ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

UNIDAD PROFESIONAL CULHUACAN

SEMINARIO DE TITULACION

"DISEÑO E IMPLEMENTACION DE UN FIREWALL ASA 5520"

Presentan:

Bárcena Borja Neffi.
Díaz Espíndola Miguel.
Gómez Hinojosa César Oswaldo.
González Hernández Carlos Alberto.

DIRECTOR DEL SEMINARIO.

M. en. C. RAYMUNDO SANTANA ALQUICIRA.

MÉXICO D. F. NOVIEMBRE DEL 2009

INDICE.

Objetivo. I
Alcance. I
Justificación. I

CAPITULO I INTRODUCCION A LAS REDES.

1.1 ¿Que es una red? 1
1.1.1 Tipos de redes. 1
1.1.2 Topología de redes. 5
1.1.3 Protocolos de redes. 7
1.1.4 Redes móviles. 15

1.2 Internet. 15
1.2.1 Internetwork. 15
1.2.2 Arquitectura de Internet. 16
1.2.3 Direcciones IP. 18

1.3 Intranet y Extranet. 18

1.4 Modelo OSI. 21
1.4.1 Modelo de referencia. 21
1.4.2 Propósito del modelo OSI. 22
1.4.3 Las 7 capas del modelo OSI. 22

1.5 Modelo TCP/IP. 25
1.5.1 Modelo de referencia TCP/IP. 25
1.5.2 Las capas del modelo TCP/IP. 26
1.5.3 Comparación del modelo OSI con el modelo TCP/IP. 27

CAPITULO II TCP/IP.

2.1 ¿Qué es TCP/IP? 29
2.1.1 Arquitectura de TCP/IP. 32
2.1.2 Capa de acceso a red. 35
2.1.3 ¿Cómo funciona ARP? 36
2.1.4 Red de conmutación de paquetes. 37

CAPITULO III SEGURIDAD DE REDES.

3.1 Tipo de amenazas a la integración de las redes. 40
3.1.1 Tipos de ataques. 41
3.1.2 Ataques de reconocimiento. 41
3.1.3 Ataques de negación. 41
3.1.4 Hackers. 42

3.2 Soluciones. 42
3.2.1 Filtro de paquetes. 42
3.2.2 Filtro de Proxy. 44
3.2.3 Filtro de paquetes con estado. 46
3.2.4 VPN. 46
3.2.5 Firewall PIX 50

CAPITULO IV FIREWALL.

4.1 ¿Que es un Firewall? 50

4.2 Por que adquirir un Firewall 50

4.3 Contra que protege un Firewall 51

4.4 Tipos de Firewall 51
4.4.1 Firewall de software 51
4.4.2 Firewall de hardware y DMZ 52

4.5 Operación del Firewall 54
4.5.1 Filtrado de paquetes 54
4.5.2 firewall a nivel de aplicación 56
4.5.3 Firewall a nivel de red 58
4.5.4 Firewall a nivel de circuito 60

CAPITULO V PROTECCIÓN PERIMETRAL DE LA EMPRESA FORTINET CON EL ASA 5520.

5.1 Estado actual del sistema. 61
5.2 Planteamiento del problema. 62
5.3 Justificación del diseño. 63
5.4 Definición del Diseño de Red con el Firewall ASA 5520. 64
5.5 Configuración del Firewall ASA 5520. 65

CONCLUCIONES 70

ANEXO A 71
ANEXO A (CONTINUACIÓN) 72
ANEXO A (CONTINUACION) 73
ANEXO A (CONTINUACION) 74

ANEXO B 75
ANEXO B (CONTINUACION) 76

ANEXO C 77

ANEXO D 78
ANEXO D (CONTINUACION) 79

ANEXO E 80

INDICE DE FIGURAS 81

BIBLIOGRAFIA 83

IPN
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

TESINA

"DISEÑO E IMPLEMENTACION DE UN FIREWALL ASA 5520"

DES/ESIME-CUL/5052005/18/09

PARA OBTENER EL TITULO DE INGENIERO EN COMUINICACIONES Y ELECTRONICA

DEBERAN DESARROLLAR: **Bárcena Borja Neffi.**
Díaz Espíndola Miguel.
Gómez Hinojosa César Oswaldo.
González Hernández Carlos Alberto.

En la actualidad el uso de redes de computadoras en nuestra vida cotidiana es ya una costumbre. Pero como tal, se enfrenta cada día más a la necesidad de entender como funcionan estas redes, para poder explicar cada proceso de envío y recepción de información.

Por lo que el motivo de este trabajo es dar al lector las herramientas para entender que son, como funcionan y cual es su función específica de una red, así como también entender la funcionalidad de cada elemento que conforman estas.

Capitulado:

1.- Introducción a las redes.
2.- TCP/IP.
3.- Seguridad de Redes.
4.- Firewall.
5.- Protección Perimetral de la empresa FORTINET con al ASA 5520.
6.- Conclusiones.

14 de Agosto del 2009 – 19 de Noviembre del 2009

M. en C. RAYMUNDO SANTANA ALQUICIRA
Director del Seminario

Dr. ANTONIO CASTAÑEDA SOLIS
Asesor

M. en C. LUIS CARLOS CASTRO MADRID
Jefe de la Carrera de I.C.

CAPITULO I INTRODUCCION A LAS REDES

1.1 ¿Que es una red?

Una red identifica un grupo genérico de mecanismos conectados en red y relacionados. Por tanto, una red puede ser una LAN o una WAN, pero debe pertenecer a una única organización y presentar una arquitectura de direccionamiento coherente.

A veces se utiliza este término para hacer referencia a una internetwork o, incluso, a Internet.

El estudio de redes de cómputo comprende un campo bastante amplio, ya que enfatizar en un todo lo correspondiente a la parte de redes de computadores es complejo debido al constante desarrollo que en este campo se da cada vez con más y mejores características relacionadas con herramientas administrativas del sistema.

Las redes de comunicación de datos son utilizadas para que varias computadoras se comuniquen y puedan intercambiar datos e información. A si como compartir recursos de computo, almacenamiento e impresión.

Su objetivo principal es lograr que todos sus programas datos y equipo estén disponible para cualquiera de la red que lo solicite, sin importar la localización física del recurso y del usuario.

Otro de sus objetivos consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro, es decir que todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias. Igualmente la presencia de varios CPU significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque su rendimiento en general sea menor.

1.1.1 Tipos de redes.

En este punto se introduce el concepto de las redes de datos y sus características básicas de los 3 principales tipos de redes.

- Redes de área local (LAN).
- Redes de área amplia (WAN).
- Redes metropolitanas (MAN).

Redes de área local (LAN)

Las LAN están constituidas por computadoras, tarjetas de interfaz de red, dispositivos periféricos, medios de red y dispositivos de la red. La Figura 1.1 ilustra una LAN.

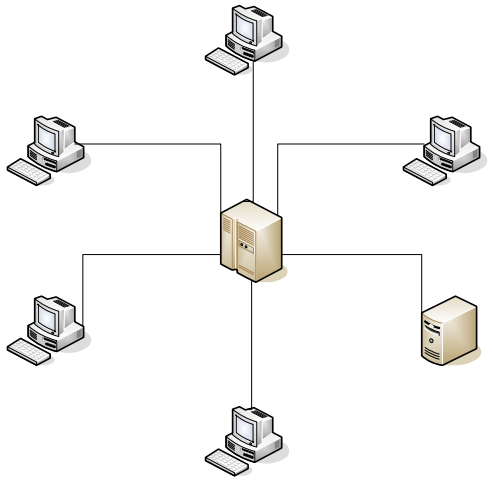


Figura 1.1 LAN.

Las LAN permiten a las empresas que emplean tecnología de computación compartir local y eficazmente ficheros e impresoras, y posibilitar las comunicaciones internas, como el correo electrónico. Unen entre si datos, comunicaciones locales y equipos de computación.

Las LAN están diseñadas para hacer lo siguiente:

- Operar dentro de una zona geográfica limitada.
- Permitir a muchos usuarios acceder a medios de gran ancho de banda.
- Proporcionar conectividad a tiempo completo a los servicios locales.
- Conectar físicamente dispositivos adyacentes.

Algunas tecnologías LAN comunes son:

- Ethernet.
- Token Ring.

Redes de área amplia (WAN)

Las WAN interconectan LAN, que proporcionan acceso o las computadoras o servidores de ficheros en otros lugares. Como las WAN conectan redes de usuario sobre un área geográfica grande, como lo muestra la Figura 1.2, hace posible que puedan comunicarse a grandes distancias.

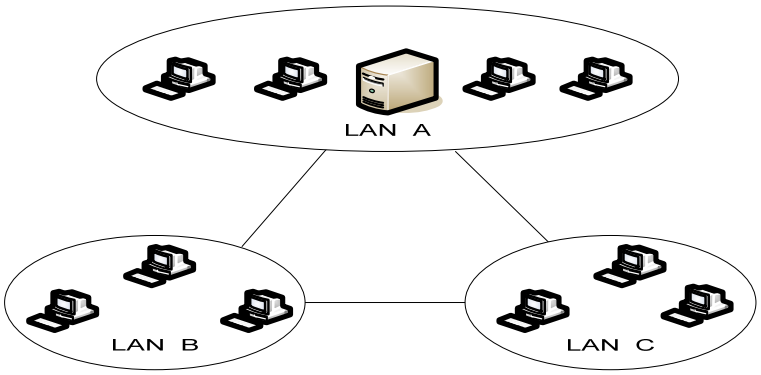


Figura 1.2 WAN.

Mediante el uso de las WAN es posible que computadoras, impresoras y otros dispositivos de una LAN compartan y sean compartidos en lugares distantes. Las LAN proporcionan comunicaciones instantáneas a través de grandes áreas geográficas. La posibilidad de enviar un mensaje instantáneo a alguien en cualquier lugar del mundo ofrece las mismas capacidades de comunicación que sólo era posible si las personas estaban en la misma oficina física.

En la mayoría de las redes de área amplia se pueden distinguir dos componentes: Las líneas de transmisión y los elementos de intercambio (Conmutación).

Las líneas de transmisión se conocen como circuitos, canales o trúncales. Los elementos de intercambio son computadores especializados utilizados para conectar dos o más líneas de transmisión.

Las redes de área local son diseñadas de tal forma que tienen topologías simétricas, mientras que las redes de área amplia tienen topología irregular. Otra forma de lograr una red de área amplia es a través de satélite o sistemas de radio.

Las WAN esta diseñadas para hacer lo siguiente:

- Operar sobre grandes áreas geográficamente separadas.
- Permitir la comunicación entre usuarios en tiempo real.
- Proporciona recurso remoto a tiempo completo con servidores locales.
- Ofrece correo electrónico, transferencia de ficheros y comercio electrónico.

Algunas tecnologías WAN comunes:

- RDSI (Red Digital de Servicios Integrados.)
- Frame Relay.
- X.25.

Redes de área metropolitana (MAN)

Una MAN es una red que se extiende por un área metropolitana, como una ciudad o un área suburbana. Las MAN son redes que conectan LAN separadas por distancia y que están ubicadas dentro de un área geográfica común.

Básicamente son una versión más grande de una Red de Área Local y utiliza normalmente tecnología similar. Puede ser pública o privada. Las MAN pueden soportar tanto voz como datos. Una MAN tiene uno o dos cables y no tiene elementos de intercambio de paquetes o conmutadores, lo cual simplifica bastante el diseño.

Teóricamente, una MAN es de mayor velocidad que una LAN, pero ha habido una división o clasificación: privadas que son implementadas en Áreas tipo campus debido a la facilidad de instalación de Fibra Óptica y públicas de baja velocidad (< 2 Mbps), como Frame Relay, ISDN, T1-E1, etc.

Teóricamente, una MAN es de mayor velocidad que una LAN, pero ha habido una división o clasificación: privadas que son implementadas en Áreas tipo campus debido a la facilidad de instalación de Fibra Óptica y públicas de baja velocidad (< 2 Mbps), como Frame Relay, ISDN, T1-E1, etc.

Figura 1.3 MAN.

1.1.2 Topología de redes.

La topología define la estructura de una red. La definición de topología puede dividirse en dos partes. La topología física, que es la disposición real de los cables (los medios) y la topología lógica, que define la forma en que los host acceden a los medios. Las topologías físicas que se utilizan comúnmente son de bus, de anillo, en estrella, en estrella extendida, jerárquica y en malla.

- La topología de bus utiliza un único segmento backbone (longitud del cable) al que todos los host se conectan de forma directa.

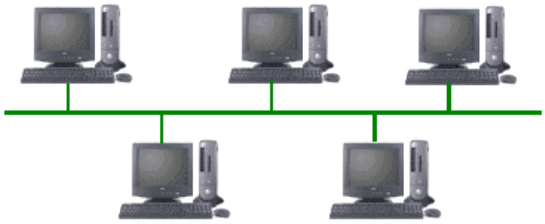


Figura 1.4 Topología en bus.

- La topología de anillo conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.

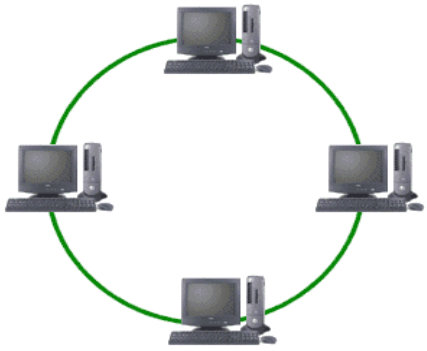


Figura 1.5 Topología en anillo.

- La topología en estrella conecta todos los cables con un punto central de concentración. Por lo general, este punto es un hub o un switch, que se describirán más adelante en este capítulo.

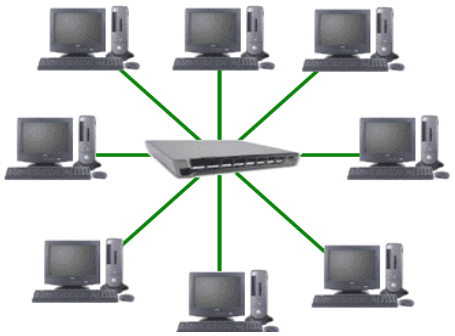


Figura 1.6 Topología de estrella.

- La topología jerárquica se desarrolla de forma similar a la topología en estrella extendida pero, en lugar de conectar los hubs/switches entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.

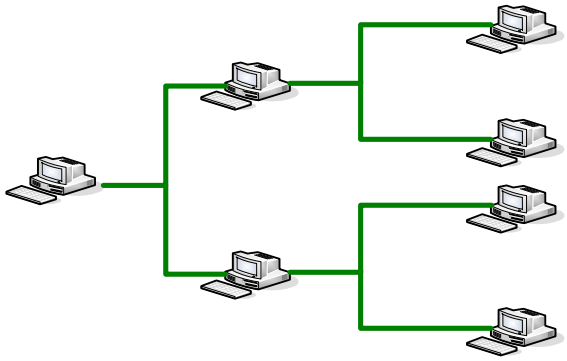


Figura 1.7 Topología jerárquica.

- La topología en malla se utiliza cuando no puede existir absolutamente ninguna interrupción en las comunicaciones, por ejemplo, en los sistemas de control de una central nuclear. De modo que, como puede observar en el gráfico, cada host tiene sus propias conexiones con los demás hosts. Esto tambien se refleja en el diseño de la Internet, que tiene múltiples rutas hacia cualquier ubicación.

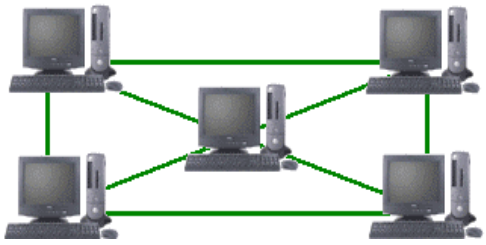


Figura 1.8 Topología en malla.

La topología lógica de una red es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast y transmisión de tokens.

La topología broadcast simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. Las estaciones no siguen ningún orden para utilizar la red, el orden es el primero que entra, el primero que se sirve. Esta es la forma en que funciona Ethernet y usted aprenderá mucho más al respecto más adelante durante este semestre.

El segundo tipo es transmisión de tokens. La transmisión de tokens controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial. Cuando un host recibe el token, eso significa que el host puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token al siguiente host y el proceso se vuelve a repetir.

1.1.3 Protocolos de redes.

Los protocolos son reglas y procedimientos para la comunicación. El término «protocolo» se utiliza en distintos contextos. Por ejemplo, los diplomáticos de un país se ajustan a las reglas del protocolo creadas para ayudarles a interactuar de forma correcta con los diplomáticos de otros países. De la misma forma se aplican las reglas del protocolo al entorno informático. Cuando dos equipos están conectados en red, las reglas y procedimientos técnicos que dictan su comunicación e interacción se denominan protocolos.

Cuando piense en protocolos de red recuerde estos tres puntos:

- Existen muchos protocolos. A pesar de que cada protocolo facilita la comunicación básica, cada uno tiene un propósito diferente y realiza distintas tareas. Cada protocolo tiene sus propias ventajas y sus limitaciones.

- Algunos protocolos sólo trabajan en ciertos niveles OSI. El nivel al que trabaja un protocolo describe su función. Por ejemplo, un protocolo que trabaje a nivel físico asegura que los paquetes de datos pasen a la tarjeta de red (NIC) y salgan al cable de la red.

- Los protocolos también puede trabajar juntos en una jerarquía o conjunto de protocolos. Al igual que una red incorpora funciones a cada uno de los niveles del modelo OSI, distintos protocolos también trabajan juntos a distintos niveles en la jerarquía de protocolos. Los niveles de la jerarquía de protocolos se corresponden con los niveles del modelo OSI.

Por ejemplo, el nivel de aplicación del protocolo TCP/IP se corresponde con el nivel de presentación del modelo OSI. Vistos conjuntamente, los protocolos describen la jerarquía de funciones y prestaciones.

La operación técnica en la que los datos son transmitidos a través de la red se puede dividir en dos pasos discretos, sistemáticos. A cada paso se realizan ciertas acciones que no se pueden realizar en otro paso. Cada paso incluye sus propias reglas y procedimientos, o protocolo.

Los pasos del protocolo se tienen que llevar a cabo en un orden apropiado y que sea el mismo en cada uno de los equipos de la red. En el equipo origen, estos pasos se tienen que llevar a cabo de arriba hacia abajo. En el equipo de destino, estos pasos se tienen que llevar a cabo de abajo hacia arriba.

Los protocolos en el equipo origen:

- Se dividen en secciones más pequeñas, denominadas paquetes.
- Se añade a los paquetes información sobre la dirección, de forma que el equipo de destino pueda determinar si los datos le pertenecen.
- Prepara los datos para transmitirlos a través de la NIC y enviarlos a través del cable de la red.

Los protocolos en el equipo de destino constan de la misma serie de pasos, pero en sentido inverso.

- Toma los paquetes de datos del cable y los introduce en el equipo a través de la NIC.
- Extrae de los paquetes de datos toda la información transmitida eliminando la información añadida por el equipo origen.
- Copia los datos de los paquetes en un búfer para reorganizarlos enviarlos a la aplicación.

Los equipos origen y destino necesitan realizar cada paso de la misma forma para que los datos tengan la misma estructura al recibirse que cuando se enviaron.

Hasta mediados de los ochenta, la mayoría de las redes de área local (LAN) estaban aisladas. Una LAN servía a un departamento o a una compañía y rara vez se conectaba a entornos más grandes. Sin embargo, a medida que maduraba la tecnología LAN, y la comunicación de los datos necesitaba la expansión de los negocios, las LAN evolucionaron, haciéndose componentes de redes de comunicaciones más grandes en las que las LAN podían hablar entre sí.

Los datos se envían de una LAN a otra, a lo largo de varios caminos disponibles, es decir, *se encaminan.* A los protocolos que permiten la comunicación LAN a LAN se les conoce como *protocolos encaminables.* Debido a que los protocolos encaminables se pueden utilizar para unir varias LAN y crear entornos de red de área extensa, han tomado gran importancia.

En una red, tienen que trabajar juntos varios protocolos. Al trabajar juntos, aseguran que los datos se preparan correctamente, se transfieran al destino correspondiente y se reciban de forma apropiada.

El trabajo de los distintos protocolos tiene que estar coordinado de forma que no se produzcan conflictos o se realicen tareas incompletas. Los resultados de esta coordinación se conocen como trabajo en niveles.

Una jerarquía de protocolos es una combinación de protocolos. Cada nivel de la jerarquía especifica un protocolo diferente para la gestión de una función o de un subsistema del proceso de comunicación. Cada nivel tiene su propio conjunto de reglas.

Los protocolos definen las reglas para cada nivel en el modelo OSI:

Nivel de aplicación	Inicia o acepta una petición
Nivel de presentación	Añade información de formato, presentación y cifrado al paquete de datos
Nivel de sesión	Añade información del flujo de tráfico para determinar cuándo se envía el paquete
Nivel de transporte	Añade información para el control de errores
Nivel de red	Se añade información de dirección y secuencia al paquete
Nivel de enlace de datos	Añade información de comprobación de envío y prepara los datos para que vayan a la conexión física
Nivel físico	El paquete se envía como una secuencia de bits

Figura 1.9 Funciones en cada nivel del modelo OSI.

Los niveles inferiores en el modelo OSI especifican cómo pueden conectar los fabricantes sus productos a los productos de otros fabricantes, por ejemplo, utilizando NIC de varios fabricantes en la misma LAN. Cuando utilicen los mismos protocolos, pueden enviar y recibir datos entre sí. Los niveles superiores especifican las reglas para dirigir las sesiones de comunicación (el tiempo en el que dos equipos mantienen una conexión) y la interpretación de aplicaciones. A medida que aumenta el nivel de la jerarquía, aumenta la sofisticación de las tareas asociadas a los protocolos.

El proceso de ligadura (binding process), el proceso con el que se conectan los protocolos entre sí y con la NIC, permite una gran flexibilidad a la hora de configurar una red. Se pueden mezclar y combinar los protocolos y las NIC según las necesidades. Por ejemplo, se pueden ligar dos jerarquías de protocolos a una NIC, como Intercambio de paquetes entre redes e Intercambio de paquetes en secuencia (IPX/SPX). Si hay más de una NIC en el equipo, cada jerarquía de protocolos puede estar en una NIC o en ambas.

El orden de ligadura determina la secuencia en la que el sistema operativo ejecuta el protocolo. Cuando se ligan varios protocolos a una NIC, el orden de ligadura es la secuencia en que se utilizarán los protocolos para intentar una comunicación correcta. Normalmente, el proceso de ligadura se inicia cuando se instala o se inicia el sistema operativo o el protocolo. Por ejemplo, si el primer protocolo ligado es TCP/IP, el sistema operativo de red intentará la conexión con TCP/IP antes de utilizar otro protocolo. Si falla esta conexión, el equipo tratará de realizar una conexión utilizando el siguiente protocolo en el orden de ligadura.

El proceso de ligadura consiste en asociar más de una jerarquía de protocolos a la NIC. Las jerarquías de protocolos tienen que estar ligadas o asociadas con los componentes en un orden para que los datos puedan moverse adecuadamente por la jerarquía durante la ejecución. Por ejemplo, se puede ligar TCP/IP al nivel de sesión del Sistema básico de entrada/salida en red (NetBIOS), así como al controlador de la NIC. El controlador de la NIC también está ligado a la NIC.

La industria informática ha diseñado varios tipos de protocolos como modelos estándar de protocolo. Los fabricantes de hardware y software pueden desarrollar sus productos para ajustarse a cada una de las combinaciones de estos protocolos. Los modelos más importantes incluyen:

- La familia de protocolos ISO/OSI.
- La arquitectura de sistemas en red de IBM (SNA).
- Digital DECnet.
- Novell NetWare.
- Apple Talk de Apple.
- El conjunto de protocolos de Internet, TCP/IP.

Los protocolos existen en cada nivel de estas jerarquías, realizando las tareas especificadas por el nivel. Sin embargo, las tareas de comunicación que tienen que realizar las redes se agrupan en un tipo de protocolo entre tres. Cada tipo está compuesto por uno o más niveles del modelo OSI.

Antes del modelo de referencia OSI se escribieron muchos protocolos. Por tanto, no es extraño encontrar jerarquías de protocolos que no se correspondan directamente con el modelo OSI.

Los protocolos de aplicación trabajan en el nivel superior del modelo de referencia OSI y proporcionan interacción entre aplicaciones e intercambio de datos.

- APPC (Comunicación avanzada entre programas): Protocolo SNA *Trabajo en Grupo* de IBM, mayormente utilizado en equipos AS/400. APPC se define como un protocolo de aplicación porque trabaja en el nivel de presentación del modelo OSI. Sin embargo, también se considera un protocolo de transporte porque APPC utiliza el protocolo LU 6.2 que trabaja en los niveles de transporte y de sesión del modelo OSI.
- FTAM (Acceso y gestión de la transferencia de archivos): Un protocolo OSI de acceso a archivos
- X.400: Un protocolo CCITT para las transmisiones internacionales de correo electrónico.
- X.500: Un protocolo CCITT para servicios de archivos y directorio entre sistemas.
- SMTP (Protocolo básico para la transferencia de correo): Un protocolo Internet para las transferencias de correo electrónico.
- FTP (Protocolo de transferencia de archivos): Un protocolo para la transferencia de archivos en Internet.
- SNMP (Protocolo básico de gestión de red): Un protocolo Internet para el control de redes y componentes.
- Telnet: Un protocolo Internet para la conexión a máquinas remotas y procesar los datos localmente.
- SMBs (Bloques de mensajes del servidor) de Microsoft y clientes o redirectores: Un protocolo cliente/servidor de respuesta a peticiones.
- NCP (Protocolo básico de NetWare) *y* clientes o redirectores: Un conjunto de protocolos de servicio.
- AppleTalk *y* AppleShare: Conjunto de protocolos de red de Apple.
- AFP (Protocolo de archivos AppleTalk): Protocolo de Apple para el acceso a archivos remotos.
- DAP (Protocolo de acceso a datos): Un protocolo de DECnet para el acceso a archivos.

Los protocolos de transporte facilitan las sesiones de comunicación entre equipos y aseguran que los datos se pueden mover con seguridad entre equipos.

- TCP: El protocolo de TCP/IP para la entrega garantizada de datos en forma de paquetes secuenciados.
- SPX: Parte del conjunto de protocolos IPX/SPX de Novell para datos en forma de paquetes secuenciados.
- NWLink: La implementación de Microsoft del protocolo IPX/SPX.
- NetBEUI (Interfaz de usuario ampliada NetBIOS): Establece sesiones de comunicación entre equipos (NetBIOS) y proporciona los servicios de transporte de datos subyacentes (NetBEUI).
- ATP (Protocolo de transacciones Apple Talk) y NBP (Protocolo de asignación de nombres): Protocolos de Apple de sesión de comunicación y de transporte de datos.

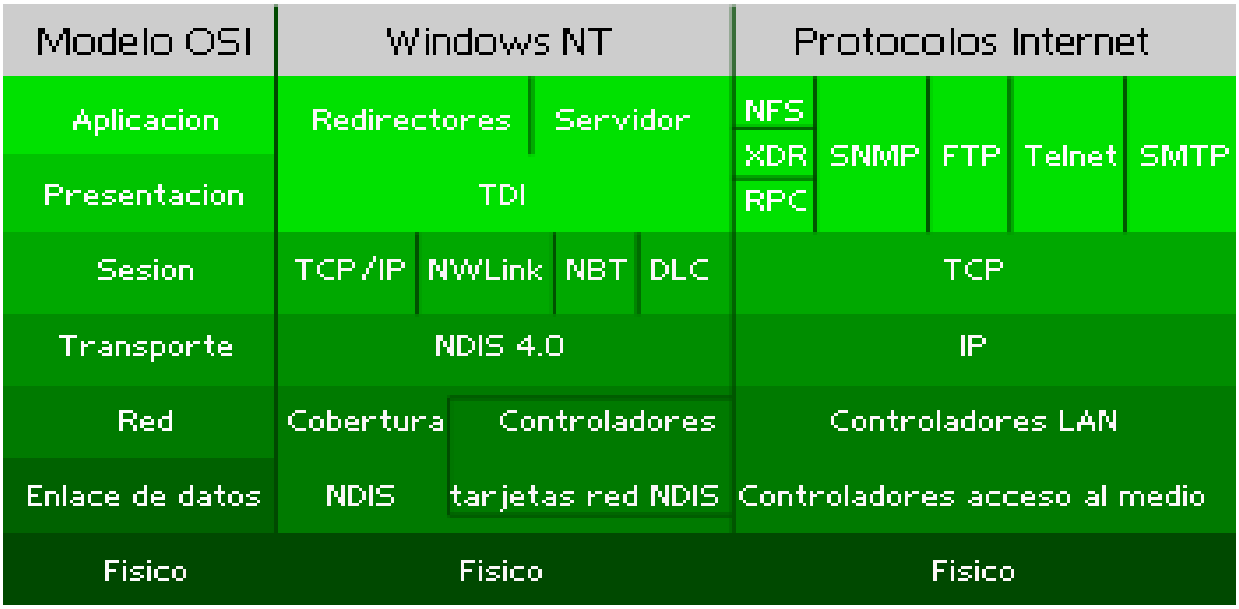


Figura 1.10 Protocolos en función de Windows NT e Internet.

Los protocolos de red proporcionan lo que se denominan «servicios de enlace». Estos protocolos gestionan información sobre direccionamiento y encaminamiento, comprobación de errores y peticiones de retransmisión. Los protocolos de red también definen reglas para la comunicación en un entorno de red particular como es Ethernet o Token Ring.

- IP: El protocolo de TCP/IP para el encaminamiento de paquetes.
- IPX: El protocolo de Novell para el encaminamiento de paquetes.
- NWLink: La implementación de Microsoft del protocolo IPX/SPX.
- NetBEUI: Un protocolo de transporte que proporciona servicios de transporte de datos para sesiones y aplicaciones NetBIOS.
- DDP (Protocolo de entrega de datagramas): Un protocolo de Apple Talk para el transporte de datos.

El modelo OSI se utiliza para definir los protocolos que se tienen que utilizar en cada nivel. Los productos de distintos fabricantes que se ajustan a este modelo se pueden comunicar entre sí.

La ISO, el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), ANSI (Instituto de Estandarización Nacional Americano), CCITT (Comité Consultivo Internacional de Telegrafía y Telefonía), ahora llamado ITU (Unión Internacional de Telecomunicaciones) y otros organismos de estandarización han desarrollado protocolos que se correspondan con algunos de los niveles del modelo OSI.

802.3 (Ethernet). Es una red lógica en bus que puede transmitir datos a 10 Mbps. Los datos se transmiten en la red a todos los equipos. Sólo los equipos que tenían que recibir los datos informan de la transmisión. El protocolo de acceso de múltiple con detección de portadora con detección de colisiones (CSMA/CD) regula el tráfico de la red permitiendo la transmisión sólo cuando la red esté despejada y no haya otro equipo transmitiendo.

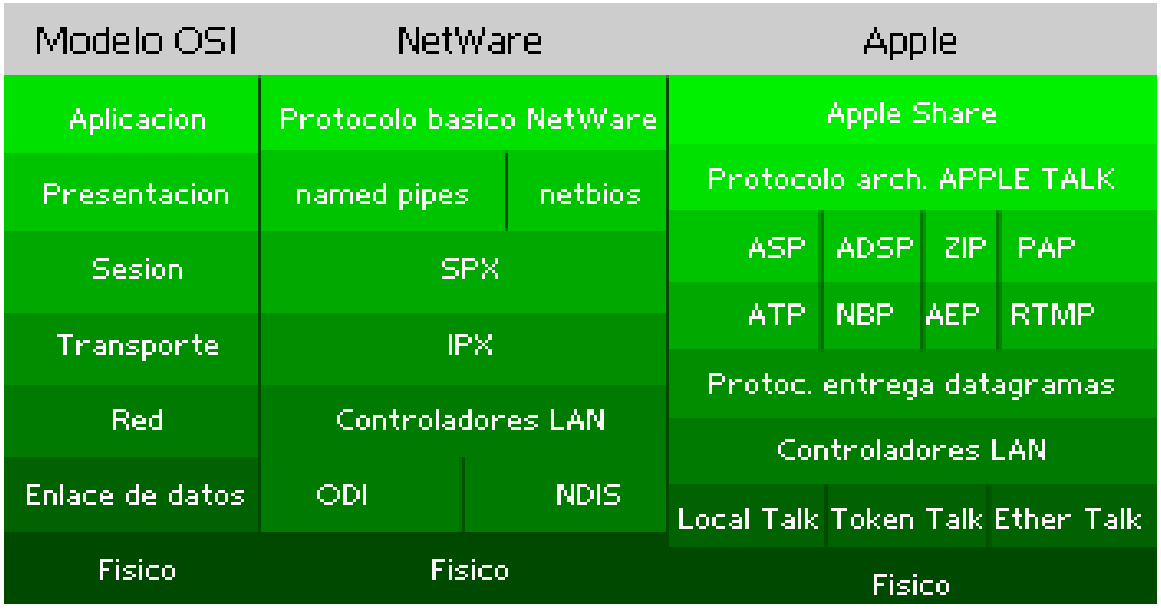


Figura 1.11 Protocolos en función de Netware y Apple.

802.4 (Token Bus**)**. Es una red en bus que utiliza un esquema de paso de testigo. Cada equipo recibe todos los datos, pero sólo los equipos en los que coincida la dirección responderán. Un testigo que viaja por la red determina quién es el equipo que tiene que informar.

802.5 (Token Ring). Es un anillo lógico que transmite a 4 ó a 16 Mbps. Aunque se le llama en anillo, está montada como una estrella ya que cada equipo está conectado a un hub. Realmente, el anillo está dentro del hub. Un token a través del anillo determina qué equipo puede enviar datos.

El IEEE definió estos protocolos para facilitar la comunicación en el subnivel de control de acceso al medio (MAC).

Un controlador MAC está situado en el subnivel de Control de acceso al medio; este controlador de dispositivo es conocido como controlador de la NIC. Proporciona acceso a bajo nivel a los adaptadores de red para proporcionar soporte en la transmisión de datos y algunas funciones básicas de control del adaptador.

Un protocolo MAC determina qué equipo puede utilizar el cable de red cuando varios equipos intenten utilizarlo simultáneamente. CSMA/CD, el protocolo 802.3, permite a los equipos transmitir datos cuando no hay otro equipo transmitiendo. Si dos máquinas transmiten simultáneamente se produce una colisión. El protocolo detecta la colisión y detiene toda transmisión hasta que se libera el cable. Entonces, cada equipo puede volver a tratar de transmitir después de esperar un período de tiempo aleatorio.

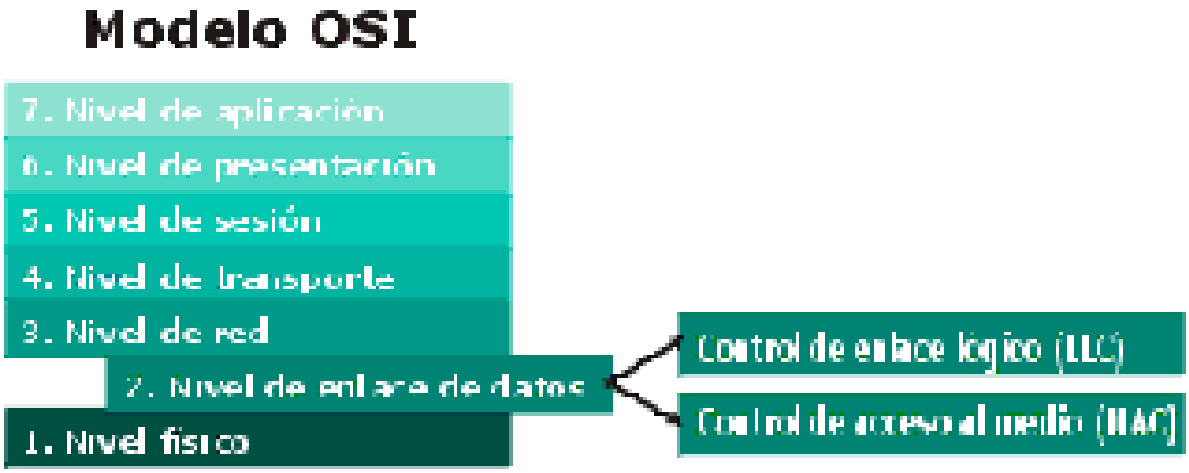


Figura 1.12 Protocolos MAC Y LLC en capa 2

1.1.4 Redes Móviles

También conocido como radiocomunicaciones en grupo cerrado de usuarios, es un servicio de telefonía móvil que sólo se presta a un colectivo de personas, en una determinada zona geográfica (una ciudad, una comarca, etc.)

El funcionamiento es prácticamente idéntico al de las redes públicas, con pequeños matices. Hay dos modalidades del servicio. En la primera cada grupo de usuarios, y sólo ellos, utiliza una determinada frecuencia.

En la segunda el sistema se encarga de asignar las frecuencias libres entre los diferentes grupos, por lo que no hay una correspondencia grupo-frecuencia.

Entre los primeros sistemas podemos destacar EDACS, controlado por un equipo fabricado por Ericsson, muy utilizado por bomberos, equipos de salvamento, policías, ambulancias, etc. Es un sistema muy seguro, capaz de establecer la comunicación en condiciones muy adversas. Los segundos se denominan sistemas Trunking, y su funcionamiento es muy parecido al de la telefonía móvil automática (TMA), uno de los primeros sistemas analógicos de telefonía móvil pública.

La mayor diferencia es que cuando no hay un canal libre para establecer una comunicación, TMA descarta la llamada y el usuario debe reintentarlo después, mientras que las redes Trunking gestionan estas llamadas, estableciendo una cola de espera.

Dos de los sistemas Trunking más populares son Taunet, que es analógico, y Tetra, que es digital. Este último es el resultado de un estándar europeo, y su equivalente estadounidense es el APCO25.

Ofrecen otras posibilidades, aparte de la comunicación vocal, como envío de mensajes cortos, transmisión de datos, conexión a redes telefónicas públicas.

1.2 Internet

1.2.1 Internetwork

Siglas de Internetwork Packet Exchange (Intercambio de paquetes interred).

Protocolo de nivel de red de Netware. Se utiliza para transferir datos entre el servidor y los programas de las estaciones de trabajo. Los datos se transmiten en datagramas.

Intercambio de paquetes interredes. Protocolo de comunicaciones NetWare que se utiliza para encaminar mensajes de un nodo a otro. Los paquetes IPX incluyen direcciones de redes y pueden enviarse de una red a otra. Ocasionalmente, un paquete IPX puede perderse cuando cruza redes, de esta manera el IPX no garantiza la entrega de un mensaje completo.

La aplicación tiene que proveer ese control o debe utilizarse el protocolo SPX de NetWare. IPX provee servicios en estratos 3 y 4 del modelo OSI (capas de red y transporte). Actualmente este protocolo esta en desuso y solo se utiliza para juegos en red antiguos.

1.2.1Arquitectura de Internet

La Internet es una red global en la cual, cada computadora actúa como un cliente y un servidor. La Internet consta de varios componentes conectados:

- Backbones: líneas de comunicación de alta velocidad y ancho de banda que unen hosts o redes.
- Redes: grupos de hardware y software de comunicación dedicados a la administración de la comunicación a otras redes. Todas las redes tienen conexiones de alta velocidad para dos o más redes.
- Proveedores del Servicio de Internet (ISPs): son computadoras que tienen acceso a la Internet. Varios proveedores de servicios en línea como Compuserve, MPSNet y Spin, actúan como ISPs proveyendo acceso a Internet a todos sus suscriptores.
- Hosts: computadoras cliente/servidor. En ellos es donde los usuarios ven la interacción con la Internet. Cada computadora que se conecta directamente a una red es un host. Todos los hosts tienen una dirección de red única. Esta es un comúnmente conocida como la dirección IP.

En una red simple, se tienen dos computadoras y una conexión de datos. Las computadoras se comunican enviando un paquete a través de la conexión. Un paquete es una unidad de datos que viaja entre hosts de una red específica.

Un paquete consiste de dos secciones:

- Encabezado: contiene la localización de la dirección física y otros datos de red.
- Datos: contiene un datagrama.

Los dos protocolos de Internet que trabajan en conjunto para la transmisión de datos son:

- Transmission Control Protocol (TCP).
- Internet Protocol (IP).

En conjunto estos protocolos son conocidos como TCP/IP. Las computadoras también pueden comunicarse con otras computadoras fuera de la LAN. Al conjunto de LANs se les conoce como redes de área amplia (WAN). Los ruteadores y gateways proveen las conexiones entre diferentes LANs. Si las LANs son del mismo tipo, se usa un ruteador. Si las LANs utilizan diferentes protocolos de comunicación, o topologías, los gateways son usados para convertir los paquetes en el formato requerido.

Cuando un gateway recibe un paquete, el gateway utiliza la información de la dirección y el encabezado del datagrama para determinar la localización del destinatario de los datos. El gateway reempaqueta el datagrama en el formato, del paquete adecuado, hacia la siguiente conexión. Los datos pueden cruzar varias LANs antes de llegar a su destino. La Internet es considerada una red de área amplia, independiente a la topología.

Esta independencia de las diversas topologías de LAN la realiza el protocolo estándar IP. El encabezado del paquete IP contiene una dirección de cuatro octetos que identifican a cada una de los equipos. Cuando un paquete es enviado hacia un host, la computadora determina si el paquete es local o remoto (dentro o fuera de la LAN).

Si el paquete es local, el mismo lo transmite; si es remoto lo envía hacia un gateway el cual determina la dirección final. La información de la dirección también determina cómo será ruteado el paquete a través de Internet. Normalmente el gateway utiliza la localización del destinatario para determinar la mejor ruta para enviar el paquete.

Si alguna red intermedia llegara a estar demasiado ocupada o no disponible, el gateway dinámicamente selecciona una ruta alterna. Una vez que el paquete es enviado, cada red que reciba el paquete, repite el proceso redirigiéndolo cuando sea necesario. Este proceso de repite hasta que el paquete llega a su destino.

Diferentes paquetes pueden tomar diferentes rutas, aún cuando contengan información del mismo archivo o mensaje. Los datos del paquete son reensamblados en el destinatario.

1.2.2 Direcciones IP

Una dirección IP es un número que identifica de manera lógica y jerárquicamente a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI. Dicho número no se ha de confundir con la dirección MAC que es un número físico que es asignado a la tarjeta o dispositivo de red (viene impuesta por el fabricante), mientras que la dirección IP se puede cambiar.

Es habitual que un usuario que se conecta desde su hogar a Internet utilice una dirección IP. Esta dirección puede cambiar al reconectar; y a esta forma de asignación de dirección IP se denomina una dirección IP dinámica (normalmente se abrevia como IP dinámica).

Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen una dirección IP fija (se aplica la misma reducción por IP fija o IP estática), es decir, no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos, servidores web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se facilita su ubicación.

Las máquinas tienen una gran facilidad para manipular y jerarquizar la información numérica, y son altamente eficientes para hacerlo y ubicar direcciones IP, sin embargo, los seres humanos debemos utilizar otra notación más fácil de recordar y utilizar, tal es el caso URLs y resolución de nombres de dominio DNS.

Existe un protocolo para asignar direcciones IP dinámicas llamado DHCP (Dynamic Host Configuration Protocol).

1.3 Intranet y Extranet

Una Intranet es una red privada empresarial o educativa que utiliza los protocolos TCP/IP de Internet para su transporte básico. Los protocolos pueden ejecutar una variedad de Hardware de red, y también, pueden coexistir con otros protocolos de red, como IPX. Aquellos empleados que están dentro de una Intranet pueden acceder a los amplios recursos de Internet, pero aquellos en Internet no pueden entrar en la Intranet, que tiene acceso restringido.

Una Intranet se compone frecuentemente de un numero de redes diferentes dentro de una empresa que se comunica con otra mediante TCP/IP. Estas redes separadas se conocen a menudo como sub-redes. El software que permite a la gente comunicarse entre ella vía e-mail y tablones de mensaje públicos, y colaborar en la producción usando software de grupos de trabajo, está entre los programas de Intranets más poderoso.

Las aplicaciones que permiten a los distintos departamentos empresariales enviar información, y a los empleados rellenar formularios de la empresa (como las hojas de asistencia) y utilizar la información corporativa financiera, son muy populares. La mayoría del software que se utiliza en las Intranets es estándar: software de Internet como el Netscape, Navigator y los navegadores Explorer para Web de Microsoft. Y los programas personalizados se construyen frecuentemente usando el lenguaje de programación de Java y el de guión de CGI.

Las Intranets también se pueden utilizar para permitir a las empresas llevar a cabo transacciones de negocio a negocio como: hacer pedidos, enviar facturas, y efectuar pagos. Para mayor seguridad, estas transacciones de Intranet a Intranet no necesitan nunca salir a Internet, pero pueden viajar por líneas alquiladas privadas.

Son un sistema poderoso para permitir a una compañía hacer negocios en línea, por ejemplo, permitir que alguien en Internet pida productos. Cuando alguien solicita un producto en Internet, la información se envía de una manera segura desde Internet a la red interna de la compañía, donde se procesa y se completa el encargo.

La información enviada a través de una Intranet alcanza su lugar exacto mediante los enrutadores, que examinan la dirección IP en cada paquete TCP (IP y determinan su destino). Después envía el paquete al siguiente direcciónador. Si este tiene que entregarse en una dirección en la misma sub - red de la Intranet desde la que fue enviado, llega directamente sin tener que atravesar otro enrutador. Si tiene que mandarse a otra sub – red de trabajo en la Intranet, se enviará a otra ruta. Si el paquete tiene que alcanzar un destino externo a la Intranet a la Intranet en otras palabras, Internet se envía a un enrutador que conecte con Internet.

Para proteger la información corporativa delicada, y para asegurar que los piratas no perjudican a los sistemas informáticos y a los datos, las barreras de seguridad llamadas firewalls protegen a una Intranet de Internet. La tecnología firewall usa una combinación de enrutadores, servidores y otro hardware y Internet, pero evitar que los intrusos se introduzcan en ella.

Muchas Intranets tienen que conectarse a "sistemas patrimoniales": el hardware y las bases de datos que fueron creadas antes de construir la Intranet. A menudo los sistemas patrimoniales usan tecnologías más antigua no basada en los protocolos TCP/IP de las Intranets. Hay varios modos mediante los que las Intranets se pueden unir a sistemas patrimoniales.

Un método común es usar los guiones CGI para acceder a la información de las bases de datos y poner esos datos en texto HTML formateado. Haciéndolos asequibles a un navegador para Web.

Lo que distingue una Intranet de cualquier otro tipo de red privada es que se basa en TCP/IP: los mismos protocolos que se aplican a Internet. TCP/IP se refiere a los dos protocolos que trabajan juntos para transmitir datos: el Protocolo de Control de Transmisión (TCP) y el Protocolo Internet (IP). Cuando envías información a través de una Intranet, los datos se fragmentan en pequeños paquetes. Los paquetes llegan a su destino, se vuelven a fusionar en su forma original.

El Protocolo de Control de Transmisión divide los datos en paquetes y los reagrupa cuando se reciben. El Protocolo Internet maneja el encaminamiento de los datos y asegura que se envían al destino exacto.

En algunas empresas, puede haber una mezcla de Intranets basadas en TCP/IP y redes basadas en otra tecnología, como NetWare. En este caso, la tecnología TCP/IP de una Intranet se puede utilizar para enviar datos entre NetWare y otras redes, usando una técnica llamada IP canalizado. Las redes NetWare usan el protocolo IPX (Intercambio de Paquetes en Internet) como medio de entregar datos y las redes TCP/IP no pueden reconocer este protocolo.

Cuando un paquete IP mediante un servidor NetWare especifico y que se dedica a ofrecer el mecanismo de transporte del IP para los paquetes IPX.

Los datos enviados dentro de una Intranet deben separase en paquetes menores de 1.500 caracteres. TCP divide los datos en paquetes. A medida que crea cada paquete, calcula y añade un número de control a éstos. El número de control se basa en los valores de los bytes, es decir, la cantidad exacta de datos en el paquete.

Cada paquete, junto al número de control, se coloca en envases IP o "sobre" separados. Estos envases contienen información que detalla exactamente donde se van a enviar los datos dentro de la Intranet o de Internet. Todos los envases de una clase de datos determinada tienen la misma información de direccionamiento así que se pueden enviar a la misma localización para reagruparse.

Los paquetes viajan entre redes Intranets gracias a enrutadores de Intranets, los enrutadores examinan todos los envases IP y estudian sus direcciones. Estos direccionadores determinan la ruta más eficiente para enviar cada paquete a su destino final. Debido a que él trafico en una Intranet cambia frecuentemente, los paquetes se pueden enviar por caminos diferentes y puedan llegar desordenados.

Si el enrutador observa que la dirección está localizada dentro de la Intranet, el paquete se puede enviar directamente a su destino, o puede enviarse a otro enrutador. Si la dirección se localiza fuera de Internet, se enviará a otro enrutador para que se pueda enviar a través de ésta.

A medida que los paquetes llegan a su destino, TCP calcula un número de control para cada uno. Después compara este número de control con el número que se ha enviado en el paquete. Si no coinciden, CP sabe que los datos en el paquete se han degradado durante él envió. Después descarta el paquete y solicita la retransmisión del paquete origina.

TCP incluye la habilidad de comprobar paquetes y determinar que se han recibido todos. Cuando se reciben os paquetes no degradaos, TCP los agrupa en su forma original, unificada. La información de cabecera de los paquetes comunica el orden de su colocación.

Una Intranet trata el paquete IP como si fuera cualquier otro, y envía el paquete a la red NetWare receptora, un servidor TCP/IP NetWare abre el paquete IP descarta el paquete IP, y lee el paquete IPX original. Ahora puede usar el protocolo IPX para entregar los datos en el destino exacto.

1.4 Modelo OSI

1.4.1 Modelo de referencia

Para poder simplificar el estudio y la implementación de la arquitectura necesaria, la ISO (Organización Internacional de Normas) creó el modelo de referencia OSI para lograr una estandarización internacional de los protocolos. Este modelo se ocupa de la Interconexión de Sistemas Abiertos a la comunicación y está divido en 7 capas, entendiéndose por "capa" una entidad que realiza de por sí una función especifica.

Los principios que se aplicaron para su división en capas son:

- Se debe crear una capa siempre que se necesite un nivel diferente de abstracción.
- Cada capa debe realizar una función bien definida.
- La función de cada capa se debe elegir pensando en la definición de protocolos estandarizados internacionalmente.
- Los límites de las capas deben elegirse a modo de minimizar el flujo de información a través de las interfaces.
- La cantidad de capas debe ser suficientes para no tener que agrupar funciones distintas en la misma capa y lo bastante pequeña para que la arquitectura no se vuelva inmanejable.

1.4.2 Propósitos del modelo OSI

El modelo de referencia OSI es el modelo principal para las comunicaciones por red. Aunque existen otros modelos, en la actualidad la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia OSI, especialmente cuando desean enseñar a los usuarios cómo utilizar sus productos.

Los fabricantes consideran que es la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

El modelo de referencia OSI permite que los usuarios vean las funciones de red que se producen en cada capa. Más importante aún, el modelo de referencia OSI es un marco que se puede utilizar para comprender cómo viaja la información a través de una red.

Además, puede usar el modelo de referencia OSI para visualizar cómo la información o los paquetes de datos viajan desde los programas de aplicación (por ej., hojas de cálculo, documentos, etc.), a través de un medio de red (por ej., cables, etc.), hasta otro programa de aplicación ubicado en otro computador de la red, aún cuando el transmisor y el receptor tengan distintos tipos de medios de red.

En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ilustra una función de red específica. Esta división de las funciones de networking se denomina *división en capas*. Si la red se divide en estas siete capas, se obtienen las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

1.4.3 Las 7 capas del modelo OSI

El problema de trasladar información entre computadores se divide en siete problemas más pequeños y de tratamiento más simple en el modelo de referencia OSI. Cada uno de los siete problemas más pequeños está representado por su propia capa en el modelo. Las siete capas del modelo de referencia *OSI* son:

Capa 7: La capa de aplicación
Capa 6: La capa de presentación
Capa 5: La capa de sesión
Capa 4: La capa de transporte
Capa 3: La capa de red
Capa 2: La capa de enlace de datos
Capa 1: La capa física

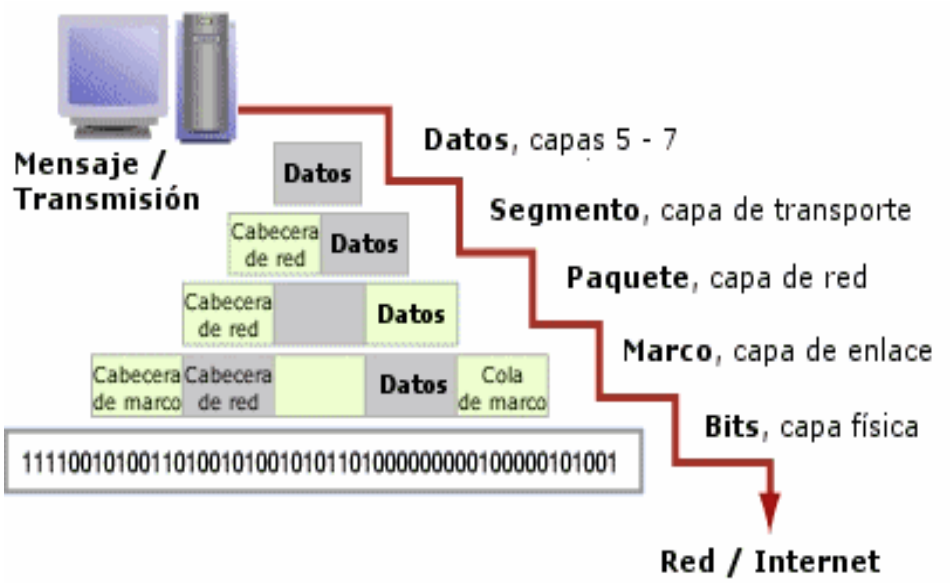


Figura 1.13 Transmisión en el modelo OSI

Nivel Físico: Define el medio de comunicación utilizado para la transferencia de información, dispone del control de este medio y especifica bits de control, mediante:

- Definir conexiones físicas entre computadoras.
- Describir el aspecto mecánico de la interface física.
- Describir el aspecto eléctrico de la interface física.
- Describir el aspecto funcional de la interface física.
- Definir la Técnica de Transmisión.
- Definir el Tipo de Transmisión.
- Definir la Codificación de Línea.
- Definir la Velocidad de Transmisión.
- Definir el Modo de Operación de la Línea de Datos.

Nivel Enlace de Datos: Este nivel proporciona facilidades para la transmisión de bloques de datos entre dos estaciones de red. Esto es, organiza los 1's y los 0's del Nivel Físico en formatos o grupos lógicos de información. Para:

- Detectar errores en el nivel físico.
- Establecer esquema de detección de errores para las retransmisiones o reconfiguraciones de la red.
- Establecer el método de acceso que la computadora debe seguir para transmitir y recibir mensajes. Realizar la transferencia de datos a través del enlace físico.
- Enviar bloques de datos con el control necesario para la sincronía.
- En general controla el nivel y es la interfaces con el nivel de red, al comunicarle a este una transmisión libre de errores.

Nivel de Red: Este nivel define el enrutamiento y el envío de paquetes entre redes.

- Es responsabilidad de este nivel establecer, mantener y terminar las conexiones.
- Este nivel proporciona el enrutamiento de mensajes, determinando si un mensaje en particular deberá enviarse al nivel 4 (Nivel de Transporte) o bien al nivel 2 (Enlace de datos).
- Este nivel conmuta, enruta y controla la congestión de los paquetes de información en una sub-red.
- Define el estado de los mensajes que se envían a nodos de la red.

Nivel de Transporte: Este nivel actúa como un puente entre los tres niveles inferiores totalmente orientados a las comunicaciones y los tres niveles superiores totalmente orientados al procesamiento. Además, garantiza una entrega confiable de la información.

Asegura que la llegada de datos del nivel de red encuentra las características de transmisión y calidad de servicio requerido por el nivel 5 (Sesión).

- Este nivel define como direccionar la localidad física de los dispositivos de la red.
- Asigna una dirección única de transporte a cada usuario.
- Define una posible multicanalización. Esto es, puede soportar múltiples conexiones.
- Define la manera de habilitar y deshabilitar las conexiones entre los nodos.
- Determina el protocolo que garantiza el envío del mensaje.
- Establece la transparencia de datos así como la confiabilidad en la transferencia de información entre dos sistemas.

Nivel Sesión: proveer los servicios utilizados para la organización y sincronización del diálogo entre usuarios y el manejo e intercambio de datos.

- Establece el inicio y termino de la sesión.
- Recuperación de la sesión.
- Control del diálogo; establece el orden en que los mensajes deben fluir entre usuarios finales.
- Referencia a los dispositivos por nombre y no por dirección.
- Permite escribir programas que correrán en cualquier instalación de red.

Nivel Presentación: Traduce el formato y asignan una sintaxis a los datos para su transmisión en la red.

- Determina la forma de presentación de los datos sin preocuparse de su significado o semántica.
- Establece independencia a los procesos de aplicación considerando las diferencias en la representación de datos.
- Proporciona servicios para el nivel de aplicaciones al interpretar el significado de los datos intercambiados.
- Opera el intercambio.
- Opera la visualización.

Nivel Aplicación: Proporciona servicios al usuario del Modelo OSI.

- Proporciona comunicación entre dos procesos de aplicación, tales como: programas de aplicación, aplicaciones de red, etc.
- Proporciona aspectos de comunicaciones para aplicaciones específicas entre usuarios de redes: manejo de la red, protocolos de transferencias de archivos (ftp), etc.

1.5 Modelo TCP/IP

1.5.1 Modelo de referencia TCP/IP

Aunque el modelo de referencia OSI sea universalmente reconocido, el estándar abierto de Internet desde el punto de vista histórico y técnico es el Protocolo de control de transmisión/Protocolo Internet (TCP/IP). El modelo de referencia TCP/IP y la pila de protocolo TCP/IP hacen que sea posible la comunicación entre dos computadores, desde cualquier parte del mundo, a casi la velocidad de la luz.

1.5.2 Las capas del modelo TCP/IP

Capa de aplicación

Los diseñadores de TCP/IP sintieron que los protocolos de nivel superior deberían incluir los detalles de las capas de sesión y presentación. Simplemente crearon una capa de aplicación que maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y garantiza que estos datos estén correctamente empaquetados para la siguiente capa.

Capa de transporte

La capa de transporte se refiere a los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Uno de sus protocolos, el protocolo para el control de la transmisión (TCP), ofrece maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de error bajo. TCP es un protocolo orientado a la conexión. Mantiene un diálogo entre el origen y el destino mientras empaqueta la información de la capa de aplicación en unidades denominadas segmentos.

Orientado a la conexión no significa que el circuito exista entre los computadores que se están comunicando (esto sería una conmutación de circuito). Significa que los segmentos de Capa 4 viajan de un lado a otro entre dos hosts para comprobar que la conexión exista lógicamente para un determinado período. Esto se conoce como conmutación de paquetes.

Capa de Internet

El propósito de la capa de Internet es enviar paquetes origen desde cualquier red en la internetwork y que estos paquetes lleguen a su destino independientemente de la ruta y de las redes que recorrieron para llegar hasta allí. El protocolo específico que rige esta capa se denomina Protocolo Internet (IP). En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes.

Esto se puede comparar con el sistema postal. Cuando envía una carta por correo, usted no sabe cómo llega a destino (existen varias rutas posibles); lo que le interesa es que la carta llegue.

Capa de acceso de red

El nombre de esta capa es muy amplio y se presta a confusión. También se denomina capa de host a red. Es la capa que se ocupa de todos los aspectos que requiere un paquete IP para realizar realmente un enlace físico y luego realizar otro enlace físico. Esta capa incluye los detalles de tecnología LAN y WAN y todos los detalles de las capas físicas y de enlace de datos del modelo OSI.

1.5.3 Comparación del modelo OSI con el modelo TCP/IP

Aunque los protocolos TCP/IP representan los estándares en base a los cuales se ha desarrollado la Internet, este currículum utiliza el modelo OSI por los siguientes motivos:

- Es un estándar mundial, genérico, independiente de los protocolos.
- Es más detallado, lo que hace que sea más útil para la enseñanza y el aprendizaje.
- Al ser más detallado, resulta de mayor utilidad para el diagnóstico de fallas.

Muchos profesionales de networking tienen distintas opiniones con respecto al modelo que se debe usar. Usted debe familiarizarse con ambos modelos.

Utilizará el modelo OSI como si fuera un microscopio a través del cual se analizan las redes, pero también utilizará los protocolos de TCP/IP a lo largo del currículum.

Recuerde que existe una diferencia entre un modelo (es decir, capas, interfaces y especificaciones de protocolo) y el protocolo real que se usa en networking. Usted usará el modelo OSI y los protocolos TCP/IP.

Si comparamos el modelo OSI y el modelo TCP/IP, observamos que ambos presentan similitudes y diferencias.

Similitudes

- Ambos se dividen en capas
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos
- Ambos tienen capas de transporte y de red similares
- Se supone que la tecnología es de conmutación por paquetes (no de conmutación por circuito)

Diferencias

- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación
- TCP/IP combina la capas de enlace de datos y la capa física del modelo OSI en una sola capa
- TCP/IP parece ser más simple porque tiene menos capas
- Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló la Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. En comparación, las redes típicas no se desarrollan normalmente a partir del protocolo OSI, aunque el modelo OSI se usa como guía

Comparación entre TCP/IP y OSI:

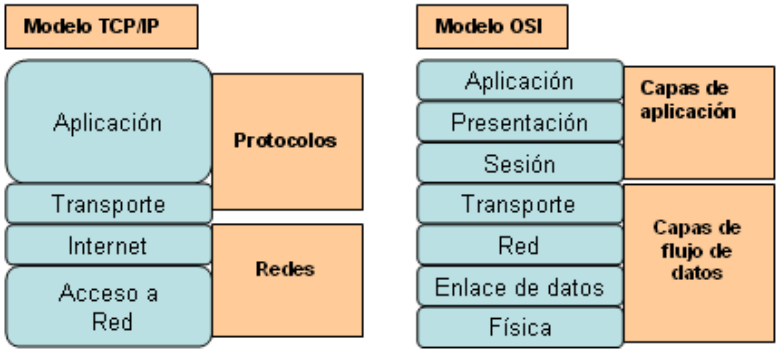


Figura1.14 Comparación de TCP/IP y OSI

Aunque los protocolos TCP/IP representan los estándares en base a los cuales se ha desarrollado la Internet, como hemos dicho antes veremos el modelo OSI por los siguientes motivos:

- Es un estándar mundial, genérico, independiente de los protocolos.
- Es más detallado, lo que hace que sea más útil para la enseñanza y el aprendizaje.
- Al ser más detallado, resulta de mayor utilidad para el diagnóstico de fallos.

Muchos administradores de red tienen distintas opiniones con respecto al modelo que se debe usar. Lo mejor es conocer los dos modelos. Utilizaremos el modelo OSI como si fuera un microscopio a través del cual se analizan las redes, pero también utilizaremos los protocolos de TCP/IP. Recuerda que existe una diferencia entre un modelo (es decir, capas, interfaces y especificaciones de protocolo) y el protocolo real que se usa en la red. Nosotros utilizaremos el modelo OSI y los protocolos TCP/IP.

CAPITULO II TCP/IP

2.1 ¿Qué es TCP/IP?

TCP/IP es el protocolo común utilizado por todos los ordenadores conectados a Internet, de manera que éstos puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectados ordenadores de clases muy diferentes y con hardware y software incompatibles en muchos casos, además de todos los medios y formas posibles de conexión.

Aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargará de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware.

TCP/IP no es un único protocolo, sino que es en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP (Transmission Control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto. En Internet se diferencian cuatro niveles o capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI de la siguiente manera:

Aplicación: Se corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET) y otros más recientes como el protocolo HTTP (Hypertext Transfer Protocol).

Transporte: Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.

Internet: Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.

Enlace: Los niveles OSI correspondientes son el de enlace y el nivel físico. Los protocolos que pertenecen a este nivel son los encargados de la transmisión a través del medio físico al que se encuentra conectado cada host, como puede ser una línea punto a punto o una red Ethernet.

El TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por este motivo hay que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP.

Sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales del TCP/IP es proporcionar una abstracción del medio de forma que sea posible el intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles.

Para transmitir información a través de TCP/IP, ésta debe ser dividida en unidades de menor tamaño. Esto proporciona grandes ventajas en el manejo de los datos que se transfieren y, por otro lado, esto es algo común en cualquier protocolo de comunicaciones. En TCP/IP cada una de estas unidades de información recibe el nombre de "datagrama" (datagram), y son conjuntos de datos que se envían como mensajes independientes.

TCP (Transmission Control Protocol).

El protocolo de control de transmisión (TCP) pertenece al nivel de transporte, siendo el encargado de dividir el mensaje original en datagramas de menor tamaño, y por lo tanto, mucho más manejables. Los datagramas serán dirigidos a través del protocolo IP de forma individual. El protocolo TCP se encarga además de añadir cierta información necesaria a cada uno de los datagramas. Esta información se añade al inicio de los datos que componen el datagrama en forma de cabecera.

La cabecera de un datagrama contiene al menos 160 bit que se encuentran repartidos en varios campos con diferente significado. Cuando la información se divide en datagramas para ser enviados, el orden en que éstos lleguen a su destino no tiene que ser el correcto. Cada uno de ellos puede llegar en cualquier momento y con cualquier orden, e incluso puede que algunos no lleguen a su destino o lleguen con información errónea.

Para evitar todos estos problemas el TCP numera los datagramas antes de ser enviados, de manera que sea posible volver a unirlos en el orden adecuado. Esto permite también solicitar de nuevo el envío de los datagramas individuales que no hayan llegado o que contengan errores, sin que sea necesario volver a enviar el mensaje completo.

- Formato de la cabecera TCP.
- Puerto origen Puerto destino
- Número de secuencia
- Señales de confirmación
- Tamaño Reservado Bits de control Window
- Checksum Puntero a datos urgentes

A continuación de la cabecera puede existir información opcional. En cualquier caso el tamaño de la cabecera debe ser múltiplo de 32 bits, por lo que puede ser necesario añadir un campo de tamaño variable y que contenga ceros al final para conseguir este objetivo cuando se incluyen algunas opciones.

El campo de tamaño contiene la longitud total de la cabecera TCP expresada en el número de palabras de 32 bits que ocupa. Esto permite determinar el lugar donde comienzan los datos.

Dos campos incluidos en la cabecera y que son de especial importancia son los números de puerto de origen y puerto de destino. Los puertos proporcionan una manera de distinguir entre las distintas transferencias, ya que un mismo ordenador puede estar utilizando varios servicios o transferencias simultáneamente, e incluso puede que por medio de usuarios distintos.

El puerto de origen contendrá un número cualquiera que sirva para realizar esta distinción. Además, el programa cliente que realiza la petición también se debe conocer el número de puerto en el que se encuentra el servidor adecuado.

Mientras que el programa del usuario utiliza números prácticamente aleatorios, el servidor deber tener asignado un número estándar para que pueda ser utilizado por el cliente. (Por ejemplo, en el caso de la transferencia de ficheros FTP el número oficial es el 21). Cuando es el servidor el que envía los datos, los números de puertos de origen y destino se intercambian.

En la transmisión de datos a través del protocolo TCP la fiabilidad es un factor muy importante. Para poder detectar los errores y pérdida de información en los datagramas, es necesario que el cliente envíe de nuevo al servidor unas señales de confirmación una vez que se ha recibido y comprobado la información satisfactoriamente.

Estas señales se incluyen en el campo apropiado de la cabecera del datagrama (Acknowledgment Number), que tiene un tamaño de 32 bit. Si el servidor no obtiene la señal de confirmación adecuada transcurrido un período de tiempo razonable, el datagrama completo se volverá a enviar. Por razones de eficiencia los datagramas se envían continuamente sin esperar la confirmación, haciéndose necesaria la numeración de los mismos para que puedan ser ensamblados en el orden correcto.

También puede ocurrir que la información del datagrama llegue con errores a su destino. Para poder detectar cuando sucede esto se incluye en la cabecera un campo de 16 bit, el cual contiene un valor calculado a partir de la información del datagrama completo (checksum). En el otro extremo el receptor vuelve a calcular este valor, comprobando que es el mismo que el suministrado en la cabecera.

Si el valor es distinto significaría que el datagrama es incorrecto, ya que en la cabecera o en la parte de datos del mismo hay algún error.

La forma en que TCP numera los datagramas es contando los bytes de datos que contiene cada uno de ellos y añadiendo esta información al campo correspondiente de la cabecera del datagrama siguiente. De esta manera el primero empezará por cero, el segundo contendrá un número que será igual al tamaño en bytes de la parte de datos del datagrama anterior, el tercero con la suma de los dos anteriores, y así sucesivamente.

Por ejemplo, para un tamaño fijo de 500 bytes de datos en cada datagrama, la numeración sería la siguiente: 0 para el primero, 500 para el segundo, 1000 para el tercero, etc.

Existe otro factor más a tener en cuenta durante la transmisión de información, y es la potencia y velocidad con que cada uno de los ordenadores puede procesar los datos que le son enviados. Si esto no se tuviera en cuenta, el ordenador de más potencia podría enviar la información demasiado rápido al receptor, de manera que éste no pueda procesarla.

Este inconveniente se soluciona mediante un campo de 16 bit (Window) en la cabecera TCP, en el cual se introduce un valor indicando la cantidad de información que el receptor está preparado para procesar. Si el valor llega a cero será necesario que el emisor se detenga. A medida que la información es procesada este valor aumenta indicando disponibilidad para continuar la recepción de datos.

2.1.1 Arquitectura de TCP/IP

TCP se diseñó para un entorno que resultaba poco usual para los años 70 pero que ahora es habitual. El protocolo TCP/IP debía conectar equipos de distintos fabricantes. Debía ser capaz de ejecutarse en diferentes tipos de medio y enlace de datos. Debía unir conjuntos de redes en una sola Internet de forma que todos sus usuarios pudiesen acceder a un conjunto de servicios genéricos.

Más aún, los desarrolladores, académicos, militares y gubernamentales de TCP/IP querían poder conectar nuevas redes sin necesidad de detener el servicio. Estos requisitos perfilaron la arquitectura del protocolo, la necesidad de independencia de tecnología del medio y una conexión automática a una red en crecimiento, condujo a la idea de transmitir datos por la red troceándolos en pequeños paquetes y encaminándolos cada uno como una unidad independiente.

Las funciones que garantizan el envío y entrega fiable de datos se situaron en los host origen y destino, por ello, los fabricantes los fabricantes debían mejorar sus esfuerzos para diseñar equipos de alta calidad.

Al hacerlo así, los protocolos de TCP/IP consiguieron escalarse muy bien ejecutándose en sistemas de cualquier calibre. Para conseguir un intercambio fiable de datos entre dos computadoras, se deben llevar a cabo muchos procedimientos separados.

La tarea de TCP/IP esencialmente es:

- Empaquetar datos.
- Determinar el camino que deben seguir.
- Transmitirlos por el medio físico.
- Regular su tasa de transferencia según el ancho de banda del medio disponible y la capacidad del receptor para absorber los datos.
- Ensamblar los datos entrantes para que mantengan la secuencia correcta y no haya pérdida de trozos.
- Comprobar los datos entrantes para ver si hay trozos perdidos.
- Notificar al transmisor que los datos se han recibido correctamente u erróneo.
- Entregar los datos a la aplicación correcta.
- Manejar eventos de errores y problemas.

El resultado es que el software de comunicaciones es complejo. Con un modelo de capas resulta más sencillo relacionar las funciones de cada protocolo con un nivel específico e implementar el software de comunicaciones de forma modular.

El modelo de comunicación de datos OSI se vió fuertemente influido por el diseño de TCP/IP. Las capas o niveles de OSI y la terminología de OSI se ha convertido en un estándar de la cultura de las comunicaciones de datos.

Los fabricantes de hardware y software deben desarrollar el diseño de sus sistemas en base al modelo OSI el cual es un estándar de la industria. A continuación se muestran las capas de TCP/IP y de OSI:

Capa Física.

La capa física trata con el medio físico, los conectores, el control de señales eléctricas representadas en unos (1) y ceros (0) binarios. Por ejemplo, las tarjetas de Red y los Cables son componentes del medio físico.

Capa de Enlace de Datos.

Se lleva a cabo la organización de unidades de datos llamadas tramas, el filtrado de errores la comprobación de direcciones de hardware (MAC) y operaciones de control de errores.

Capa de Red: IP.

IP realiza funciones en la capa de Red, IP encamina datos entre sistemas. Los datos pueden atravesar un enlace único o enviarse por múltiples enlaces a través de Rotures, los datos se transportan en unidades de bits llamados datagramas.

Un datagrama contiene una cabecera de IP que contiene información de direcciones de la capa 3 (Transporte), los encaminadores examinan la dirección de destino de la cabecera IP, para dirigir los datagramas al destino.

La capa de IP se denomina no orientada a conexión ya que cada datagrama se encamina de manera independiente e IP no garantiza la entrega fiable, ni secuencia de los mismos. IP sólo encamina su tráfico sin tener en cuenta la relación entre las aplicaciones a las que pertenece un determinado datagrama.

Capa de Transporte: TCP.

El Protocolo de Control de Transmisión realiza labores en la capa de transporte, debido a que proporciona a las aplicaciones servicios de conexión fiable de datos, por lo tanto, es un protocolo orientado a conexión. TCP dispone de los mecanismos que garantizan que los datos se entregan sin errores, sin omisiones y en secuencia.

Una aplicación, como la de transferencia de archivos, transmite datos a TCP. TCP le añade una cabecera creando una unidad denominada segmento. TCP envía los segmentos pasándoselos a su nivel inferior Capa 3 (IP) quien los encamina a su destino. Del otro lado TCP acepta los segmentos entrantes de IP, determina la aplicación de destino y traslada los datos a la aplicación en el orden en que fueron enviados.

Capa de Transporte: UDP.

Una aplicación envía un mensaje independiente a otra aplicación mediante el Protocolo de Datagramas de Usuario (UDP). UDP añade una cabecera creando una unidad denominada datagrama de UDP o mensaje de UDP. UDP traslada los mensajes de UDP salientes a IP. UDP acepta mensajes de UDP entrantes de IP y determina la aplicación de destino. UDP es un servicio de comunicaciones no orientado a conexión que suele usarse en aplicaciones de búsquedas simples en bases de datos.

Capa de Aplicación.

El Protocolo de Control de Transmisión incluye una variedad de servicios como; Telnet, FTP, WEB, Correo, IRC, Vídeo Conferencia entre otros.

2.1.2 Capa de acceso a red

Es la capa inferior de la jerarquía de protocolos de TCP/IP. Es equivalente a la capa 1 y 2 del modelo OSI (con algunas funciones de la capa 3).Hay muchos protocolos de acceso a la red (uno por cada estándar físico de red). Encapsula Datagramas en Frames y mapea direcciones IP a direcciones físicas.

Ejemplos de RFC's que definen protocolos de la capa de acceso a red son: RFC826 y RFC894. Esta capa se construye con la tarjeta de red, los drivers y los programas asociados. Un ejemplo: el Sistema Ethernet

Ethernet es una tecnología de redes de área local (LAN) que transmite información entre computadores a una velocidad de 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet) ó 1000 Mbps (Gigabit Ethernet).

- Los medios que soporta 10 Mbps son coaxial grueso, coaxial delgado, par trenzado y fibra óptica.
- Los medios que soportan 100 Mbps son par trenzado y fibra óptica
- Los medios que soporta 1000 Mbps son par trenzado y fibra óptica

El frame Ethernet

- El corazón del sistema Ethernet es el frame Ethernet utilizado para llevar datos entre computadores.
- El "frame" consta de varios bits organizados en varios campos.
- Estos campos incluyen la dirección física de las interfaces Ethernet, un campo variable de datos (entre 46 y 1500 bytes) y un campo de chequeo de error.
- El frame Ethernet Versión 2

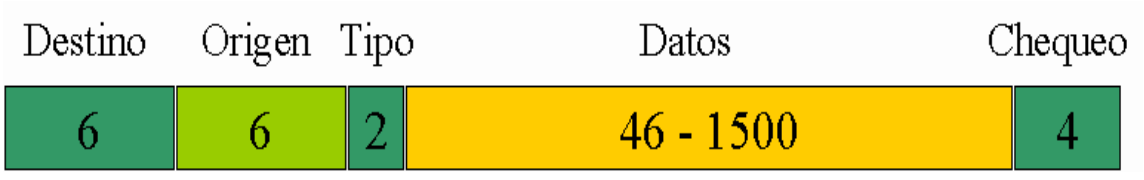


Figura 2.1 Trama Ethernet

- Destino: 6 bytes, dirección física del nodo destino (MAC address)
- Origen: 6 bytes, dirección del nodo origen
- Tipo: 2 bytes, especifica el protocolo de la capa superior
- Datos: entre 46 y 1500 bits, información de las capas superiores
- Chequeo: Secuencia de chequeo del frame.

Cuando un frame Ethernet es enviado al canal todas las interfaces revisan los primeros 6 bytes (48 bits). Si es su dirección MAC (o broadcast) reciben el paquete y lo entregarán al software de red instalado en el computador.

- Las interfaces con diferentes direcciones no continuarán leyendo el frame.
- Protocolos de alto nivel y las direcciones Ethernet
- Los paquetes de los protocolos de alto nivel (como TCP/IP) se mueven entre computadores dentro del campo de datos del frame Ethernet
- Los protocolos de alto nivel tienen su propio esquema de direcciones (por ejemplo, direcciones IP)

El software de red instalado en un equipo conoce su dirección IP (32 bits) y su dirección MAC (48 bits), PERO NO CONOCE LAS DIRECCIONES MAC DE LAS OTRAS ESTACIONES.

El mecanismo que permite descubrir las otras direcciones MAC se llama ARP (Address Resolution Protocol)

2.1.3 Como funciona ARP.

El protocolo ARP es un protocolo estándar específico de las redes. Su status es electivo.

El protocolo de resolución de direcciones es responsable de convertir las direcciones de protocolo de alto nivel (direcciones IP) a direcciones de red físicas. Primero, consideremos algunas cuestiones generales acerca de Ethernet.

ARP se emplea en redes IEEE 802 además de en las viejas redes DIX Ethernet para mapear direcciones IP a dirección hardware. Para hacer esto, ha de estar estrechamente relacionado con el manejador de dispositivo de red.

De hecho, las especificaciones de ARP en RFC 826 sólo describen su funcionalidad, no su implementación, que depende en gran medida del manejador de dispositivo para el tipo de red correspondiente, que suele estar codificado en el microcódigo del adaptador.

Si una aplicación desea enviar datos a una determinado dirección IP de destino, el mecanismo de encaminamiento IP determina primero la dirección IP del siguiente salto del paquete (que puede ser el propio host de destino o un "router") y el dispositivo hardware al que se debería enviar. Si se trata de una red 802.3/4/5, deberá consultarse el módulo ARP para mapear el par <tipo de protocolo, dirección de destino> a una dirección física.

El módulo ARP intenta hallar la dirección en su caché. Si encuentra el par buscado, devuelve la correspondiente dirección física de 48 bits al llamador(el manejador de dispositivo). Si no lo encuentra, descarta el paquete (se asume que al ser un protocolo de alto nivel volverá a transmitirlo) y genera un broadcast de red para una solicitud ARP.

El protocolo ARP es el mismo aunque haya subredes. Recordar que cada datagrama IP pasa primero por el algoritmo de encaminamiento IP. Este algoritmo selecciona el manejador de dispositivo que debería enviar el paquete. Sólo entonces se consulta al módulo ARP asociado con ese manejador.

2.1.4 Red de conmutación de paquetes.

El mundo de las comunicaciones se da diferentes topologías o diseños de las redes. Dos de las más conocidas son la configuración de conmutación con circuitos dedicados y la configuración de conmutación por paquetes con medios con acceso compartido. La conmutación de paquetes se emplea, por ejemplo, en la telefonía de voz, módems de transferencia de datos por teléfono (2.4 – 28.8 Kbps), ISDN y las telecomunicaciones de datos transferidos vía satélite de la actualidad.

En todos estos ámbitos los usuarios establecen una conexión dedicada (es decir, exclusiva) con una computadora anfitriona en el otro extremo. Esta conexión se mantiene o reserva hasta que el usuario decide finalizar (por ejemplo, el usuario se desconecta).

Estas conexiones se caracterizan por una capacidad relativamente restringida de ancho de banda y ofrecen un caudal de procesamiento máximo (de entrada y salida) de alrededor de 64 a 128 Kbps usando ISDN, o 28.8 Kbps o menos con un módem estándar que usa el teléfono.

La otra configuración, la conmutación por paquetes, semejante a la que se emplea en muchas redes de área local ("LANs"), xDSL, y entorno de transferencia de datos a través de cable, es muy diferente. En el universo de la conmutación por paquetes, hay un sólo "conducto" con ancho de banda amplio, compartido por muchos usuarios.

Este canal proporciona capacidad de caudal de procesamiento de entrada y salida desde varias decenas de Megabits por segundo hasta varios cientos de Megabits por segundo, dependiendo de la red. Puesto que varios usuarios comparten un conducto o canal común, existe la necesidad de contar con un conjunto de reglas que todos los usuarios deben observar para compartir ese recurso de manera justa y eficiente (en estos sistemas, el nivel de enlace de datos está dividido en la capa MAC y en la LLC generalmente). Con un conjunto de reglas o "protocolo" bien diseñado, la red de acceso compartido es capaz de proporcionar un servicio eficiente y eficaz al usuario.

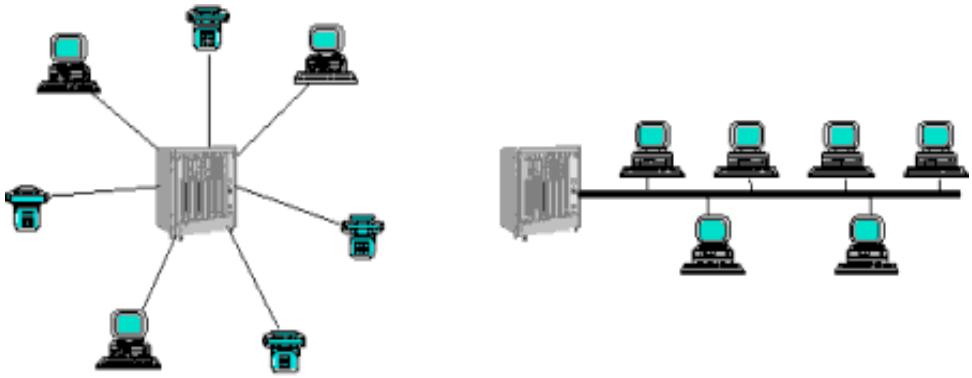


Figura 2.2 Conexión de conmutación por circuitos (izquierda) frente a de conmutación por paquetes (derecha).

En primer lugar una red de conmutación por paquetes con acceso compartido proporciona una capacidad superior de transmisión de datos a alta velocidad. Cuando un usuario hace clic en un hipervínculo, quiere que la página se descargue de inmediato. La capacidad para transmitir esa página de manera oportuna se conoce como la capacidad de "estallido" de la red.

Con una red de conmutación por paquetes con acceso compartido, el usuario tiene la capacidad de tomar un fragmento grande (por ejemplo, varios Mbps) del conducto compartido para descargar la página Web solicitada y luego liberar dicho recurso para que sea asignado a los demás usuarios. Esta capacidad de usar los recursos sólo cuando es necesario proporciona un gran beneficio de desempeño (conocido como transmisión múltiplex estadística), así como una ventaja económica inherente tanto para el proveedor del servicio como para el cliente.

De este modo, una arquitectura de conmutación por paquetes proporciona no sólo una velocidad promedio mayor y una velocidad máxima más grande, sino también permite al proveedor del servicio proporcionarlo a un costo mucho más bajo.

En segundo lugar, una red de conmutación por paquetes con acceso compartido otorga al abonado la capacidad de contar con una conexión activa todo el tiempo, sin la molestia de establecer una conexión por la red cada vez que necesite enviar un mensaje de correo electrónico o buscar información. Tercero, todos los usuarios de una red con acceso compartido se conectan al mismo conducto de información.

Esto da al proveedor de contenidos la capacidad única de transmitir corrientes de datos (por ejemplo, enviar una corriente de datos por el conducto y hacer que cientos de usuarios la vean simultáneamente; esto se conoce como multivaciado). Esta puede ser una manera sumamente eficiente y eficaz de proveer servicios como las cotizaciones bursátiles para las teleimpresoras, difusión de noticias, juegos para participantes múltiples y descarga de software.

CAPITULO III SEGURIDAD DE REDES.

3.1 Tipo de amenazas a la integración de las redes.

Las amenazas a la seguridad en las redes se pueden clasificar en cuatro categorías:

- Amenazas no estructuradas: Suelen ser originadas por personas inexpertas que utilizan herramientas denominadas “hack-tools” obtenidas de Internet. Algunas de estas personas suelen obrar de mala fe, pero la mayoría se ve arrastrada por los retos intelectuales, y suelen conocerse como script kiddies. No son programadores ni usuarios expertos, pero están muy motivados.

- Suponen una amenaza muy seria a la seguridad de las redes. A veces, pueden introducir un virus o un caballo de Troya en la red, sin ser conscientes de las consecuencias, que pueden ser a nivel mundial y causar pérdidas de millones de dólares. En algunos casos, los virus pueden contener información que revele la identidad de su autor, lo que denominamos “firmas”

- Amenazas estructuradas: Son causadas por personas mucho más motivadas y competentes a nivel técnico que los script kiddies. Estas personas suelen conocer los diseños de los sistemas de redes y sus puntos débiles. Pueden entender y crear scripts piratas que penetren en los sistemas. Una persona que plantee una amenaza estructurada suele dirigirse a un destino o grupo específico.

- Amenazas externas: Suelen ser causadas por personas o empresas ajenas a la propia empresa, que no tienen acceso autorizado a los sistemas o a la red de la misma. Suelen entrar en una red desde Internet o desde servidores de acceso telefónico.

- Amenazas internas: Normalmente, estas amenazas son causadas por personas que tienen un acceso autorizado a la red. Estos usuarios o bien tienen una cuenta en un servidor o acceso físico a la red. Una amenaza interna puede proceder de un empleado despedido o un colaborador insatisfecho. Algunos estudios reflejan que la gran mayoría de incidentes de seguridad procede de amenazas internas.

3.1.1 Tipos de ataques.

Existen tres tipos de ataques a una red:

- Ataques de reconocimiento: Un intruso trata de descubrir sistemas, servicios y puntos débiles: por ejemplo uso del nmap.
- Ataques de acceso: Un intruso ataca las redes o sistemas para recuperar datos, obtener acceso, o incrementar sus privilegios de acceso personales.
- Ataques de denegación de servicio: Un intruso ataca la red de tal forma que daña o interfiere en los servicios del sistema, e impide que otros usuarios autorizados puedan acceder a sus redes, sistemas o servicios.

3.1.2 Ataques de reconocimiento.

El reconocimiento tiene lugar cuando un usuario no autorizado trata de descubrir dispositivos, servicios disponibles y puntos débiles del sistema de red. También se conoce como recopilación de información y, en la mayoría de los casos, precede a un acceso real o a un ataque de denegación de servicio (DoS).

El intruso primero suele barrer la red con pings para determinar qué direcciones IP están activas y responden. Esto puede llevar al intruso a localizar información acerca de los servicios o puertos activos en las direcciones IP.

A partir de la información de la dirección IP activa, el intruso consulta los puertos de la aplicación con el fin de determinar el tipo y versión de la misma, así como el tipo y versión del sistema operativo que se está ejecutando en el host de destino. A veces con una simple consulta al DNS se puede obtener toda la información de la estructura de red de una empresa.

3.1.3 Ataques de negación.

Los ataques DoS (denegación de servicio) tiene lugar cuando un atacante desactiva o interfiere en el normal funcionamiento de las redes, los sistemas o los servicios para denegar el servicio a los usuarios.

Suele implicar que el sistema se colapse o que se ralentice hasta un punto en que sea inutilizable. Los ataques de DoS también pueden ser tan sencillos como borrar o corromper información necesaria. En la mayoría de los casos, el ataque suele consistir en la ejecución de un script o una herramienta.

El atacante no necesita tener acceso previo al destino, sino sólo una ruta a éste. Cuando la ruta se concreta, se puede hacer mucho daño. Dado que la mayoría de los ataques de DoS son muy fáciles de iniciar y pueden ser realizados de forma anónima, es el ataque más temido en Internet.

Un ataque de denegación de servicio distribuida (DDoS) es aquel en el que el origen del ataque proviene de muchos ordenadores, haciendo que sea muy complicado localizar y detener el origen o los orígenes.

3.1.4 Hackers

Hacker (del inglés hack, recortar) es el neologismo utilizado para referirse a un experto (véase Gurú) en varias o alguna rama técnica relacionada con las Tecnologías de la Información y las Telecomunicaciones: programación, redes de comunicaciones, sistemas operativos, hardware de red/voz, etc.

Su entendimiento es más sofisticado y profundo respecto a los sistemas informáticos, ya sea de tipo hardware o software. Se suele llamar hackeo y hackear a las obras propias de un hacker.

El término "**Hacker**" trasciende a los expertos relacionados con la informática, para también referirse a cualquier profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas.

En palabras de Richard Stallman, "Hacker, usando la palabra inglesa, quiere decir divertirse con el ingenio [cleverness], usar la inteligencia para hacer algo difícil. No implica trabajar sólo ni con otros necesariamente. Es posible en cualquier proyecto. No implica tampoco hacerlo con computadoras. Es posible ser un hacker de las bicicletas. Por ejemplo, una fiesta sorpresa tiene el espíritu del hack, usa el ingenio para sorprender al homenajeado, no para molestarle"

3.2 Soluciones

3.2.1 Filtro de paquetes.

Un firewall provisto de un filtro de paquetes TCP/IP generalmente analiza el tráfico de red en la capa de transporte o en la capa Internet (de red) de la pila de protocolos TCP/IP. Siempre y cuando los datos que fluyan por una determinada red estén basados en la pila de protocolos TCP/IP estándar (o en cualquier otra pila de protocolos estándar), podrán ser filtrados.

Los campos de cada paquete de datos que fluye por la red son conocidos (como, por ejemplo, la dirección IP de origen, la dirección IP de destino, el puerto de origen y el puerto de destino). La información analizada por un filtro de paquetes es la información estática de la cabecera del paquete. Cuando se configura un filtro de paquetes, se crean reglas que utilizan criterios de origen y/o destino específicos. Como vemos en esta representación

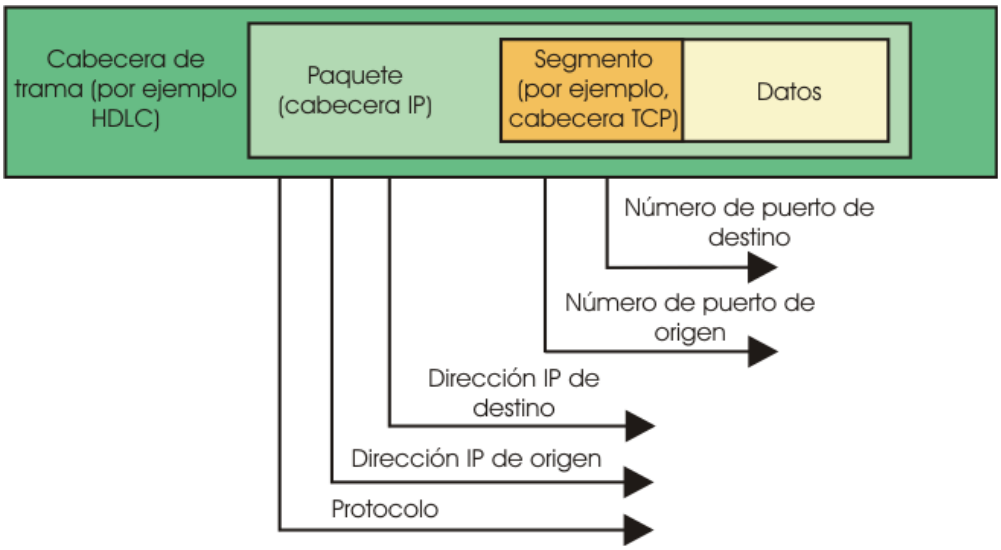


Figura 3.1 Filtro de paquetes

Siguientes criterios:

- Dirección IP de origen
- Dirección IP de destino
- Protocolo
- Puerto de origen
- Puerto de destino

Un router configurado con una lista de control de acceso (ACL) para filtrar el tráfico que pasa por él, constituye un ejemplo de filtro de paquetes. Un aspecto importante de un filtro de paquetes es que no guarda información con estado.

Cuando el filtro de paquetes recibe un paquete, toma la decisión de autorizar o denegar el paquete en base a la lista de filtros de paquetes. Cuando el filtro de paquetes ha procesado el paquete, no guarda información acerca de ese paquete concreto. Se recibe el paquete siguiente y se repite el proceso de decisión.

Algunos inconvenientes de un filtro de paquetes son:

- Es posible enviar paquetes arbitrarios que encajen con los criterios ACL y que, en consecuencia, pasen por el filtro.
- Los paquetes pueden pasar por el filtro si son fragmentados.
- Las ACL complejas resultan difíciles de crear, implementar y mantener correctamente.
- Algunos servicios no pueden ser filtrados (es posible especificar números de puerto, pero con algunas aplicaciones, especialmente las aplicaciones multimedia más recientes, los números de puerto no se conocen hasta que se inicia la sesión).

3.2.2 Filtro de Proxy

Un filtro de proxy es un dispositivo firewall que examina los paquetes en las capas superiores del modelo OSI, que suelen ser las capas de la 4 a la 7.

Este dispositivo oculta datos valiosos exigiendo que los usuarios se comuniquen con un sistema seguro a través de un proxy. Los usuarios obtienen acceso a la red pasando por un proceso que establece el estado de la sesión, la autenticación del usuario y la política autorizada. Esto implica que los usuarios se conectan con servicios externos a través de programas de aplicación (proxies) que se ejecutan en el gateway conectado con la zona externa desprotegida.

Una forma de que funcione un firewall de filtro de proxy consiste en exigir que el usuario del interior (el área de confianza) del firewall construya primero una sesión en el propio firewall (el proxy es el destino de la sesión). El usuario deberá autenticarse en ese momento. En base al tipo de usuario, se le permite tener un acceso específico al exterior.

Cuando se usa un firewall de proxy como este, se construyen dos sesiones únicas (una desde el usuario al proxy y otra desde el proxy hasta el destino) Otra forma de que funcione un firewall de proxy es que el usuario (en la zona de confianza) cree la sesión directamente con el destino (en el exterior no fiable). Al menos esto es lo que supone el usuario.

Lo que en realidad sucede es que el proxy intercepta la sesión y en base a cierta información (como la dirección IP de origen) lleva a cabo la autenticación y crea dos sesiones únicas (una desde el usuario hasta el proxy, y otra desde el proxy hasta el destino). Esta segunda forma de funcionamiento de un firewall de proxy es mucho más transparente para el usuario.

Entre las aportaciones que nos ofrece un servicio Proxy estas son las más destacadas:

- Cada Proxy es configurado para soportar únicamente un subconjunto de aplicaciones estándar de un conjunto de comandos. Si un comando estándar no es soportado por la aplicación Proxy, es porque simplemente no esta disponible para el usuario.

- Cada Proxy esta configurado para dejar acceder únicamente a los servidores especificados en el sistema. Esto significa que existe un conjunto de características/comandos que podrán ser aplicados para un subconjunto de sistemas en la red protegida.

- Cada Proxy mantiene la información detallada y auditada de todos los registros del tráfico, cada conexión, y la duración de cada conexión. El registro de audición es una herramienta esencial para descubrir y finalizar el ataque de un intruso.

- Cada Proxy es un programa pequeño y sencillo específicamente diseñado para la seguridad de redes. Este permite que el código fuente de la aplicación pueda revisar y analizar posibles intrusos y fugas de seguridad. Por ejemplo, una típica aplicación - UNIX mail - puede tener alrededor de 20,000 líneas de código cuando un correo Proxy puede contener menos de mil.

- Cada Proxy es independiente de todas las demás aplicaciones Proxy en el servidor de defensa. Si se suscitara un problema con la operación de cualquier Proxy, o si se descubriera un sistema vulnerable, este puede desinstalarse sin afectar la operación de las demás aplicaciones. Aun, si la población de usuarios requiere el soporte de un nuevo servicio, el administrador de redes puede fácilmente instalar el servicio Proxy requerido en el servidor de defensa.

- Un Proxy generalmente funciona sin acceso al disco lo único que hace es leer su archivo de configuración inicial. Desde que la aplicación Proxy no ejecuta su acceso al disco para soporte, un intruso podrá encontrar más dificultades para instalar caballos de Troya perjudiciales y otro tipo de archivos peligrosos en el servidor de defensa.

- Cada Proxy corre como un usuario no-privilegiado en un directorio privado y seguro del servidor de defensa.

- Un Proxy debe entender el protocolo de la aplicación que esta haciendo usada, aunque también pueden implementar protocolos específicos de seguridad por decir un Proxy FTP puede ser configurado para permitir FTP entrante y bloquear FTP saliente.

3.2.3 Filtro de paquetes con estado.

El tercer tipo de firewall combina lo mejor de las tecnologías de filtrado de paquetes y de las de filtrado de proxies. Un filtro de paquete con estado mantiene una información completa del estado de sesión para cada sesión que se construya en el firewall.

Cada vez que se establece una conexión IP para una conexión entrante o saliente, la información queda registrada en una tabla de flujo de sesión con estado. El filtrado de paquetes con estado es el método que utiliza el firewall ASA 5520 de Cisco.

La tabla de flujo de sesión con estado contiene las direcciones de origen y de destino, los números de puerto, información de las secuencias TCP e indicadores adicionales para cada conexión TCP/UDP que esté asociada con una determinada sesión.

Cuando se inicia una sesión a través del firewall, se crea un objeto de conexión y, consecuentemente, se comparan todos los paquetes entrantes y salientes con los flujos de sesión de la tabla de flujo de sesión con estado. Sólo si hay una conexión apropiada que valide el paso, se autoriza el paso de los datos a través del firewall.

Este método es efectivo, ya que:

- Funciona sobre paquetes individuales y los compara con las conexiones establecidas.
- Funciona a un nivel de rendimiento superior que el filtrado de paquetes o que el filtro de proxy.
- Graba los datos en una tabla por cada transacción con conexión o sin conexión que se produzca. Esta tabla sirve como punto de referencia para determinar si los paquetes pertenecen a una conexión existente o proceden de un origen no autorizado.

3.2.4 VPN

Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte.

Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública como se muestra en la siguiente figura.

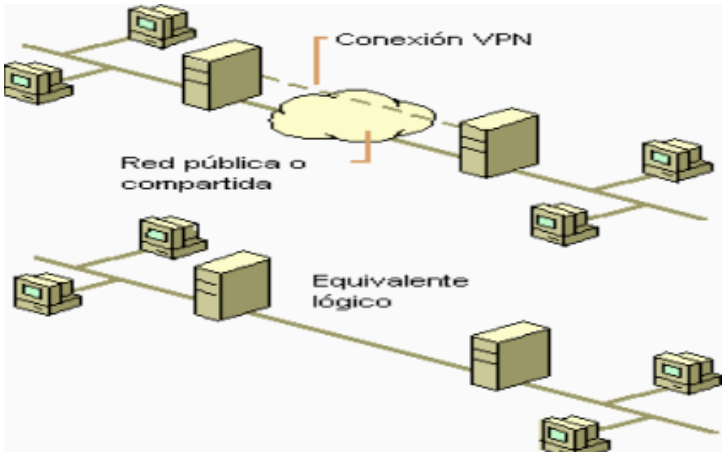


Figura 3.2 Función de la VPN

En la siguiente figura se muestra como viajan los datos a través de una VPN ya que el servidor dedicado es del cual parten los datos, llegando a firewall que hace la función de una pared para engañar a los intrusos a la red, después los datos llegan a nube de internet donde se genera un túnel dedicado únicamente para nuestros datos para que estos con una velocidad garantizada, con un ancho de banda tambien garantizado y lleguen a su vez al firewall remoto y terminen en el servidor remoto.

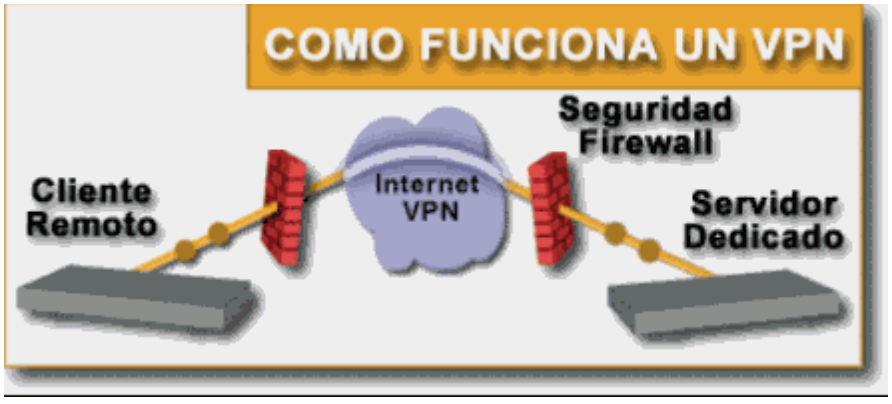


Figura 3.3 Traslado de datos en la VPN

Las VPN pueden enlazar mis oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas mediante los protocolos como internet, IP, Ipsec, Frame Relay, ATM como lo muestra la figura siguiente.

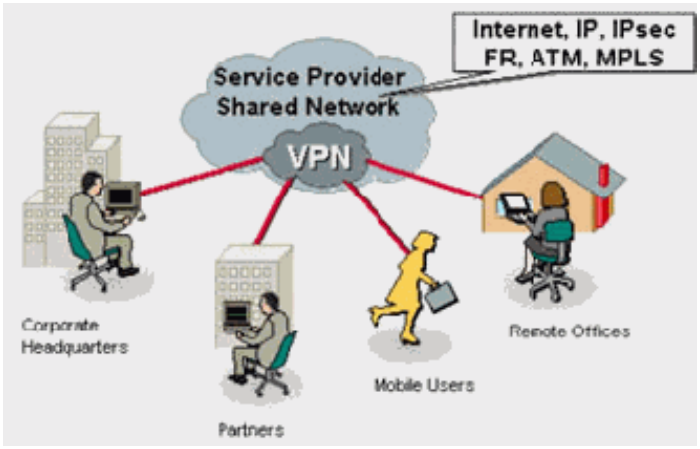


Figura 3.4 Alcance en enlace de la VPN

Las redes privadas virtuales crean un túnel o conducto de un sitio a otro para transferir datos a esto se le conoce como encapsulación además los paquetes van encriptados de forma que los datos son ilegibles para los extraños.

El servidor busca mediante un ruteador la dirección IP del cliente VPN y en la red de transito se envían los datos sin problemas.

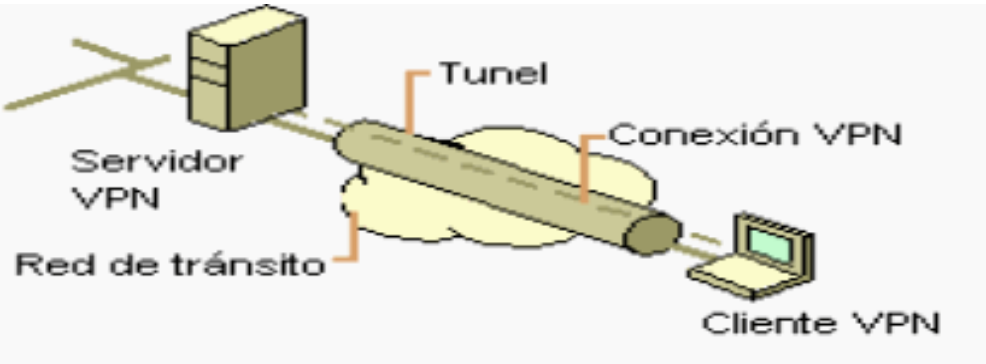


Figura 3.5 Red de transito de la VPN

Por lo general cuando se desea implantar una VPN hay que asegurarse que esta proporcione:

- Identificación de usuario.
- Administración de direcciones.
- Codificación de claves.
- Soporte a protocolos múltiples.
- Identificación de usuario.

La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien acceso, que información y cuando.

Administración de direcciones

La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

Codificación de datos

Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

Administración de claves

La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

Soporte a protocolos múltiples

La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de internet (IP), el intercambio de paquete de internet (IPX) entre otros.

Dentro de las ventajas más significativas podremos mencionar la integridad, confidencialidad y seguridad de los datos.

- Reducción de costos.
- Sencilla de usar.
- Sencilla instalación del cliente en cualquier PC Windows.
- Control de Acceso basado en políticas de la organización.
- Herramientas de diagnostico remoto.
- Los algoritmos de compresión optimizan el tráfico del cliente.
- Evita el alto costo de las actualizaciones y mantenimiento a las PC´s remotas.

CAPITULO IV FIREWALL

4.1 ¿Que es un Firewall?

Un Firewall es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización.

El Firewall forma una barrera para proteger a los ordenadores conectados a Internet en las dos direcciones: evitan una intrusión a la PC desde la Red e impiden que los programas instalados accedan a Internet sin permiso.

Un firewall puede ser un dispositivo de software o hardware sobre un sistema operativo, es decir, un aparatito que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que tiene el modem que conecta con Internet.

Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

4.2 ¿Por que adquirir un Firewall?

Esta es una de las preguntas mas frecuentes para las empresas y que merecen una respuesta clara y concisa, así entonces estos son los argumentos necesarios para lograr la adquisición.

- Internet es el principal punto de contacto con agentes malignos para el sistema. No únicamente virus, sino también de aplicaciones potencialmente peligrosas para el sistema

- El propósito del firewall es restringir el acceso al sistema a personas ajenas a él o a la red.
- El propósito del Firewall es mantener a los intrusos fuera del alcance de los trabajos que son propiedad de uno.
- Es garantía de que la conexión a Internet es segura.
- Todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información.

4.3 ¿Contra que protege un Firewall?

- Evita accesos no permitidos y ajenos al sistema, generalmente provenientes de direcciones IP inseguras y vulnerables.
- Bloquea el tráfico generado de fuera hacia adentro.
- Establecen un punto de inflexión de seguridad y de auditoria o de control, que puede ser configurado tanto para elementos externos al sistema, como para personas que trabajen desde dentro del sistema.
- Un firewall protege la red privada de una empresa de las redes públicas o compartidas a las que se conecta.
- Ayuda principalmente, a prevenir actos de vandalismos en máquinas y software de nuestra red.

4.4 Tipos de Firewall

4.4.1 Firewall de software

Los Firewalls pueden ser implementados en hardware (opción más recomendable pero muy cara) y por software.

Los Firewalls personales o de software son programas que filtran el tráfico que entra y sale de una computadora. Una vez instalados, el usuario debe definir el nivel de seguridad: permite o deniega el acceso de determinados programas a Internet (de forma temporal o definitiva) y autoriza o no los accesos desde el exterior.

En el caso de las redes personales o conexiones permanentes domésticas, lo habitual es que el ordenador esté conectado directamente a Internet, de ahí la necesidad de un Firewall por software. Algunas empresas proporcionan un sistema de protección por hardware, pero este tipo de servicio suele restringirse a empresas y se trata de conexiones mucho más caras que las pensadas para el hogar.

Los Firewalls de software no son tan complejos como otras soluciones profesionales mucho más caras y pensadas para empresas, pero en general cumplen bien con su cometido y son suficientes para la seguridad de un ordenador conectado a Internet o una red doméstica.

A la hora de escoger un buen Firewall de software el punto más importante, obviamente, es la protección que nos otorgue el programa. Sin embargo al tratarse de programas dirigidos supuestamente al usuario más inexperto, esta protección debe producirse con la mínima intervención del usuario.

Que ofrece un Firewall de software:

- Tiene la ventaja añadida de ser gratuito para uso personal.
- Ofrecen una administración sencilla y además un control exhaustivo sobre las reglas de filtrado.
- Incluye actualizaciones automáticas y soporte técnico en español.
- Soporta varios idiomas.
- Funciona sobre cualquier versión de Windows.
- Verificación de que no se envían datos personales.
- Todas las acciones que hacen los programas que ejecutemos, analizando si tienen permiso o no para llevarlas a cabo, e impidiéndoles dañar el sistema de algún modo.
- Poseen dos enfoques a la hora de filtrar el tráfico de un ordenador: controlando tráfico del sistema y controlando el de las aplicaciones.
- Algunos tienen tres niveles de configuración automática (baja, media y alta protección), además de poder definir niveles personalizados.
- Pueden enviar notificaciones por correo electrónico cuando se produzca cualquier circunstancia sospechosa de peligro.
- Ante cualquier ataque o intento de conexión externo se nos informa inmediatamente y se nos pregunta si queremos permitir el acceso.

4.4.2 Firewall de hardware y DMZ

Hoy en día un firewall es un hardware específico con un sistema operativo que filtra el tráfico y decide si un paquete pasa, se modifica, se convierte o se descarta.

Para que un firewall entre redes funcione como tal debe tener al menos dos tarjetas de red. Esta sería la tipología clásica de un firewall de hardware.

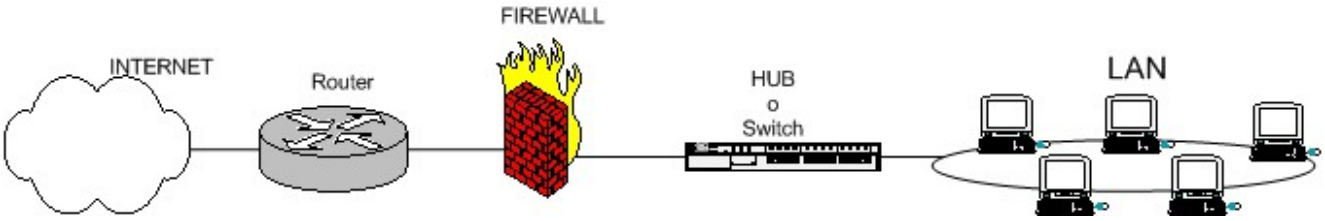


Figura 4.1 Firewall típico entre red local e Internet.

Este es el esquema típico de un firewall para proteger una red local conectada a internet a través de un router. El firewall debe colocarse entre el router (con un único cable) y la red local (conectado al switch o al hub de la LAN).

Dependiendo de las necesidades de cada red, puede ponerse uno o más Firewalls para establecer distintos perímetros de seguridad en torno a un sistema.

Es frecuente también que se necesite exponer algún servidor a internet (como es el caso de un servidor web, un servidor de correo, etc...), y en esos casos obviamente en principio se debe aceptar cualquier conexión a ellos.

Lo que se recomienda en esa situación es situar ese servidor en lugar aparte de la red, el que denominamos DMZ o zona desmilitarizada. El firewall tiene entonces tres entradas:

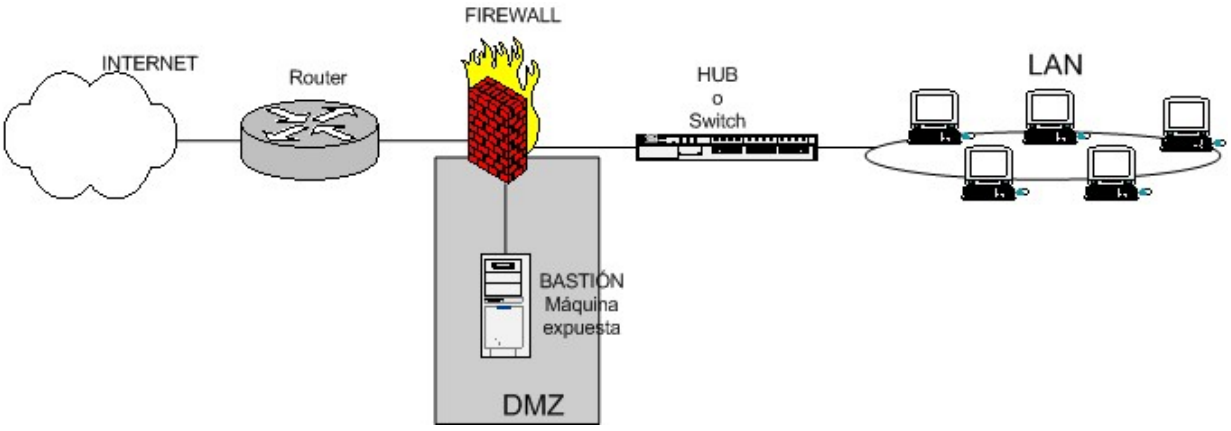


Figura 4.2 Firewall entre red local e Internet con zona DMZ para servidores expuestos.

En la zona desmilitarizada se pueden poner tantos servidores como se necesiten. Con esta arquitectura, permitimos que el servidor sea accesible desde internet de tal forma que si es atacado y se gana acceso a él, la red local sigue protegida por el firewall.

Los Firewalls se pueden usar en cualquier red. Es habitual tenerlos como protección de internet en las empresas, aunque ahí también suelen tener una doble función: controlar los accesos externos hacia dentro y también los internos hacia el exterior; esto último se hace con el firewall.

4.5 Operación del Firewall

4.5.1 Filtrado de paquetes

Esta tecnología pertenece a la primera generación de Firewalls la cual analiza el tráfico de la red. Cada paquete que entra o sale de la red es inspeccionado y lo acepta o rechaza basándose en las reglas definidas por el usuario.

El filtrado de paquetes es efectivo y transparente para los usuarios de la red, pero es difícil de configurar. Este Firewall toma las decisiones de rehusar/permitir el paso de cada uno de los paquetes que son recibidos. El Firewall examina cada datagrama para determinar si este corresponde a uno de sus paquetes filtrados y que a su vez haya sido aprobado por sus reglas.

Las reglas de filtrado se basan en revisar la información que poseen los paquetes en su encabezado, lo que hace posible su desplazamiento en un proceso de IP. Esta información consiste en la dirección IP fuente, la dirección IP destino, el protocolo de encapsulado (TCP, UDP, ICMP,), el puerto fuente TCP/UDP, el puerto destino TCP/UDP, el tipo de mensaje ICMP, la interface de entrada del paquete, y la interface de salida del paquete.

Si se encuentra la correspondencia y las reglas permiten el paso del paquete, este será desplazado de acuerdo a la información a la tabla de ruteo, si se encuentra la correspondencia y las reglas niegan el paso, el paquete es descartado.

Si estos no corresponden a las reglas, un parámetro configurable por incumplimiento determina descartar o desplazar el paquete.

Las reglas acerca del filtrado de paquetes a través de un Firewall para rehusar/permitir el trafico esta basado en un servicio en especifico, desde entonces muchos servicios vierten su información en numerosos puertos TCP/UDP conocidos.

Algunas características típicas de filtrado que un administrador de redes podría solicitar en un Firewall filtra-paquetes para perfeccionar su funcionamiento serian:

- Permitir la entrada de sesiones Telnet únicamente a una lista especifica de servidores internos.

- Permitir la entrada de sesiones FTP únicamente a los servidores internos especificados.
- Permitir todas las salidas para sesiones Telnet.
- Permitir todas las salidas para sesiones FTP.
- Rehusar todo el trafico UDP.

La mayoría de sistemas firewall son desplegados usando únicamente ruteadores filtra-paquetes. Otros que tienen tiempo planean los filtros y configuran el ruteador, sea este pequeño o no, el costoso para implementar la filtración de paquetes no es cara; desde que los componentes básicos de los ruteadores incluyen revisiones estándar de software para dicho efecto.

Desde entonces el acceso a Internet es generalmente provisto a través de interfaces WAN, optimando la operación del ruteador moderando el tráfico y definiendo menos filtros. Finalmente, el ruteador de filtrado es por lo general transparente a los usuarios finales y a las aplicaciones por lo que no se requiere de entrenamiento especializado o software especifico que tenga que ser instalado en cada uno de los servidores.

Definir el filtrado de paquetes puede ser una tarea compleja porque el administrador de redes necesita tener un detallado estudio de varios servicios de Internet, como los formatos del encabezado de los paquetes, y los valores específicos esperados a encontrase en cada campo. Si las necesidades de filtrado son muy complejas, se necesitara soporte adicional con lo cual el conjunto de reglas de filtrado puede empezar a complicar y alargar el sistema haciendo mas difícil su administración y comprensión.

Finalmente, estas serán menos fáciles de verificar para las correcciones de las reglas de filtrado después de ser configuradas en el Firewall. Potencialmente se puede dejar una localidad abierta sin probar su vulnerabilidad. Cualquier paquete que pasa directamente a través de un Firewall puede ser posiblemente usado como parte inicial un ataque dirigido de datos.

Generalmente, los paquetes entorno al Firewall disminuyen conforme el numero de filtros utilizados se incrementa. Los Firewall son optimizados para extraer la dirección destino IP de cada paquete, haciendo relativamente simple la consulta a la tabla de ruteo, y el desplazamiento de paquetes para la interface apropiada de la transmisión.

Si esta autorizado el filtro, no únicamente podrá el ruteador tomar la decisión de desplazar cada paquete, pero también sucede aun aplicando todas las reglas de filtrado. Esto puede consumir ciclos de CPU e impactar el perfecto funcionamiento del sistema.

El filtrado de paquetes IP no puede ser capaz de proveer el suficiente control sobre el tráfico. Un Firewall Filtra-Paquetes puede permitir o negar un servicio en particular, pero no es capaz de comprender el contexto/dato del servicio.

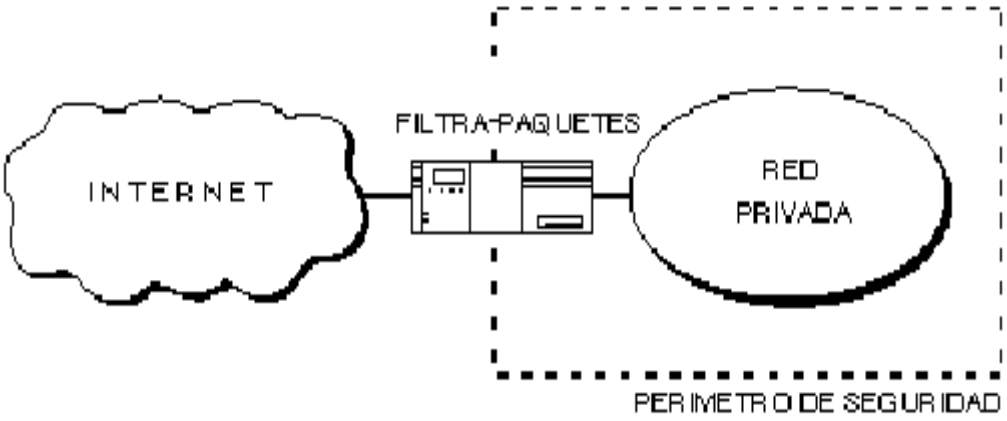


Figura 4.3 Firewall filtra paquetes.

4.5.2 Firewall a nivel de aplicación

Pertenece a la tercera generación de Firewalls. Examina la información de todos los paquetes de la red y mantiene el estado de la conexión y la secuencia de la información. En este tipo de tecnología también se puede validar claves de acceso y algunos tipos de solicitudes de servicios.

La mayoría de estos tipos de Firewalls requieren software especializado y servicios Proxy. Recordemos que un servicio Proxy es un programa que aplica mecanismos de seguridad a ciertas aplicaciones, tales como FTP o HTTP.

Un servicio Proxy puede incrementar el control al acceso, realizar chequeos detallados a los datos y generar auditorias sobre la información que se transmite.

Son generalmente, hosts que corren bajo servidores Proxy, que no permiten tráfico directo entre redes y que realizan logines elaborados y auditan el tráfico que pasa a través de ellas.

Los Firewall a nivel de aplicación se pueden usar como traductores de direcciones de red, desde que el tráfico entra por un extremo hasta que sale por el otro. Los primeros Firewalls a nivel de aplicación eran poco transparentes a los usuarios finales, pero los modernos Firewalls a nivel de aplicación son bastante transparentes.

Los Firewalls a nivel de aplicación, tienden a proporcionar mayor detalle en los informes auditados e implementan modelos de conservación de la seguridad.

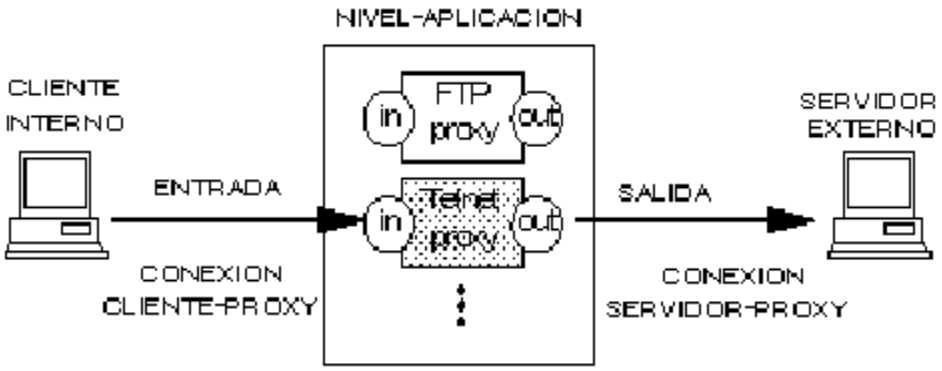


Figura 4.4 Firewall a nivel de aplicación.

Un ejemplo de una Firewall a nivel de aplicación es el mostrado en la siguiente figura.

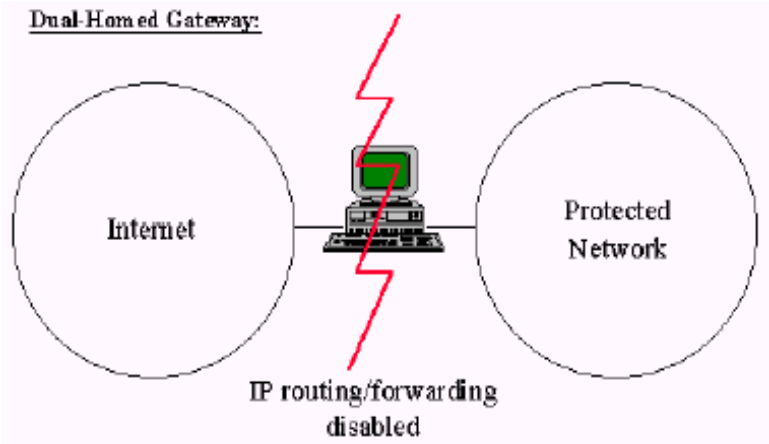


Figura 4.5 Firewall a nivel de aplicación.

En este ejemplo, se representa un Firewall a nivel de aplicación llamada "dual homed gateway". Un Firewall de este tipo es un host de alta seguridad que corre bajo software Proxy. Consta de 2 interfaces de red (uno a cada red) los cuales bloquean todo el tráfico que pasa a través del host.

Un Firewall filtra-paquetes permite la circulación directa de los paquetes dentro y fuera del sistema, diferente a esto el Firewall a nivel-aplicación deja que la información circule entre los sistemas pero no permite el intercambio directo de paquetes.

El principal riesgo de permitir que los paquetes se intercambien dentro y fuera del sistema se debe a que el servidor residente en los sistemas de protección de la red podrá ser asegurado contra cualquier amenaza representada por los servicios permitidos.

Un Firewall a nivel-aplicación por lo regular es descrito como un "servidor de defensa" porque es un sistema diseñado específicamente blindado y protegido contra cualquier ataque. Son muchos los beneficios desplegados en un Firewall a nivel-aplicación. Ellos dan a la administración de red un completo control de cada servicio desde aplicaciones proxy limitadas por un conjunto de comandos y la determinación del servidor interno donde se puede accesar a los servicios.

Aun cuando, el administrador de la red tenga el completo control acerca de que servicios que son permitidos desde la carencia de un servicio proxy para uno en particular significa que el servicio esta completamente bloqueado.

Los Firewalls a nivel-aplicación tienen la habilidad de soportar autenticaciones forzando al usuario para proveer información detallada de registro. Finalmente, las reglas de filtrado para un Firewall de este tipo son mucho mas fáciles de configurar y probar que en un Firewall filtra-paquetes.

Probablemente una de las grandes limitaciones de un Firewall a nivel de aplicación es que requiere de modificar la conducta del usuario o requiere de la instalación de software especializado en cada sistema que accese a los servicios Proxy.

4.5.3 Firewalls a nivel de red.

Los Firewalls a nivel de red, toman las decisiones basándose en la fuente, dirección de destino y puertos, todo ello en paquetes individuales IP. Un simple router es un "tradicional" Firewall a nivel de red, particularmente, desde el momento que no puede tomar decisiones sofisticadas en relación con quién está hablando un paquete ahora o desde donde está llegando en este momento.

Los modernos Firewall a nivel de red se han sofisticado ampliamente, y ahora mantienen información interna sobre el estado de las conexiones que están pasando a través de ellos, los contenidos de algunos datagramas y más cosas. Un aspecto importante que distingue a los Firewall a nivel de red es que ellos enrutan el tráfico directamente a través de ellas, de forma que un usuario cualquiera necesita tener un bloque válido de dirección IP asignado.

Los Firewalls a nivel de red tienden a ser más veloces y más transparentes a los usuarios.

Un ejemplo de un Firewall a nivel de red se muestra en la siguiente figura:

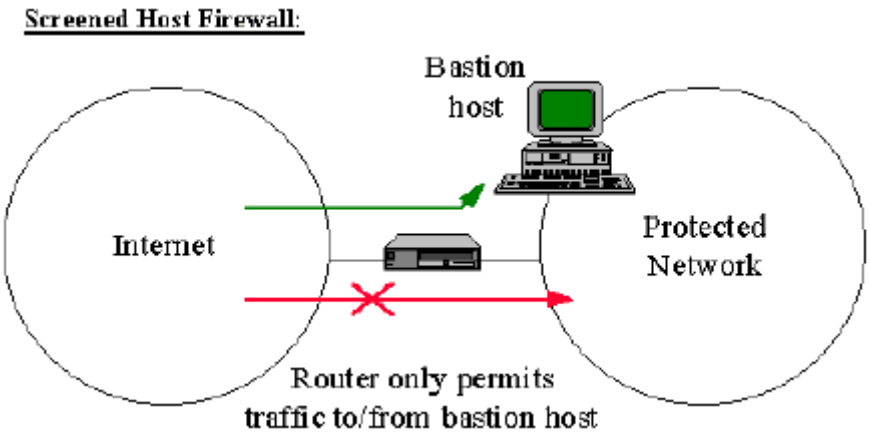


Figura 4.6 Firewall a nivel de red.

En este ejemplo se representa un Firewall a nivel de red llamada "Screend Host Firewall". En dicho Firewall, se accede a y desde un único host el cual es controlado por un router operando a nivel de red. El host es como un bastión, dado que está muy defendido y es un punto seguro para refugiarse contra los ataques.

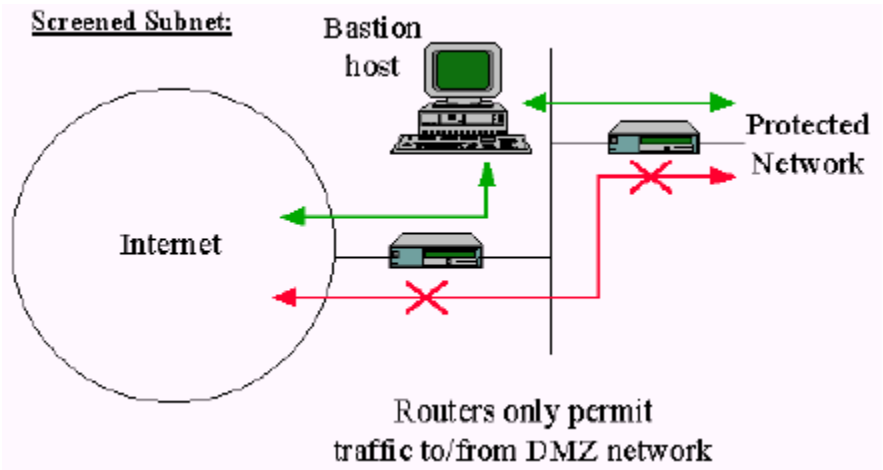


Figura 4.7 Firewall a nivel de red (red mas efectiva que la anterior)

Otro ejemplo sobre un Firewall a nivel de red es el mostrado en la figura anterior. En este ejemplo se representa un Firewall a nivel de red llamada "screened subnet Firewall".

En dicho Firewall se accede a y desde el conjunto de la red, la cual es controlada por un router operando a nivel de red. Es similar al Firewall indicado en el ejemplo anterior salvo que esta si que es una red efectiva de hosts protegidos.

4.5.4 Firewall a nivel de circuito

Esta tecnología pertenece a la segunda generación de Firewalls y valida que los paquetes pertenezcan ya sea a una solicitud de conexión o bien a una conexión entre dos computadoras. Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Una vez que la conexión se establece, los paquetes pueden ir y venir entre las computadoras sin tener que ser revisados cada vez.

El firewall mantiene una tabla de conexiones válidas y permite que los paquetes de la red pasen a través de ella si corresponden a algún registro de la tabla. Una vez terminada la conexión, la tabla se borra y la transmisión de información entre las dos computadoras se cierra.

Un Firewall a nivel-circuito es en si una función que puede ser perfeccionada en un Firewall a nivel-aplicación. A nivel-circuito simplemente trasmite las conexiones TCP sin cumplir cualquier proceso adicional en filtrado de paquetes.

El Firewall a nivel-circuito se usa frecuentemente para las conexiones de salida donde el administrador de sistemas somete a los usuarios internos. La ventaja preponderante es que el servidor de defensa puede ser configurado como un Firewall "híbrido" soportando nivel-aplicación o servicios Proxy para conexiones de venida y funciones de nivel-circuito para conexiones de ida.

Esto hace que el sistema de firewall sea fácil de usar para los usuarios internos quienes desean tener acceso directo a los servicios de Internet mientras se proveen las funciones del firewall necesarias para proteger la organización de los ataques externos.

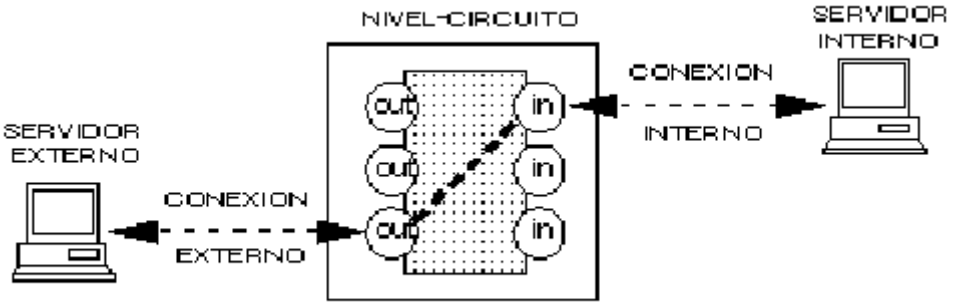


Figura 4.8 Firewall a nivel circuito.

CAPITULO V PROTECCIÓN PERIMETRAL DE LA EMPRESA FORTINET CON EL ASA 5520

5.1 Estado actual del sistema

La empresa “FORTINET” esta dedicada a crear herramienta y maquinaria en la industria azucarera.

Como es bien sabido hoy en día las transacciones ya no se hacen personalmente, la empresa “FORTINET”, en este sentido, para poder generar mas productividad ha decidido agregarse al INTERNET para poder hacer ventas por este medio así como transacciones de pagos con proveedores y bancos.

La empresa actualmente tiene asignados los siguientes dispositivos:

- Un router 2800.
- Tres servidores (FTP, Email, Web)
- Tres switches

La empresa “FORTINET” tiene asignados en este momento 3 switches interconectados entre ellos los cuales soportan la comunicación de datos entre todos los clientes, por otro lado, gran parte de la comunicación dentro de la empresa es con cable par trenzado categoría 5 con velocidad de 100Mbps conectando a 30 computadoras (la mayoría sin ningún tipo de seguridad), además de enlaces Ethernet para sus diferentes departamentos. Es decir, dicha red es grande y sin embargo ha crecido de manera desordenada y con poca planeación.

El router 2800 cuenta solo con dos interfaces una para la red interna y otra para la red externa, esto quiere decir que todo el flujo de información proveniente de la Internet tiene acceso a la red interna, esto representa un peligro para la empresa empresa “FORTINET” ya que en sus servidores (FTP, Email, Web) cuenta con datos importantes de la misma empresa como también de la de sus trabajadores.

Al emigrar de un router a un Firewall ASA 5520 la empresa “FORTINET” contara con los siguientes servicios en seguridad:

- No permitir acceso desde el exterior hasta el interior.
- Permitir un acceso limitado desde el exterior hasta la DMZ.
- Permitir todo el acceso desde el interior hasta el exterior.
- Permitir un acceso limitado desde el interior hasta la DMZ.

Para visualizar la situación actual de la empresa empresa “FORTINET.” observe la figura 1 del **anexo A**.

5.2 Planteamiento del problema.

La empresa “FORTINET” se ha ido estableciendo en los últimos años como una de las principales distribuidoras y procesadoras a nivel nacional. La empresa sabe de las ventajas y beneficios de estar conectados a Internet pero requieren de mantener la confidencialidad, integridad y disponibilidad de información.

Es por esa necesidad que nos solicito la instalación de un servicio de seguridad para sus enlaces a Internet, en respuesta nosotros le ofrecimos el servicio basado en la tecnología Firewall ASA 5520.

Al inspeccionar la red y acercarnos al administrador encontramos los siguientes riesgos para la empresa “FORTINET”.

La información que se trasmite desde el interior de la red a clientes legítimos para sus entregas de pedidos muestra la ruta del transporte, la cantidad a entregar y la cantidad a pagar por el pedido, esto para la empresa representa un gran riesgo ya que los intrusos observan y guardan la información para eventuales asaltos carreteros y también porque no decirlo para un asalto a la misma sucursal.

Se les han hecho muchos pedidos ficticios.

Los intrusos tienen acceso al servidor Web, esto afecta directamente a los clientes para realizar sus pedidos, lo más común es la saturación del servidor y la espera innecesaria de los clientes legítimos.

Los ataques a la administración de la empresa en cuanto a sus trabajadores; cada uno tiene una cuenta bancaria y por supuesto sus registros personales para evitar cualquier tipo de fraude es necesario que solo los trabajadores tengan el acceso a su información desde la misma empresa.

El atacante del exterior inunda al servidor con solicitudes de venta de maquinaria o equipo para procesar la azúcar; ellos ya tienen a una empresa que les provee de estos servicios, esto trae como resultado la denegación del servicio.

La ultima y talvez la más importante es que se pueda acceder al servidor que contiene información sensible de la empresa como lo es la cuenta bancaria de persona moral y a las palabras claves de acceso de la misma.

5.3 Justificación del diseño.

Formalmente hablando de la seguridad en sistemas de cómputo es una medida de confianza en la integridad de la información manejada por éstos. Resulta de gran relevancia ya que un sistema de cómputo carecería de sentido si la integridad y la confidencialidad de la información que procesa fuera violada.

El hecho de disponer de una conexión a Internet puede ser causa de multitud de ataques a nuestros servidores desde el exterior.

Cuanto más tiempo permanezcamos conectados mayor es la probabilidad de que la seguridad de nuestro sistema se vea comprometida por un atacante desconocido.

La seguridad es implementada mediante mecanismos de protección, que controlan el acceso a los recursos de cómputo ofrecidos y a los mismos usuarios.

La consecuencia de la correcta implementación de mecanismos de seguridad en un sistema de cómputo es el mejoramiento del desempeño del mismo, ya que nadie se apropiará de un recurso por más tiempo del asignado, además de la verificación de las condiciones de ese uso.

5.4 Definición del Diseño de Red con el Firewall ASA 5520.

Como ya hemos mencionado en el transcurso de este trabajo un Firewall en su concepción más práctica separa redes privadas de redes públicas. En este caso practico la empresa "FORTINET" requiere el servicio de seguridad para sus enlaces a Internet.

De a cuerdo al diseño que tiene actualmente y con la necesidad de contar con un punto de acceso que pueda determinar que tipo de flujo pueda circular por la red interna y además que se tome en cuenta la confiabilidad de la información que llega del exterior hemos propuesto la siguiente solución con un Firewall ASA 5520. Vea la figura 1 del **anexo A**.

Observando el diseño que planteamos podemos determinar lo siguiente:

Al emigrar de un router a un Firewall ASA 5520 se logra que la información fluya de manera segura; sin embargo también se requiere que cierta información del exterior logre llegar a los servidores (Web, Mail, FTP) esto se puede lograr con la incorporación de una tercer interfaz, así entonces al colocar el Firewall ASA 5520 se tienen tres interfaces, entonces se crean tres subredes.

Las tres subredes que crea el Firewall ASA 5520 se describen de este modo:

A todos los componentes que se encuentren atrás del Firewall ASA 5520 que en este caso son los switches y el total de las computadoras para clientes la denominaremos red interior, que es nuestra área de confianza de la Internetwork, estos elementos comparten un mismo nivel con respecto a la red exterior (Internet).

De manera opuesta, a los componentes que se encuentren delante del Firewall ASA 5520 la denominaremos red exterior esto quiere decir que es el área de no confianza de la Internetwork, todo lo que provenga de esta red será peligroso para el los componentes de nuestra red.

Por ultimo la DMZ que es una subred aislada, posibilita que la empresa ponga la información y los servicios a los dispositivos de los usuarios del exterior dentro de un entorno seguro y controlado.

Para que usted pueda ver estas interfaces revise la figura 2 del **anexo A**.

5.5 Configuración del Firewall ASA 5520.

La primera vez que accedemos al Firewall ASA 5520 lo haremos en modo no privilegiado y nos aparecerá el indicador ">" en el prompt, para pasar al modo privilegiado usaremos el comando "enable" el prompt cambiara al indicador "#". Al realizar esto por primera vez no se pedirá un password ya que no lo hemos configurado. Si queremos pasar a al modo de configuración utilizaremos el comando "configure terminal" y el promt cambiara al indicador "(config) #.

ASA 5520firewall> enable
ASA 5520firewall# configure terminal
ASA 5520firewall(config)# exit
ASA 5520firewall# disable
ASA 5520firewall>

Borramos la configuración por defecto y comenzamos.

ASA 5520firewall (config)# write erase
Erase ASA 5520 configuration in flash memory? [confirm] <Enter>

El siguiente paso será cambiar el hostname del Firewall ASA 5520 con el fin de contar con una expresión que corresponda e identifique ya a la empresa esto se logra cuando se esta en el modo de configuración, lo anterior se establece con la siguiente sintaxis:

ASA 5520firewall(config)# hostname Empresa FORTINET

Siguiendo con las necesidades de seguridad de la empresa se tiene que declarar una contraseña que solo la tendrá el administrador de la red, con el comando password se logra esta declaración. Recuerde que ya establecimos el nuevo hostname del Firewall ASA 5520, entonces se tiene la siguiente sintaxis

Empresa FORTINET (config) # password aguaH2O

Para evitar el uso de direcciones IP directamente y/o consultas a un DNS externo vamos a configurar la opción de resolución de nombres estática con la ayuda del comando "name" se tiene la siguiente sintaxis:

Empresa FORTINET (config) # name 172.16.1.2 bastionhost

También es necesario configurar la resolución de forma local en el Firewall ASA 5520 esto también se realiza con el comando "name". Se tiene la siguiente sintaxis:

Empresa FORTINET (config) # name 10.0.1.11 insidehost

Al configurar el Firewall ASA 5520 para el flujo de datos en necesario tener en cuenta el siguiente razonamiento:

"Los datos puede acceder al Firewall ASA 5520 a través de una interfaz con un nivel de confianza más alto, pasar por él y salir a través de una interfaz con un nivel de confianza mas bajo. Por el contrario, los datos que acceden una interfaz provista de un nivel de confianza mas bajo no pueden pasar por él y salir a través de una interfaz con un nivel de confianza más alto".

Lo que realizaremos en este momento es la configuración de las interfaces de a cuerdo con el nivel de confianza para la red interna, la red externa y la DMZ.

Comenzaremos con la parte de la red externa de nuestro diseño, esto quiere decir que estamos hablando de todo lo que pueda afectar, destruir, desconfigurar la red interna, por el momento no se tomaran en cuenta las direcciones IP de cada interfaz.

Para esta interfaz se le asignara nivel mas bajo de seguridad. Este nivel de seguridad es cero, se usa para la interfaz externa. Es la configuración predeterminada y no puede ser modificada. Esta interfaz sirve para conectarse a Internet.

Con ayuda del comando "name if" especificamos la interfaz de perímetro y su ubicación física en el Firewall ASA 5520. Se tiene la siguiente sintaxis:

Empresa FORTINET (config) # nameif ethernet0 outside sec0

Para la red interna se le asigna el nivel más alto de seguridad en una interfaz. Este nivel de seguridad es cien, se utiliza para la interfaz de acceso a clientes. Es la configuración predeterminada y no puede ser cambiada.

Empresa FORTINET (config) # nameif ethernet1 inside sec100

Para nuestro diseño conectaremos una interfaz de perímetro a la DMZ. Recuerde que la DMZ es un área aislada, separada del entorno interno y fiable. Se esta considerando un nivel de seguridad de 50 esto porque para la red externa (outside sec0) la DMZ es considerada como interna y para el nivel de seguridad de la red interna (inside sec100) la DMZ es considerada como externa.

Empresa FORTINET (config) # nameif ethernet2 inside sec50

Observe los niveles de seguridad en la figura 3 del **anexo A**.

Luego debemos utilizar el comando “interface” para configurar la velocidad de cada una de las interfaces y queden completamente activas, se tiene la siguiente sintaxis:

Empresa FORTINET (config) # interface ethernet0 100baset

Puede verificar la configuración de las tres interfaces revise la figura 1 del **anexo B**.

Ahora bien, cada una de las interfaces del Firewall ASA 5520 deberá estar configurada con una dirección IP y una mascara de red, si no se especifica una mascara de red, se supondrá la mascara de red con clase A: 255.0.0.0, clase B: 255.255.0.0, clase C: 255.255.255.0.

En nuestro diseño las direcciones IP son las siguientes: 10.0.1.1 para la red interna, 172.16.1.1 para la DMZ, 192.168.1.2 para la red externa.

Para la distribución de las direcciones observe la figura 2 del **anexo B**. La configuración para cada una de las interfaces lo realizaremos con el comando “ip address”, se tendrá la siguiente sintaxis:

Empresa FORTINET (config) # ip address inside 10.0.1.1 255.255.255.0

Recuerde que esta configuración la realizara con las tres direcciones IP. Para que verifique la configuración revise la figura 3 en el **anexo B**.

Para que el Firewall ASA 5520 pueda encaminar el flujo de datos dado que también hace funciones de router, configuraremos una ruta estática por defecto al router de Internet con coste 1 y lo realizaremos con el comando route y tiene la siguiente sintaxis:

Empresa FORTINET (config) # route outside 0.0.0.0 0.0.0.0 192.168.1.1 1

La traducción de direcciones de red (NAT) es un recurso que implantaremos a nuestro diseño de red con la finalidad de que impida que las redes externas conozcan las direcciones IP internas (aquellas que se encuentran detrás del Firewall ASA 5520).

Por ejemplo, cuando se conecta con Internet o con otra red externa, el comando “nat “ lleva a cabo este proceso convirtiendo las direcciones IP internas y no registradas, que no tienen que ser únicas a nivel global, en direcciones IP registradas y globalmente aceptadas antes de que los paquetes sean reenviados a la red externa.

También implantaremos el recurso del comando “global” que definirá la dirección o intervalo de direcciones en que se convertirá la dirección de origen.

La siguiente sintaxis será para la configuración de la red interna respecto a la red externa y lo haremos con identificativo "1":

Empresa FORTINET (config) # nat (inside) 1 10.0.1.0 255.255.255.0
Empresa FORTINET (config) # global (outside) 1 192.168.1.200-192.168.1.254 netmask 255.255.255.0

Aunque la mayoría de las conexiones tiene lugar desde una interfaz provista de un nivel de seguridad alto hasta una interfaz provista de un nivel de seguridad bajo, existen circunstancias que requieren que haya conexiones desde una interfaz provista de un nivel de seguridad bajo hasta una interfaz provista de un nivel de seguridad alto, para esto utilizamos el comando "static".

En otras palabras se usa para hacer que las direcciones IP de las interfaces de nivel de seguridad alto estén accesibles para los dispositivos de nivel de seguridad bajo. Para nuestro diseño el servidor Web, Mail y FTP tienen que ser accesibles desde Internet para lograrlo se configura de la siguiente forma:

Empresa FORTINET (config) # static (inside, outside) 204.69.198.3 172.16.1.2 netmask 255.255.255.255 0 0

Aplicamos el comando "acces-list 100" para la interfaz de salida:

Empresa FORTINET (config) # access-group 100 in interface outside

Para verificar la configuración de los tres servidores vea la figura 1 del **anexo C**.

Hasta este momento se ha configurado el flujo de datos de la red interna a la red externa y el acceso a los servidores por parte de nuestra red, pero recuerde que también los usuarios del exterior necesitan los recursos que se encuentran en la DMZ también tiene que configurarlos.

La siguiente sintaxis será para la configuración de la red DMZ respecto a la red externa y lo haremos con identificativo "1":

Empresa FORTINET (config) # global (dmz) 1 172.16.1.200-172.16.1.254 netmask 255.255.255.0

Permitimos que se devuelvan las repuestas de ICMP con el comando "access-list 100" se tiene entonces la siguiente sintaxis:

Empresa FORTINET (config) # access-list 100 permit icmp any any echo-reply

Empresa FORTINET (config) # access-list 100 permit icmp any any time-exceeded
Empresa FORTINET (config) # access-list 100 permit icmp any any unreachable

Permitimos que todo el mundo se conecte a los servidores Web, Mail, FTP.

Empresa FORTINET (config) # access-list 100 permit tcp any host 204.69.198.3 eq www

Verifique los accesos de cada servidor el la figura 2 del **anexo C**.

Definimos las conversiones estáticas para que el servidor web, Mail, FTP, puedan ser accesibles desde Internet.

Empresa FORTINET (config) # static (inside, outside) 204.69.198.3 192.168.1.4 netmask 255.255.255.255 0 0

Verifique las tres configuraciones en la figura 3 del **anexo C**.

Aplicamos “access-list 100 interface” para la interfaz de salida.

Empresa FORTINET (config) # access-group 100 in interface outside

Por ultimo guardamos la configuracion:

Empresa FORTINET (config) # write memory

Una vez finalizado, las configuraciones deben quedar como se muestra en el **anexo D**.

La figura del diseño queda como se muestra en el **anexo E**.

CONCLUCIONES

Los Firewalls son dispositivos de gran ayuda, pero se requieren delimitar y determinar claramente las políticas de acceso para que realmente cumpla con su objetivo, las políticas de acceso son: políticas recomendables y genéricas que sirven para protegernos de los ataques más comunes.

Los Firewalls por sí mismos no son la solución a la implementación de seguridad en una red. La seguridad no es un concepto estático, una red no es segura una vez y ya lo será para siempre, se requiere de una vigilancia continua, y para ello requerimos de herramientas que nos faciliten ésta tarea. Podemos afirmar que en estos momentos el flujo de información de la red esta al nivel de lo que requiere en estos momentos la empresa FORTINET C.V.

Pero con el transcurrir del tiempo y los nuevos modos de ataque a la integridad y confidencialidad de la red es necesario mantener un monitoreo continuo y establecer en algunos casos nuevas políticas de acceso para que la seguridad de los enlaces a Internet sean lo mas seguro posibles.

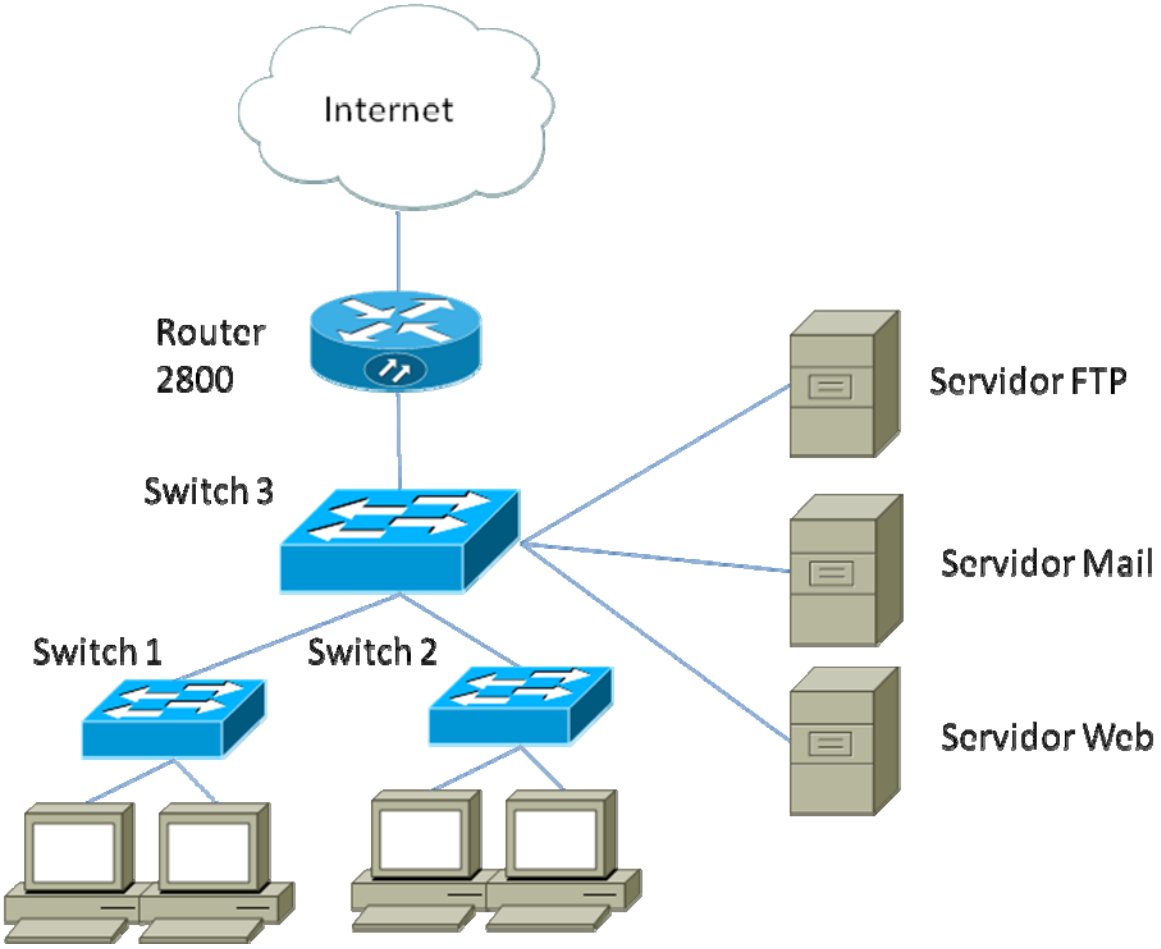
Faltan además otros mecanismos que hagan cumplir las políticas de seguridad deseadas, como la actualización y censo constante de los servidores Web, FTP, Email.

Debemos tener en cuenta que en la empresa FORTINET C.V. interactúan hombre-maquina y la responsabilidad de mantener la seguridad dentro de la misma no recae en su totalidad en el Firewall sino también en la responsabilidad y honestidad de quienes trabajan en su totalidad dentro de la empresa.

El trabajo que se presenta cumple con la primera etapa de seguridad en el interior de la empresa FORTINET C.V. Podemos mencionar que faltan otras etapas para que la administración y seguridad de la empresa este a un 100%, considerando este trabajo como un buen comienzo y un gran paso hacia un mejor funcionamiento de la red.

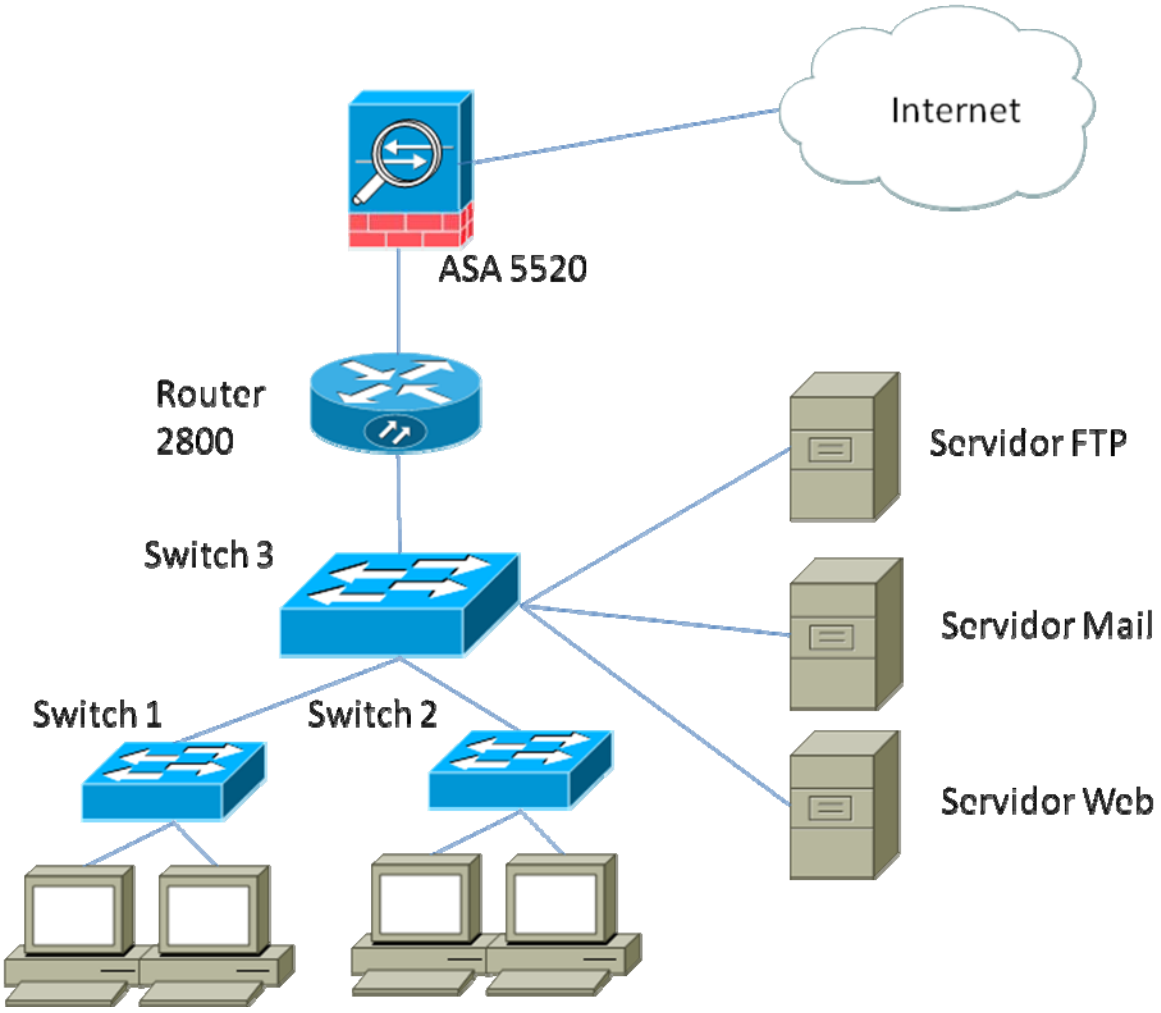
ANEXO A

FIGURA 1 "SITUACION ACTUAL"



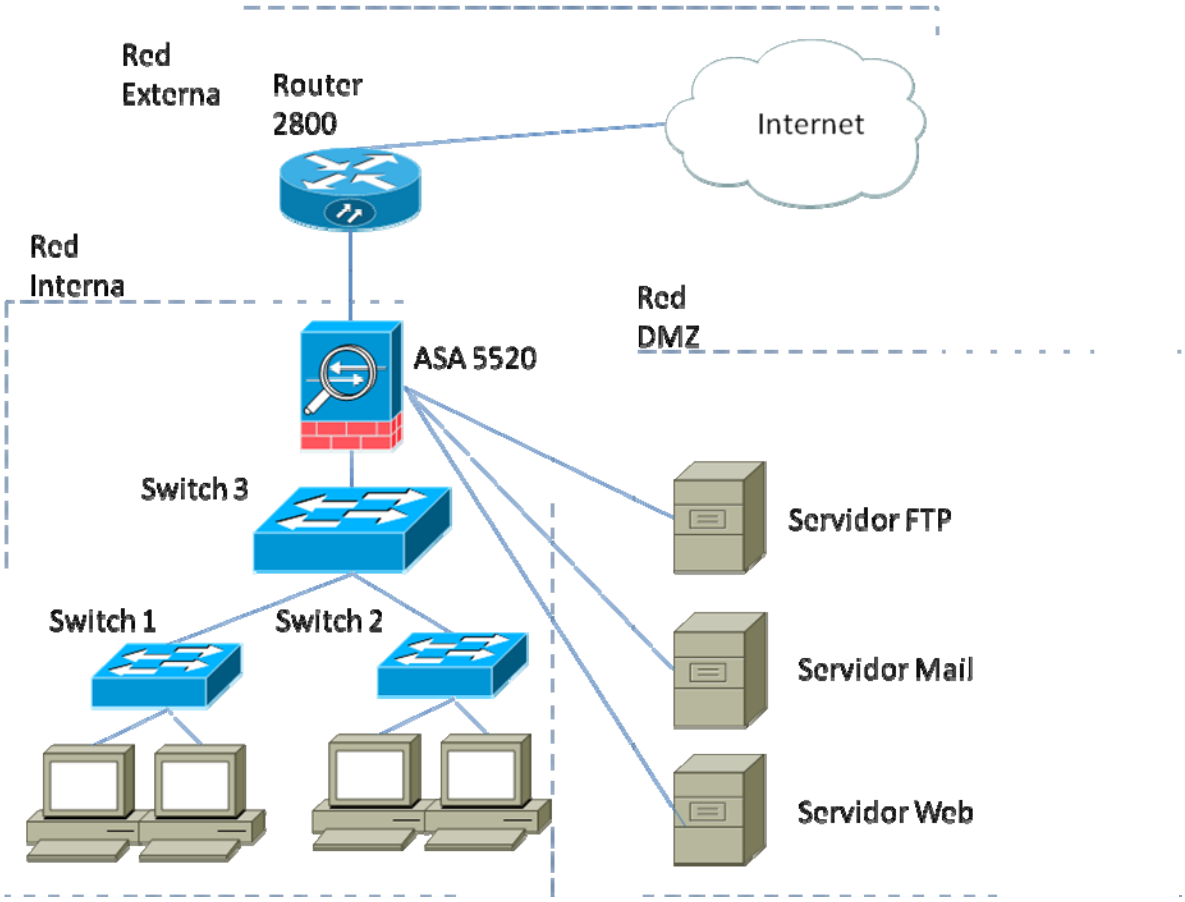
ANEXO A (CONTINUACION)

FIGURA 2 "DISEÑO DE RED CON EL FIREWALL ASA 5520"



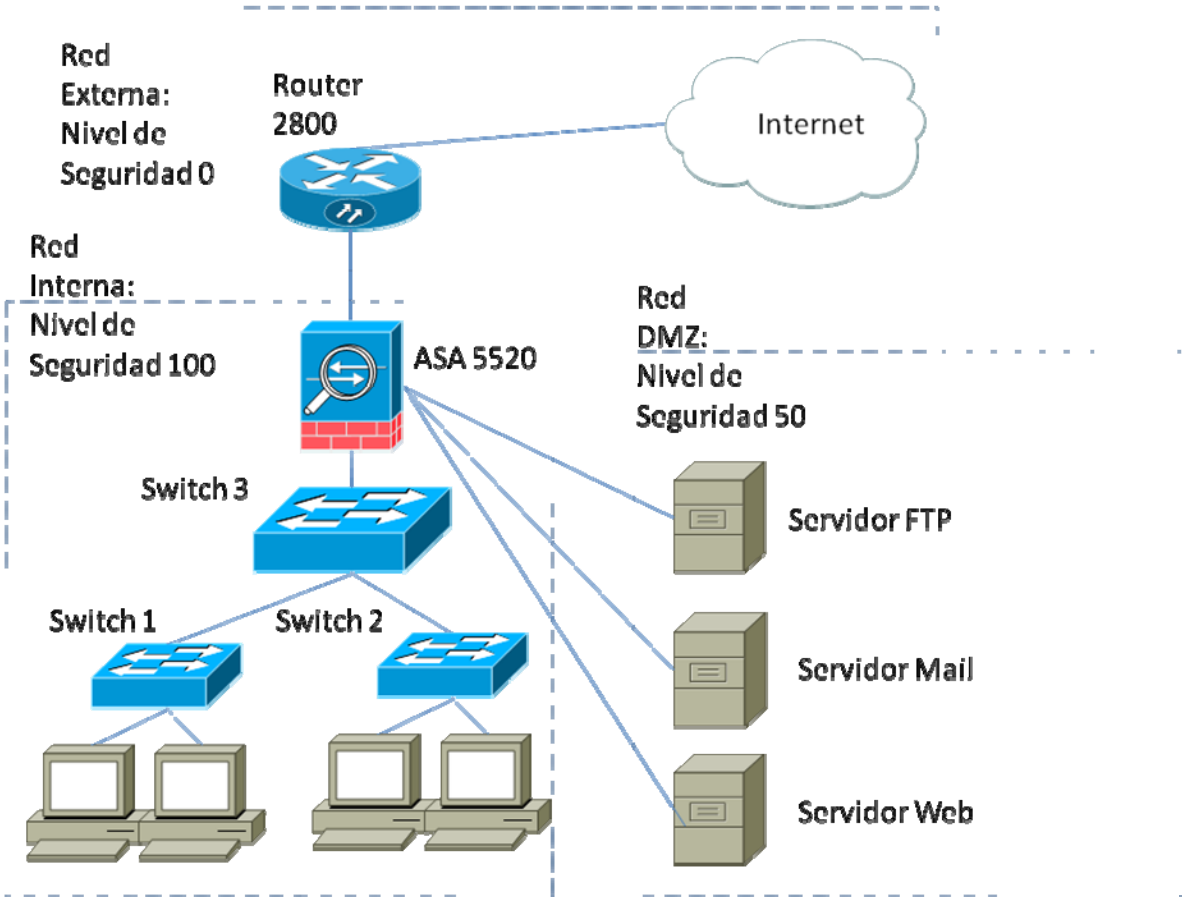
ANEXO A (CONTINUACION)

FIGURA 3 "DESCRIPCION DE LAS TRES REDES QUE CREA EL FIREWALL ASA 5520".



ANEXO A (CONTINUACION)

FIGURA 4 "NIVELES DE SEGURIDAD EN EL FIREWALL ASA 5520"



ANEXO B

FIGURA 1 "CONFIGURACION DE LAS INTERFACES CON EL COMANDO INTERFACE"

```
Empresa (config)# interface  ethernet0  100baset

Empresa (config)# interface  ethernet1  100baset

Empresa (config)# interface  ethernet2  100baset
```

FIGURA 2 "CONFIGURACION DE LAS INTERFACES CON EL COMANDO IP ADDRESS".

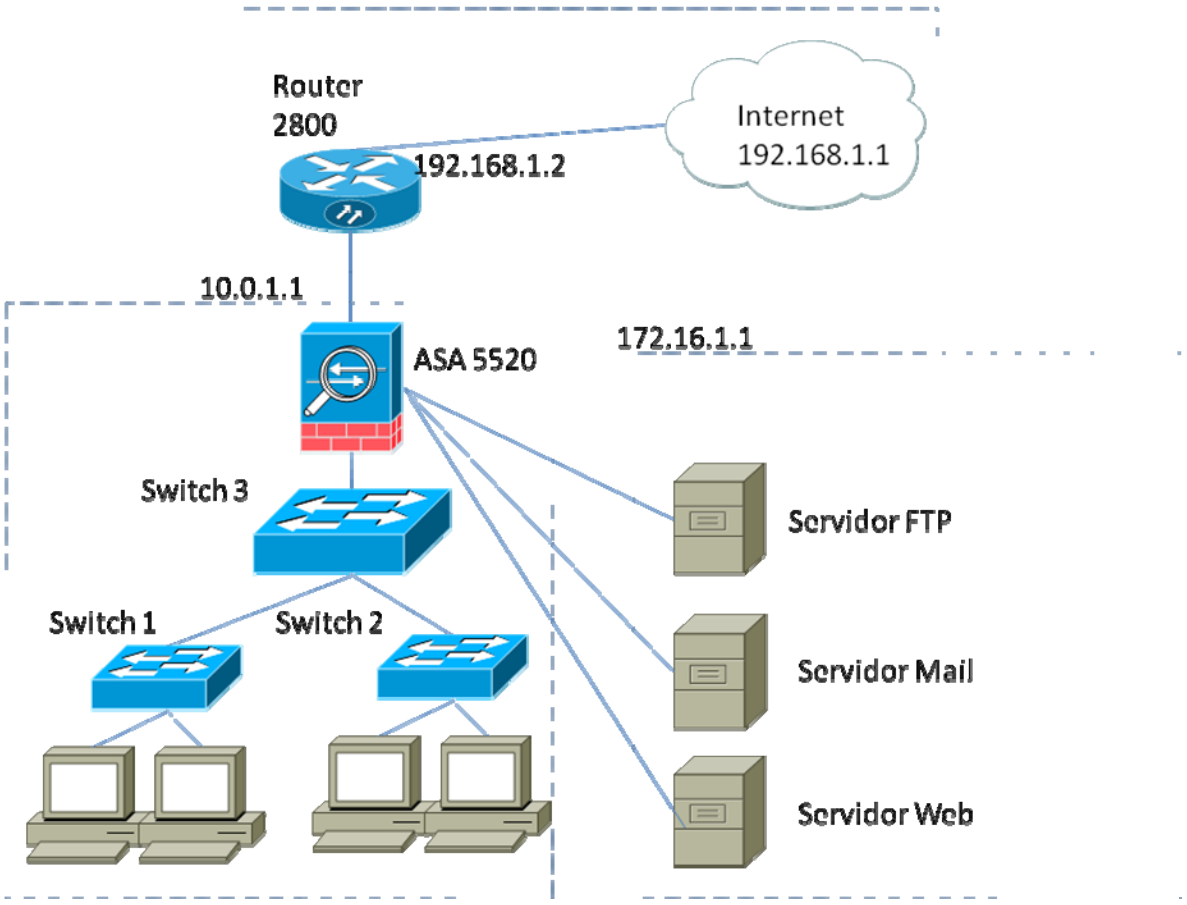
```
Empresa (config)# ip address inside 10.0.1.1 255.255.255.0

Empresa (config)# ip address dmz 192.16.0.1 255.255.255.0

Empresa (config)# ip address outside 192.168.1.2 255.255.255.0
```

ANEXO B (CONTINUACION)

FIGURA 3 "DISTRIBUCION DE DIRECCIONES IP EN EL DISEÑO DE RED"



ANEXO C

FIGURA 1 “CONFIGURACION DE CONVERSIONES ESTATICAS PARA QUE LOS TRES SERVIDORES SEAN ACCESIBLES DESDE INTERNET (INSIDE-OUTSIDE)”.

Empresa FORTINET (config)# static (inside,outside) 204.69.198.3 172.16.1.2 netmask 255.255.255.255 0 0

Empresa FORTINET (config)# static (inside,outside) 204.69.198.4 172.16.1.5 netmask 255.255.255.255 0 0

Empresa FORTINET (config)# static (inside,outside) 204.69.198.5 172.16.1.9 netmask 255.255.255.255 0 0

FIGURA 2 “CONFIGURACION PARA PERMITIR EL ACCESO DEL EXTERIOR A LOS SERVIDORES”.

Empresa FORTINET (config)# access−list 100 permit tcp any host 204.69.198.3 eq www

Empresa FORTINET (config)# access−list 100 permit tcp any host 204.69.198.4 eq smtp

Empresa FORTINET (config)# access−list 100 permit tcp any host 204.69.198.5 eq ftp

FIGURA 3 “CONFIGURACION DE CONVERSIONES ESTATICAS PARA QUE LOS TRES SERVIDORES SEAN ACCESIBLES DESDE INTERNET (INSIDE-DMZ)”.

Empresa (config)# static (inside,outside) 204.69.198.3 192.168.1.4 netmask 255.255.255.255 0 0

Empresa (config)# static (inside,outside) 204.69.198.4 192.168.1.15 netmask 255.255.255.255 0 0

Empresa (config)# static (inside,outside) 204.69.198.5 192.168.1.10 netmask 255.255.255.255 0 0

ANEXO D

CONFIGURACION DEL FIREWALL ASA 5520 PARA EL DISEÑO DE RED IMPLEMENTADO.

```
ASA 5520 Version 6.3(3)
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
hostname ASA 5520
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
name 172.16.1.2 bastionhost
name 10.0.1.11 insidehost
access-list outside_access_in permit icmp any any
access-list outside_access_in permit tcp any host 192.168.1.11 eq telnet
mtu outside 1500
mtu inside 1500
mtu dmz 1500
ip address outside 192.168.1.2 255.255.255.0
ip address inside 10.0.1.1 255.255.255.0
ip address dmz 172.16.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
```

```
global (outside) 1 192.168.1.200-192.168.1.254 netmask 255.255.255.0
global (dmz) 1 172.16.1.200-172.16.1.254 netmask 255.255.255.0
nat (inside) 1 10.0.1.0 255.255.255.0 0 0
static (dmz,outside) 192.168.1.11 bastionhost netmask 255.255.255.255 0 0
static (inside,outside) 192.168.1.10 insidehost netmask 255.255.255.255 0 0
```

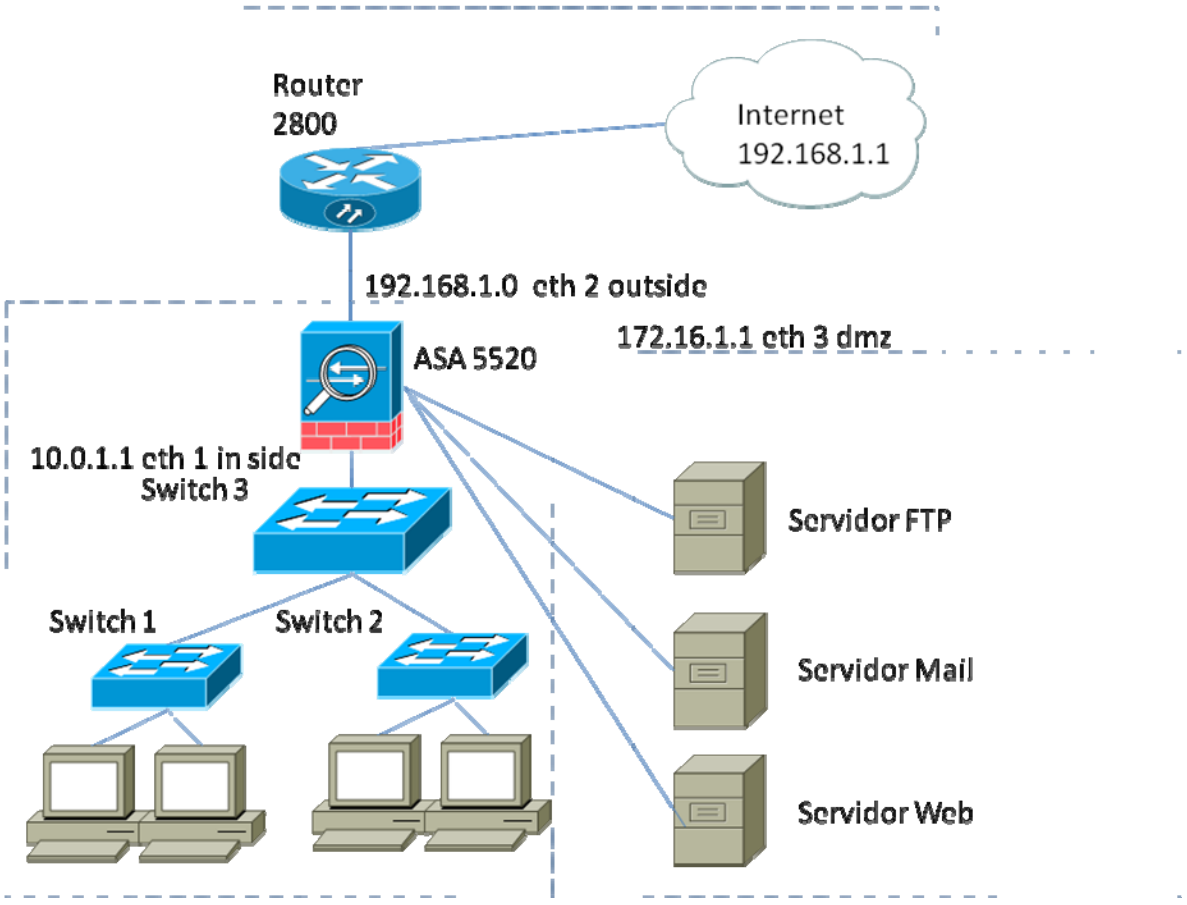
ANEXO D (CONTINUACION).

CONFIGURACION DEL FIREWALL ASA 5520 PARA EL DISEÑO DE RED IMPLEMENTADO (CONTINUACION).

```
access-group outside_access_in in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
```

ANEXO E

"DISEÑO DE RED CON EL FIREWALL ASA 5520 Y SUS DIRECCIONAMIENTOS CORRESPONDIENTES"



ÍNDICE DE FIGURAS

CAPITULO I

Figura 1.1 Red LAN. 2
Figura 1.2 Red WAN. 3
Figura 1.3 Red MAN. 4
Figura 1.4 Topología en Bus. 5
Figura 1.5 Topología en Anillo. 5
Figura 1.6 Topología en Estrella. 6
Figura 1.7 Topología Jerárquica. 6
Figura 1.8 Topología en Malla. 6
Figura 1.9 Funciones en cada nivel del modelo OSI. 9
Figura 1.10 Protocolos en función de Windows NT e Internet. 12
Figura 1.11 Protocolos en función de Netware y Apple. 13
Figura 1.12 Protocolos MAC y LLC en capa 2. 14
Figura 1.13 Transmisión en el modelo OSI. 23
Figura 1.14 Comparación de TCP/IP y OSI. 28

CAPITULO II

Figura 2.1 Trama Ethernet. 35
Figura 2.2 Conexión de conmutación por circuitos (izquierda) frente a de conmutación por paquetes (derecha). 38

CAPITULO III

Figura 3.1 Filtro de paquetes. 43
Figura 3.2 Función de la VPN. 47
Figura 3.3 Traslado de datos en la VPN. 47
Figura 3.4 Alcance en enlace de la VPN. 48
Figura 3.5 Red de transito de la VPN. 48

CAPITULO IV

Figura 4.1 Firewall típico entre red local e Internet. 56
Figura 4.2 Firewall entre red local e Internet con zona DMZ para servidores expuestos. 56
Figura 4.3 Firewall filtra paquetes. 59
Figura 4.4 Firewall a nivel de aplicación. 60
Figura 4.5 Firewall a nivel de aplicación. 60
Figura 4.6 Firewall a nivel de red. 62
Figura 4.7 Firewall a nivel de red (red mas efectiva que la anterior). 62
Figura 4.8 Firewall a nivel de circuito. 63

BIBLIOGRAFIA

David W. Chapman Jr.
Andy Fox
"Firewall ASA 5520 de CISCO Secure"
Pearson Educación, S.A. España 2005.

Academia de Networking de Cisco Systems.
"Guia del primer año CCNA 1 y 2"
Pearson Educación, S.A. Madrid 2004.

León García Alberto
Widjaja Indra
"Redes de Comunicación",
Ed. Mc Graw Hill. MEXICO 2008

http://es.wikipedia.org/wiki/Man.

http://ciberhabitat.gob.mx

http://ditec.um.es/laso/docs/tut-tcp/ip/3376c49.html

http://www.ignside.net/man/redes/protocolos.php

http://www.ignside.net/man/redes/tcp_ip_basico.php