 se muestran los estados de una conexión.

Tabla C. 6 Estados de una conexión.

Estado	Significado
ESTABLISHED	Conexión establecida.
SYN_SENT	Intentando establecer una conexión.
SYN_RECV	Petición de conexión recibida.
FIN_WAIT1	El socket está cerrado y la conexión finalizando.
FIN_WAIT2	La conexión está cerrada, y el socket está esperando que finalice la conexión.
CLOSED	El socket está esperando después de cerrarse.
CLOSE_WAIT	El socket no está siendo usado.
LAST_ACK	La conexión remota ha finalizado y se espera que se cierre el socket.
LISTEN	El socket está esperando posibles conexiones entrantes.
CLOSING	Ambos sockets han finalizado pero aún no fueron enviados todos los datos.
UNKNOWN	El estado del socket se conoce.

En el momento que se establece la conexión se está verificando constantemente el estado de la misma, e incluso es posible eliminar una conexión si durante un periodo de tiempo no se observa comunicación.

c) **Gateway de aplicación.**

En este tipo de firewall, conocido como Gateway de aplicación o como servidor intermediario, los paquetes son analizados a nivel de aplicación, por lo que cuando un usuario desea comunicarse deberá pasar a través de este servidor, el cual funciona como un proxy-servidor intermediario asociado a una o más aplicaciones.

El servidor *proxy* se encargará de realizar las conexiones solicitadas con el exterior y cuando reciba una respuesta la retransmitirá al equipo que había iniciado la conexión, por lo que éste determina si acepta o rechaza una petición de conexión, para los usuarios este proceso es transparente como se puede observar en la figura C.6.

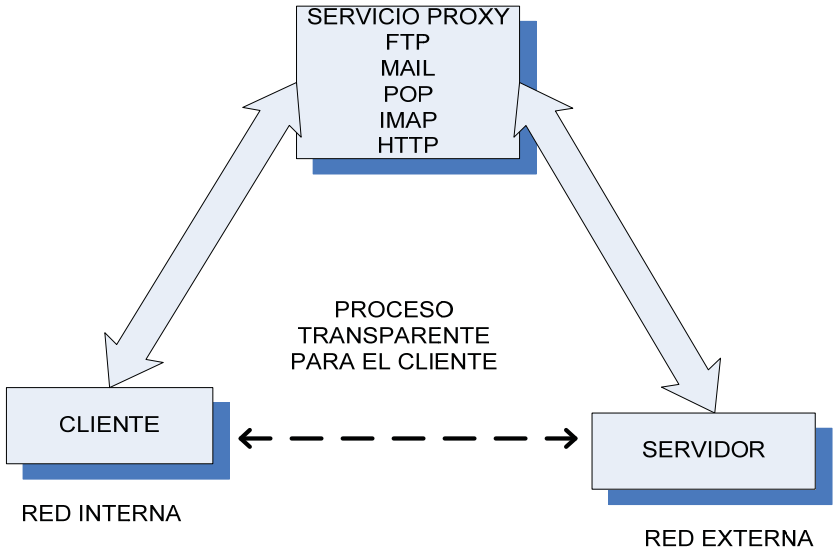

Figura C. 6 Firewall de aplicación.

Una de las desventajas de este tipo de firewalls es que requieren de un procesamiento mayor, debido a que atienden a un gran número de peticiones y analiza todo el contenido de cada paquete, a cambio de mayor seguridad ya que sólo los servicios para las cuales hay un servidor proxy, se les permite el acceso, por lo que si se compara con un firewall de filtrado de paquetes éste resulta ser menos eficiente, en la práctica se suele utilizar ambos tipos.

Otros tipos de firewall

a) Firewalls comerciales

Los firewalls también se clasifican en firewalls comerciales y de distribución libre, los firewalls comerciales pueden ser appliance o de software, dichos dispositivos basados en software o como una combinación de hardware y software cuya finalidad básica es bloquear el tráfico de datos desde una red segura a otra insegura o viceversa.

Algunas de las ventajas de estos dispositivos son:

- Facilidad de implementación.
- Ofrecen una administración más sencilla.
- Definen reglas utilizadas en el mercado.
- Actualizaciones constantes.
- Posibilidad de crecimiento y comunicación con otros dispositivos de monitoreo.
- Ofrecen un alto procesamiento, lo que los hace eficientes.
- Soporte.

Desventajas:

- Presentan un alto costo.
- Aunque presentan facilidad de comunicación con otros dispositivos, en su mayoría deben ser de la misma marca.
- Ofrecen menos flexibilidad en cuanto a necesidades se refiere.

Existen en el mercado diversas compañías encargadas de producir estos firewalls como son CISCO, 3com, Juniper, Cyberoam, Endian, Barracuda Networks, WatchGuard, Fortinet, Check Point, ZyXEL, entre muchos otros, cada uno tratando de ofrecer más características con la finalidad de obtener el beneficio de compra, en la figura C.7 se muestra un diagrama de un firewall basado en hardware.

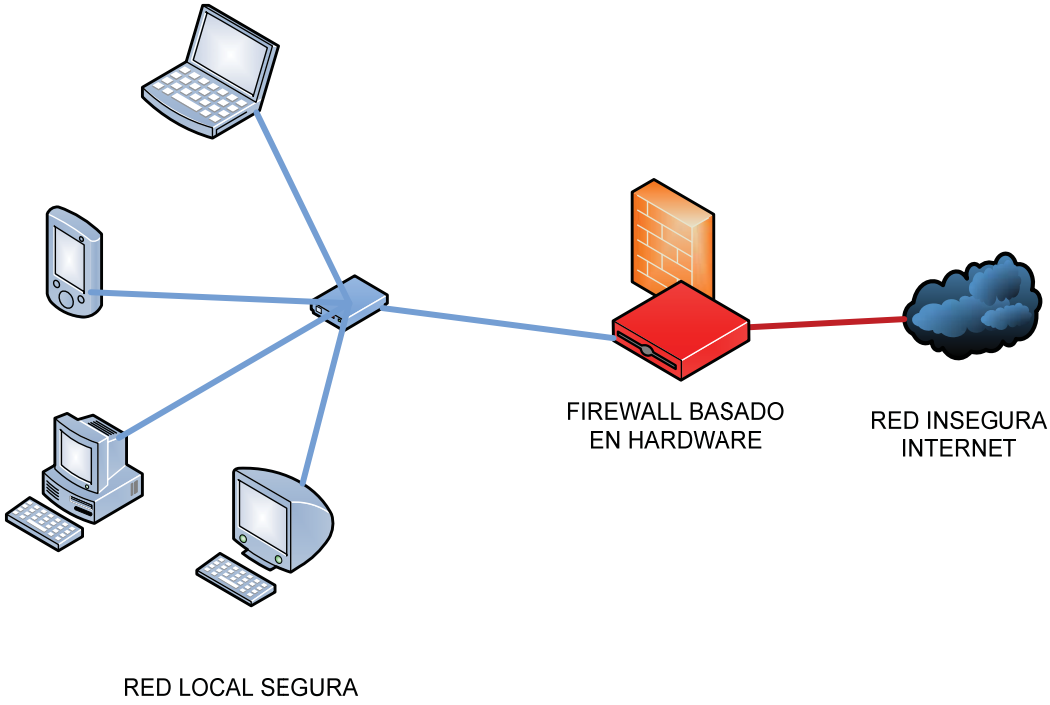

Figura C. 7 Firewall basado en hardware.

b) Firewall por software

Los firewalls basados en software existen en sus versiones comerciales y libres, en el caso de los comerciales ofrecen cierta facilidad de implementación, los costos no simpre son menores comparados con appliance – hardware de propósito dedicado, algunos ejemplos son Microsoft ISA server, Microsoft ForeFront, otros de distribución libre de UNIX emplean iptables y pf, éstos últimos ofrecen flexibilidad para su implementación ya que se adaptan fácilmente a las necesidades, aunque su implementación requiere invertir más tiempo y monitoreo constante, además de no brindar soporte en tiempo real.

III. Tipos de detectores de intrusos

Tipos de IDS

De acuerdo con la funcionalidad de los sistemas detectores de intrusos, se clasifican en tres categorías principales, detector de intrusos para un solo equipo llamado HIDS, detector de intrusos para una red (NIDS), y el sistema detector de intrusos distribuido (DIDS).

- Sistema detector de intrusos de red - Network Based Intrusion Detection System (NIDS).
- Sistema detector de intrusos para un equipo Host-Based Intrusion Detection System (HIDS).

- Sistema detector de intrusos distribuido Distributed Intrusion Detection System (DIDS).

La utilidad de cada uno depende del tipo de actividad a monitorear, finalmente en la práctica se utiliza una combinación de HIDS y NIDS.

a) Host IDS

El sistema detector de intrusos de un equipo, opera a nivel local, analizando eventos y bitácoras de un solo equipo, lanzando una alerta si detecta comportamientos extraños, el hecho de que la tarjeta de red no opere en modo promiscuo ofrece ventajas en cuanto a recursos de equipo se refiere, ya que disminuye la carga de trabajo. Otra de las ventajas que se tienen al implementar un HIDS es la facilidad de implementación de las reglas ya que sólo es necesario tener las reglas específicas para cada servicio con el que se cuente.

Si alguna institución cuenta con servidores de correo, web y se instala un HIDS para cada servidor, las reglas se personalizan de acuerdo con el tipo de ataques a los que cada servidor está propenso, de esta manera se están protegiendo servicios críticos y sólo será necesario actualizar de manera constante las reglas dependiendo de las nuevas vulnerabilidades que surjan, y las necesidades propias de cada organización.

Sin embargo, los HIDS pueden ser instalados en cualquier equipo que se desee monitorear, en la figura C.8 se muestra este tipo de IDS.

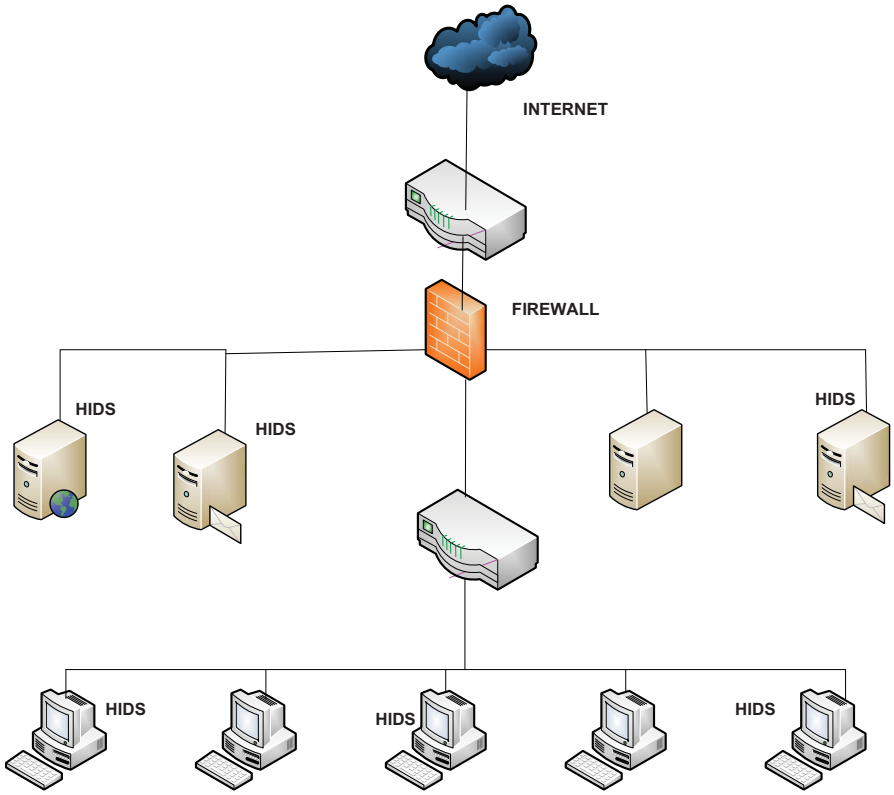

Figura C. 8 IDS.

En la tabla C.7 se resumen algunos HIDS actualmente utilizados.

Tabla C. 7 HIDS.

Nombre	Sistema operativo	Comercial	Código Abierto	Características principales
Open Source Tripwire 2.x	GNU /Linux	Sí		Verifica integridad de los archivos. Una licencia por equipo. Soporte sólo por la comunidad
Tripwire Enterprise 7.x	Solaris/SPARC, Solaris/x86, AIX, HP-UX Red Hat, SUSE, CentOS and Fedora Core 2	Sí	NO	Analiza cambios en los sistemas de archivos y propiedades del sistema, administración centralizada, las reglas pueden ser aplicadas a distintos dispositivos, soporte por Tripwire.
Tripwire for Servers 4.x	Solaris/SPARC, AIX, HP-UX, FreeBSD Red Hat, SUSE, TurboLinux	Sí	NO	Analiza cambios en los sistemas de archivos y propiedades del mismo. Genera reportes de manera gráfica. Soporte por Tripwire.
SNORT	Windows/Linux/ OpenBSD		Sí	Sistema detector de intrusos de código abierto. Capaz de analizar paquete en tiempo real. Es posible configurarlo de tres maneras distintas snnifer, IDS y como analizador de bitácoras.

b) Network IDS

NIDS este un tipo de sistema detector de intrusos encargado de monitorear toda una red, es decir, que actúa sobre todo un segmento de red, generalmente una tarjeta de red no está configurada en modo promiscuo, por lo que sólo puede ver el tráfico dirigido a ella, sin embargo, si se desea analizar todo el tráfico sin importar el destinatario, es necesario configurar la tarjeta de red en modo promiscuo, NIDS opera en modo promiscuo para monitorear todo el tráfico del segmento tanto el que entra como el que sale e incluso el tráfico local.

Aunque es una de las arquitecturas más utilizadas, demanda un alto procesamiento de recursos, de igual manera que los firewalls, es posible contar con la cantidad de NIDS que se deseen dependiendo de la estrategia de seguridad o necesidades, por otro lado, cabe mencionar que el análisis de los paquetes que circulan por la red debe de ser tratado con especial cuidado para evitar un mal uso, en la figura C.9 se muestra una arquitectura NIDS.

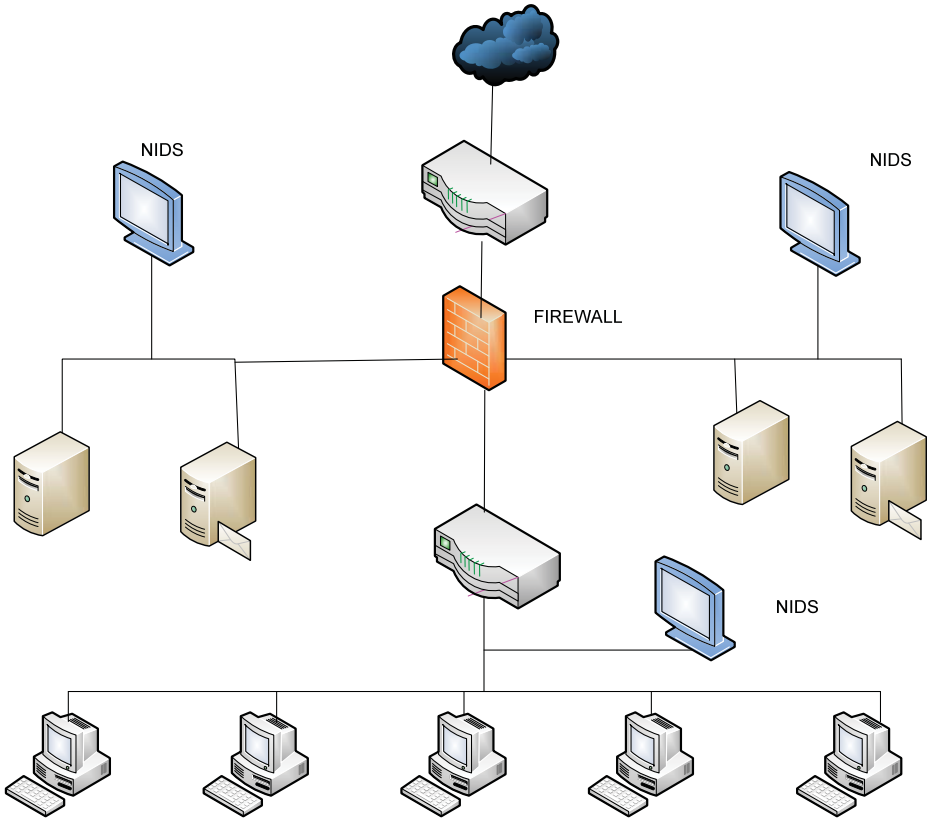

Figura C. 9 NIDS.

En la figura C.9 se observa que existen varios NIDS que se encargan de monitorear la red, éste es un ejemplo de arquitectura de seguridad en profundidad.

c) DIDS network

Los DIDS son otra variante de los sistemas detectores de intrusos, para esta arquitectura se cuenta con una estación central encargada de administrar los sistemas detectores remotos, lo cual permite una administración centralizada, la estación es la encargada de administrar bitácoras de los ataques de manera continua, las reglas de cada sistema se encuentran centralizadas y sólo si es necesario, las reglas son adaptadas para cada dispositivo en particular.

Cuando existe una alerta lanzada por alguno de los sistemas detectores, ésta es enviada a la estación de administración, la información es utilizada para notificar a los administradores de cada IDS.

Los DIDS pueden estar formados por HIDS, NIDS o una combinación de los dos, también pueden estar configurados en modo promiscuo, lo único que se requiere es que cada HIDS o NIDS envíe reportes a la estación de administración.

La comunicación entre los sensores y la base encargada de la administración se puede implementar a través de VPN's, utilizando la infraestructura existente.

En la figura C.10 se muestra un esquema de arquitectura DIDS.

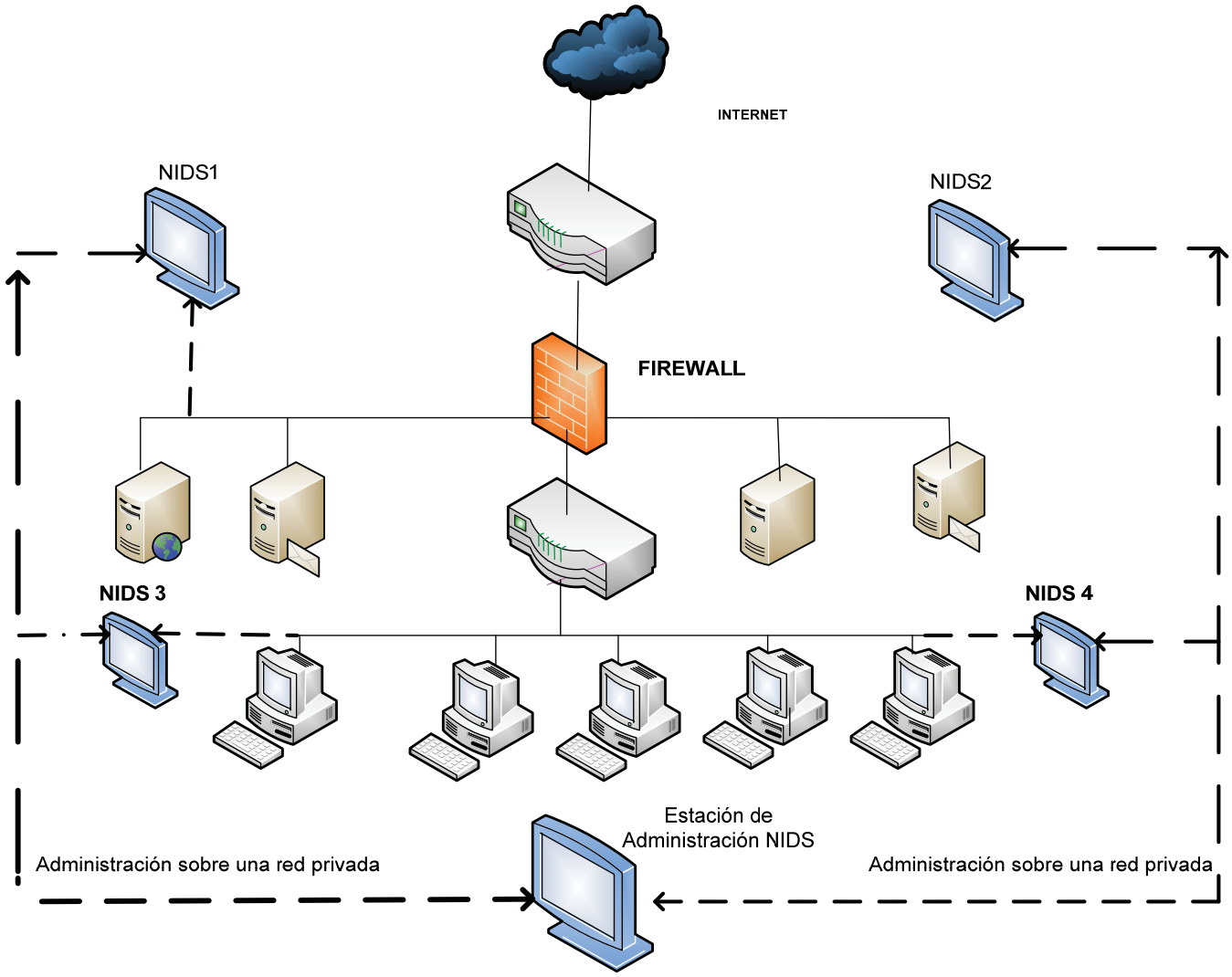

Figura C. 10 DIDS.

Los IDS pueden clasificarse también en:

a) IDS comerciales

Dentro de la clasificación de sistemas detectores de intrusos existen IDS comerciales y aquellos que son de código abierto.

Actualmente existe una gran cantidad de empresas que se dedican a producir IDS comerciales entre los que se encuentran CISCO, check point, Fortinet, IDS sourcefire, Dragon IDS, IDS Center.

b) IDS por software

De acuerdo con una de las clasificaciones de sistemas detectores de intrusos pueden estar basados sólo en software o una combinación de software y hardware, los IDS que se basan en software

deben instalarse en el equipo que se desea monitorear o en equipos dependiendo de si éstos son es un HIDS o NIDS.

Para la implementación de los distintos IDS que existen en el mercado se requiere de una cuidadoso análisis de los requerimientos de cada uno, ya que muchos de ellos dependen de otras herramientas además del tipo de sistema operativo para un adecuado funcionamiento, por lo que es conveniente contar con la documentación.

En la tabla C.8 se muestra un resumen de IDS basados en software.

Tabla C. 8 IDS por software.

Nombre	Comercial	Libre	Tipo
Snort		Sí	NIDS
Tripwire	Sí	Sí	HIDS
IDS center			NIDS, IPS
Cisco	Sí		NIDS
Nagios		Sí	HIDS
ELM			
DRAGON SQUIRE			HIDS
INTERNET SECURITY SYSTEMS	Sí		HIDS ,NIDS
DRAGON CENSOR	Sí		NIDS
SNARE	Sí		NIDS

Sistemas encargados de prevenir intrusiones (IPS)

Intrusión Prevention System- Sistemas encargados de prevenir intrusiones, cuando surgieron los primeros sistemas detectores de intrusos, las tareas que éstos realizaban eran simples, sin embargo, se han desarrollado sistemas que no únicamente lanzan alertas de posibles anomalías, debido a que los ataques cada día son más sofisticados, surge la necesidad inherente de evadir ataques en tiempo real con el uso de sistemas detectores que no sólo lancen alertas sino que además tengan la capacidad de responder a los ataques.

Un IPS opera de la siguiente manera, cuando se detecta un ataque la comunicación entre el intruso y el equipo comprometido, es bloqueada, se eliminan procesos que sean sospechosos o que intenten provocar un desbordamiento de memoria, se bloquea en el router o firewall el puerto o dirección IP del atacante para evitar ataques futuros.

Sin embargo, se debe tener especial cuidado en el manejo de un IPS ya que existen riesgos como el hecho de que un atacante pueda buscar nuevas alternativas para evadir su detección haciendo uso de

herramientas de escaneo pasivo que le permitan determinar nuevos caminos e incluso cabe la posibilidad de estar bloqueando tráfico legítimo.

Los conocidos falsos positivos permiten que un IPS realice un bloqueo tráfico legítimo, por lo que conocer el comportamiento normal de la red es recomendable para evitar problemas de bloqueo, aunque esto no es una regla conveniente para realizar pruebas de estrés que permitan analizar si el IPS bloquea tráfico legítimo.

Cabe mencionar que los sistemas detectores de intrusos han permitido investigar nuevas técnicas para detectar y mitigar ataques. Desde hace ya varios años se han desarrollado y buscado nuevas técnica que han permitido a los sistemas detectores de intrusos ser mucho más eficientes y sofisticados, entre algunas de esas técnicas se encuentra el uso de métodos distribuidos para la detección de intrusiones, detección de intrusiones basada en grafos, entre otras muchas más.