UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

"PREVENCIÓN DE ATAQUES HACIA UNA RED INTERNA MEDIANTE LA IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL"

T E S I S

QUE PARA OBTENER EL TITULO DE

INGENIERO MECÁNICO ELÉCTRICISTA.

P R E S E N T A :

MARCO ANTONIO BASILIO TADEO.
EDGAR ROBERTO VARELA ALVARADO.

ASESOR: ING. BENITO BARRANCO CASTELLANOS

Estado de México **Septiembre 2010.**

"PREVENCIÓN DE ATAQUES HACIA UNA RED INTERNA MEDIANTE LA IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL"

OBJETIVO.

Conocer de manera general los aspectos más importantes relacionados con la seguridad en redes e internet considerando tanto aspectos técnicos como operativos. Unificando los parámetros básicos necesarios para el conocimiento de los principales ataques existentes.

INTRODUCCIÓN.

Seguridad informática

La seguridad informática se encarga de proteger la información, más específicamente, podemos definir que lo logrará preservando su:

Confidencialidad.

Disponibilidad.

Integridad.

Autenticidad.

La mayoría de las empresas sufren la problemática de seguridad debido a sus necesidades de acceso y conectividad con:

Internet.

Conectividad mundial.

Red corporativa.

Acceso Remoto.

Proveedores.

Se deberían proteger todos los elementos de la red interna, incluyendo hardware, software e información, no solo de cualquier intento de acceso no autorizado desde el exterior sino también de ciertos ataques desde el interior que puedan proveerse y prevenirse.

¿Cómo protegerlos?

Paradigmas de seguridad:

Lo que no se prohíbe expresamente está permitido.

Lo que no se permite expresamente está prohibido.

Métodos de defensa:

En profundidad.

Perimetral.

Seguridad Perimetral.

La seguridad perimetral es uno de los métodos posibles de defensa de una red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles.

Esto nos permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

El objetivo de todo ataque informático, entendiendo como ataque hackear un sistema, es utilizar alguna vulnerabilidad existente en un programa para lograr llevar a cabo una acción que en un principio no se nos estaba permitida. Con esta definición se está dejando fuera a cualquier tipo de DoS[1]. En la mayoría de los casos el objetivo será lograr llevar a cabo una acción bajo un nivel de privilegio superior, siendo habitual en un escenario de ataque típico, la utilización de varias técnicas con el fin de escalar de un nivel de privilegio a otro hasta llegar al nivel de superusuario (root).

Las técnicas de ataque que veremos no están restringidas a ningún sistema operativo especifico y pueden ser aplicadas desde en un Solaris[2] hasta en un Windows (a excepción de en los format strings[3]). Casi todas las técnicas de ataque se fundamentan en lo mismo, una falta de validación de los datos

---

[1] **DoS.** Es una familia de sistemas operativos para PC. El nombre son las siglas de Disk Operating System (sistema operativo de disco). Fue creado originalmente para computadoras de la familia IBM PC, que utilizaban los procesadores Intel 8086 y 8088, de 16 bits, siendo el primer sistema operativo popular para esta plataforma. Contaba con una interfaz de línea de comandos en modo texto o alfanumérico, vía su propio intérprete de órdenes, command.com. Probablemente la más popular de sus variantes sea la perteneciente a la familia MS-DOS, de Microsoft, suministrada con buena parte de los ordenadores compatibles con IBM PC, en especial aquellos de la familia Intel, como sistema operativo independiente o nativo, hasta la versión 6.22 (bien entrados los 90), frecuentemente adjunto a una versión de la interfaz gráfica Ms Windows de 16 bits, como las 3.1x.

[2] **Solaris.** Es un sistema operativo de tipo Unix desarrollado desde 1992 inicialmente por Sun Microsystems y actualmente por Oracle Corporation como sucesor de SunOS. Es un sistema certificado oficialmente como versión de Unix. Funciona en arquitecturas SPARC y x86 para servidores y estaciones de trabajo.

[3] **El método To String** puede aceptar un parámetro de cadena que indica el objeto cómo dar formato a sí mismo. En la llamada a String. Format, la cadena de formato se pasa después de la posición, por ejemplo, "(0 :##}". The El texto dentro de las llaves es ([argument Index, la alineación]).

Si la alineación es positivo, el texto se haga el relleno para cubrir la longitud del campo especificado, si es negativo, es la izquierda para ajustarla.

introducidos por el usuario. Es muy importante que como programadores nunca nos fiemos de los datos introducidos por el usuario. Cuando hablamos de datos introducidos por el usuario se refiere a cualquier dato suministrado por el usuario que sea susceptible de ser procesado por nuestro programa. Datos introducidos por el usuario podrían ser los datos introducidos por consola en las lecturas

En muchos textos y manuales sobre Seguridad Informática se habla de la seguridad física concerniente a la ubicación de los servidores, los accesos físicos a las máquinas, etc. Aunque es seguridad relacionada con la informática, esas medidas son más propias de un ingeniero o arquitecto que diseñe edificios seguros, que de un especialista en Seguridad Informática. (Ejemplo: poco tiene que ver con la protección informática el hecho de que se haya decidido ubicar el servidor de la empresa en la sala en la que toman café los empleados en sus descansos. Una computadora es un componente físico y debería estar sujeto a las mismas medidas de seguridad que el resto de materiales valiosos de una organización).

Como ejemplos de las posibilidades en cuanto a intrusismo a nivel físico, analizaremos dos aspectos:

El cifrado de datos almacenados en soporte físico, captura de emisiones residuales de nuestros equipos (tempest[4]). A pesar de todas las trabas que podamos poner para que un soporte no sea físicamente suplantado o robado, la realidad es que muchos ataques se producen mediante la manipulación física de los soportes de los datos. (Ejemplo: montar un disco duro desde un Sistema Operativo al que tenemos acceso total (trinux)).

Para evitar este tipo de ataque es recomendable cifrar los datos. Una opción comercial para hacer esto es usar PGPDisk, integrada en la Suite PGP de NAI. Para UNIX tenemos CFS y TCFS (Cyphered File System y Transparent Cyphered

[4] **TEMPEST** es un nombre en clave referido a diversos estudios e investigaciones acerca de emanaciones comprometedoras (señales electromagnéticas, acústicas, mecánicas, etc.) que emiten los equipos eléctricos y electrónicos, y que, si son interceptadas y analizadas, pueden revelar información transmitida, recibida o, en general, procesada por dichos equipos.
El término TEMPEST fue acuñado a finales de los años 60 y principios de los 70 por la NSA en el marco de una operación destinada a la creación de un conjunto de estándares que protegieran los equipos de comunicaciones electrónicas de posibles espías, así como al desarrollo de métodos para interceptar e interpretar señales ajenas. El gobierno de los Estados Unidos ha indicado que dicho término no es un acrónimo y que no tiene un significado en particular.

File System), que ofrecen una encriptación fuerte mediante el empleo de llaves distribuidas (cada usuario tiene una parte de la llave, y se comprueba que su parte está dentro de la llave de protección).

El caso más espectacular en cuanto a cifrado de datos físicos es el de los sistemas de ficheros esteganográficos[5], como el StegFS. En estos sistemas de protección existen varias claves que permiten el acceso a varios niveles de protección dentro del sistema de ficheros. Alguien que consiga una de las claves, nunca tendrá la certeza de que está accediendo a todos los sistemas de ficheros o sólo a una parte. De esta manera, aunque alguien fuerce a otro a proporcionarle la clave del sistema (Ejemplo: escenario policial), nunca podrá saber si a lo que está accediendo es a una parte del sistema o a todo.

Existen varias implementaciones más extrañas de sistemas de ficheros esteganográficos, como el ScreamFS, que guarda información confidencial en los bits menos significativos de ficheros de audio.

Otro punto que puede sorprender a quien no esté habituado a sistemas seguros es el hecho de que las radiaciones que emiten todos los dispositivos electrónicos, pueden capturarse y analizarse.

Un programa de ejemplo muy impactante es el Tempest. Mediante cambios en la frecuencia del monitor y utilizando imágenes extrañas, es capaz de emitir música que puede ser captada por una radio AM sencilla.

Nosotros hemos hecho la prueba en nuestros ordenadores y el resultado es sorprendente. Tempest es sólo una prueba de concepto, pero demuestra que lo que muestran nuestros monitores puede ser captado sin mucho esfuerzo por un

---

5 **La esteganografía** es la disciplina en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia. Es una mezcla de artes y técnicas que se combinan para conformar la práctica de ocultar y enviar información sensible en un portador que pueda pasar desapercibido.

Si bien la esteganografía suele confundirse con la criptografía, por ser ambas parte de los procesos de protección de la información, son disciplinas bastante distintas, tanto en su forma de implementar como en su objetivo mismo. Mientras que la criptografía se utiliza para cifrar o codificar información de manera que sea ininteligible para un probable intruso, a pesar del conocimiento de su existencia, la esteganografía oculta la información en un portador de modo que no sea advertida el hecho mismo de su existencia y envío. De esta última forma, un probable intruso ni siquiera sabrá que se está transmitiendo información sensible.

Sin embargo, la criptografía y la esteganografía pueden complementarse, dando un nivel de seguridad extra a la información, es decir, es muy común (aunque no imprescindible) que el mensaje a esteganografiar sea previamente cifrado, de tal modo que a un eventual intruso no sólo le costará advertir la presencia misma de la mensajería oculta, sino que si la llegara a obtener, la encontraría cifrada.

receptor potente. Tempest permite incluso reproducir MP3s desde el monitor, pero existen además dispositivos capaces de captar las corrientes de 5 voltios que discurren por el cable del teclado, u otros dispositivos.

Quizá en estos momentos el nivel de paranoia esté creciendo y a más de uno se le está ocurriendo forrar de plomo su habitación, conforme vayamos avanzando en los contenidos de esta tesis veremos como toda protección es poca.

CAPÍTULO 1.
REDES

1.1 Un mundo centrado en la red.

En la actualidad nos encontramos en un momento decisivo respecto del uso de la tecnología para extender y potenciar nuestra red humana. La globalización de Internet se ha producido más rápido de lo que cualquiera hubiera imaginado. El modo en que se producen las interacciones sociales, comerciales, políticas y personales cambia en forma continua para estar al día con la evolución de esta red global. En la próxima etapa de nuestro desarrollo, los innovadores usarán Internet como punto de inicio para sus esfuerzos, creando nuevos productos y servicios diseñados específicamente para aprovechar las capacidades de la red. Mientras los desarrolladores empujan los límites de lo posible, las capacidades de las redes interconectadas que forman Internet tendrán una función cada vez más importante en el éxito de esos proyectos.

Este capítulo presenta la plataforma de las redes de datos, de las cuales dependen cada vez más nuestras relaciones sociales y de negocios. El material presenta las bases para explorar los servicios, las tecnologías y los problemas que enfrentan los profesionales de red mientras diseñan, desarrollan y mantienen la red moderna.

Entre todos los elementos esenciales para la existencia humana, la necesidad de interactuar está por debajo de la necesidad de sustentar la vida. La comunicación es casi tan importante para nosotros como el aire, el agua, los alimentos y un lugar para vivir.

Los métodos que utilizamos para compartir ideas e información están en constante cambio y evolución. Mientras la red humana estuvo limitada a conversaciones cara a cara, el avance de los medios ha ampliado el alcance de nuestras comunicaciones. Desde la prensa escrita hasta la televisión, cada nuevo desarrollo ha mejorado la comunicación.

Al igual que con cada avance en la tecnología de comunicación, la creación e interconexión de redes de datos sólidas tiene un profundo efecto.

Las primeras redes de datos estaban limitadas a intercambiar información basada en caracteres entre sistemas informáticos conectados. Las redes actuales evolucionaron para agregarle voz, flujos de video, texto y gráficos, a los diferentes tipos de dispositivos (Fig.1.1). Las formas de comunicación anteriormente individuales y diferentes se unieron en una plataforma común. Esta plataforma proporciona acceso a una amplia variedad de métodos de comunicación alternativo y nuevo que permiten a las personas interactuar directamente con otras en forma casi instantánea.

La naturaleza inmediata de las comunicaciones en Internet alienta la formación de comunidades globales. Estas comunidades motivan la interacción social que depende de la ubicación o el huso horario.

Es increíble la rapidez con la que Internet llegó a ser una parte integral de nuestra rutina diaria. La compleja interconexión de dispositivos y medios electrónicos que abarca la red es evidente para los millones de usuarios que hacen de ésta una parte personal y valiosa de sus vidas.

Las redes de datos que fueron alguna vez el transporte de información entre negocios se replanificaron para mejorar la calidad de vida de todas las personas. En el transcurso del día, los recursos disponibles en Internet pueden ayudarlo a:

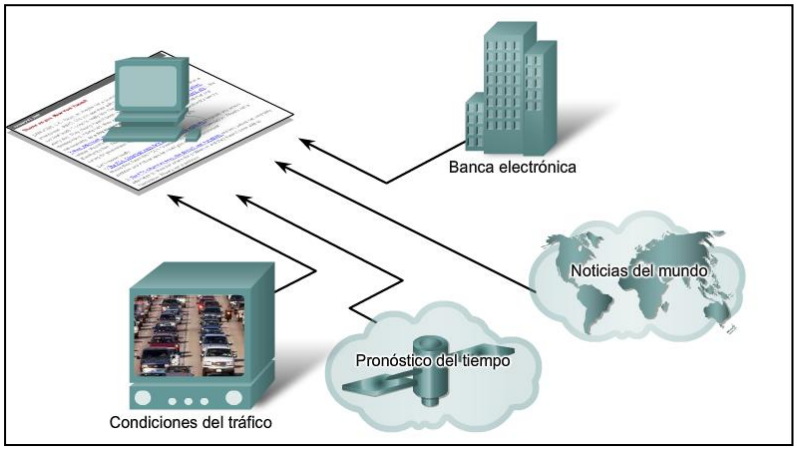


Fig.1.1 La forma en que vivimos está respaldada por servicios provistos por la red de datos.

- decidir cómo vestirse consultando en línea las condiciones actuales del clima,
- Buscar el camino menos congestionado hacia su destino observando vídeos de cámaras Web que muestran el clima y el tráfico,
- Consultar su estado de cuenta bancario y pagar electrónicamente las boletas,
- Recibir y enviar correo electrónico o realizar una llamada telefónica a través de Internet durante el almuerzo en un bar con Internet,
- Obtener información sobre la salud y consejos sobre nutrición de parte de expertos de todo el mundo y compartir en un foro esa información o tratamientos,
- Descargar nuevas recetas y técnicas de cocina para crear cenas fabulosas, o
- Enviar y compartir sus fotografías, vídeos caseros y experiencias con amigos o con el mundo.

1.2 Redes que respaldan la forma en que trabajamos.

En principio, las empresas utilizaban redes de datos para registrar y administrar internamente la información financiera, la información del cliente y los sistemas de nómina de empleados. Las redes comerciales evolucionaron para permitir la transmisión de diferentes tipos de servicios de información, como e-mail, video, mensajería y telefonía.

Las intranets, redes privadas utilizadas sólo por una empresa, les permiten comunicarse y realizar transacciones entre empleados y sucursales globales. Las compañías desarrollan extranets o internetwork extendidas para brindarles a los proveedores, fabricantes y clientes acceso limitado a datos corporativos para verificar estados, inventario y listas de partes.

En la actualidad, las redes ofrecen una mayor integración entre funciones y organizaciones relacionadas que la que era posible en el pasado.

La adopción generalizada de Internet por las industrias de viaje y entretenimiento mejora la posibilidad de disfrutar y compartir diferentes formas de recreación, sin

importar la ubicación. Es posible explorar lugares en forma interactiva que antes soñábamos visitar, como también prever los destinos reales antes de realizar un viaje. Los detalles y las fotografías de estas aventuras pueden publicarse en línea para que otros los vean.

Internet también se utiliza para formas tradicionales de entretenimiento. Escuchamos artistas grabados, vemos o disfrutamos de avances de películas, leemos libros completos y descargamos material para acceder luego sin conexión. Los eventos deportivos y los conciertos en vivo pueden presenciarse mientras suceden, o grabarse y verse cuando lo desee.

Las redes permiten la creación de nuevas formas de entretenimiento, como los juegos en línea. Los jugadores participan en cualquier clase de competencia en línea que los diseñadores de juegos puedan imaginar. Competimos con amigos y adversarios de todo el mundo como si estuviéramos en la misma habitación.

Incluso las actividades sin conexión son mejoradas con los servicios de colaboración en red cómo se muestra en la Fig.1.2. Las comunidades globales de interés han crecido rápidamente. Compartimos experiencias comunes y hobbies fuera de nuestro vecindario, ciudad o región. Los fanáticos del deporte comparten opiniones y hechos sobre sus equipos favoritos. Los coleccionistas muestran valiosas colecciones y reciben comentarios de expertos.

Los mercados y los sitios de subasta en línea brindan la oportunidad de comprar, vender y comercializar todo tipo de mercancía.

En la red humana podemos disfrutar cualquier forma de recreación, las redes mejoran nuestra experiencia.

Fig.1.2 servicios provistos por la red de datos.

1.3. Elementos de una red.

La Fig.1.3 muestra los elementos de una red típica, incluyendo dispositivos, medios y servicios unidos por reglas, que trabajan en forma conjunta para enviar mensajes. Utilizamos la palabra mensajes como un término que abarca las páginas Web, los e-mails, los mensajes instantáneos, las llamadas telefónicas y otras formas de comunicación permitidas por Internet. En este curso, aprenderemos acerca de una variedad de mensajes, dispositivos, medios y servicios que permiten la comunicación de esos mensajes. Aprenderemos además sobre las reglas o protocolos que unen a estos elementos de red.

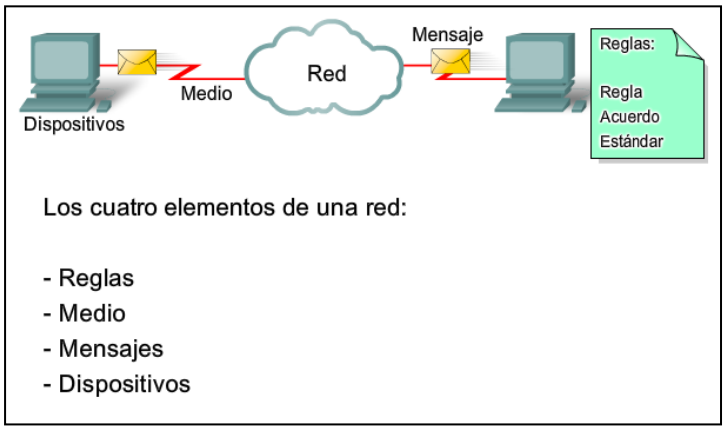


Fig.1.3 Elementos de una red.

La interconexión de redes es un tema orientado gráficamente y los íconos se utilizan comúnmente para representar sus dispositivos como se muestra en la Fig.1.4. En la parte izquierda del diagrama se muestran algunos dispositivos comunes que generalmente originan mensajes que constituyen nuestra comunicación. Esto incluye diversos tipos de equipos (se muestran íconos de una computadora de escritorio y de una portátil), servidores y teléfonos IP. En las redes de área local, estos dispositivos generalmente se conectan a través de medios LAN (con cables o inalámbricos).

El lado derecho de la figura muestra algunos de los dispositivos intermedios más comunes, utilizados para direccionar y administrar los mensajes en la red, como así también otros símbolos comunes de interconexión de redes. Los símbolos genéricos se muestran para:

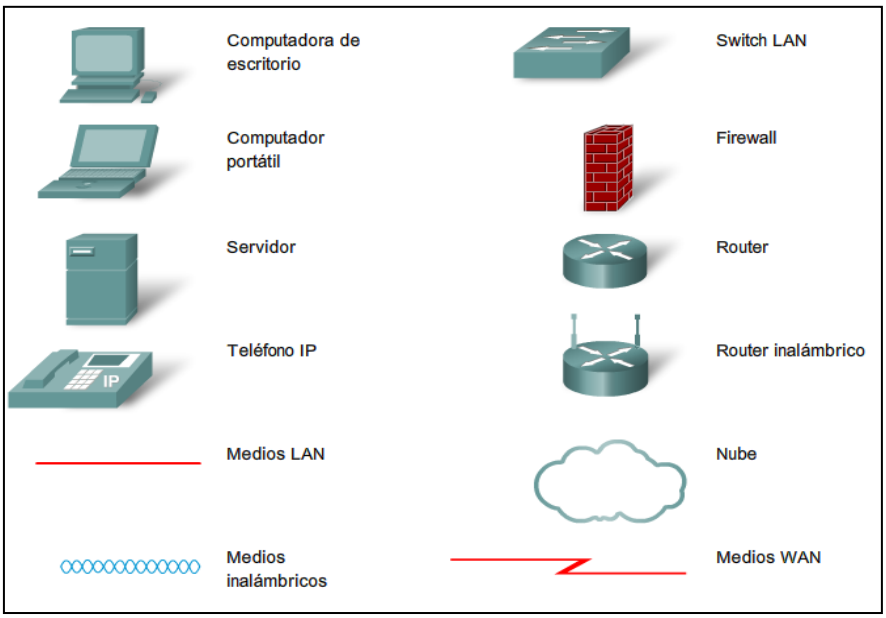


Fig.1.4 Símbolos comunes de las redes de datos.

- Switch: el dispositivo más utilizado para interconectar redes de área local,
- Firewall: proporciona seguridad a las redes,
- Router: ayuda a direccionar mensajes mientras viajan a través de una red,
- Router inalámbrico: un tipo específico de router que generalmente se encuentra en redes domésticas,
- Nube: se utiliza para resumir un grupo de dispositivos de red, sus detalles pueden no ser importantes en este análisis,
- Enlace serial: una forma de interconexión WAN (Red de área extensa), representada por la línea en forma de rayo.

Para que funcione una red, los dispositivos deben estar interconectados. Las conexiones de red pueden ser con cables o inalámbricas. En las conexiones con cables, el medio puede ser cobre, que transmite señales eléctricas, o fibra óptica, que transmite señales de luz. En las conexiones inalámbricas, el medio es la atmósfera de la tierra o espacio y las señales son microondas. Los medios de cobre incluyen cables, como el par trenzado del cable de teléfono, el cable coaxial o generalmente conocido como cable de par trenzado no blindado (UTP) de Categoría 5e y/o 6. Las fibras ópticas, hebras finas de vidrio o plástico que

transmiten señales de luz, son otra forma de medios de networking. Los medios inalámbricos incluyen conexiones inalámbricas domésticas entre un router inalámbrico y una computadora con una tarjeta de red inalámbrica, ver Fig.1.5, conexión inalámbrica terrestre entre dos estaciones de tierra o comunicación entre dispositivos en tierra y satélites. En un viaje típico a través de Internet, un mensaje puede viajar en una variedad de medios.

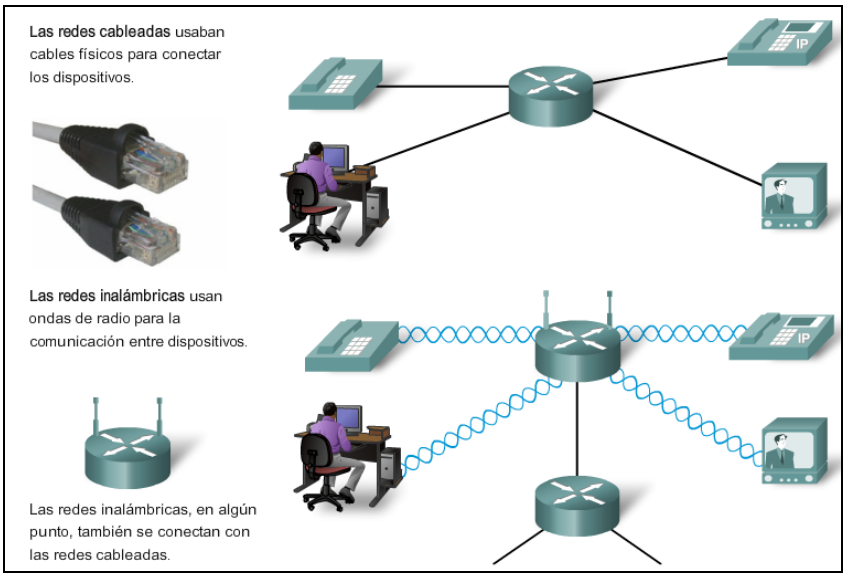


Fig.1.5 Conexiones de red.

Las personas generalmente buscan enviar y recibir distintos tipos de mensajes a través de aplicaciones informáticas; estas aplicaciones necesitan servicios para funcionar en la red. Algunos de estos servicios incluyen World Wide Web, e-mail, mensajería instantánea y telefonía IP. Los dispositivos interconectados a través de medios para proporcionar servicios deben estar gobernados por reglas o protocolos. En el cuadro se enumeran algunos servicios y un protocolo vinculado en forma más directa con ese servicio.

Los protocolos son las reglas que utilizan los dispositivos de red para comunicarse entre sí. Actualmente el estándar de la industria en redes es un conjunto de protocolos denominado TCP/IP (Protocolo de control de transmisión/Protocolo de Internet). TCP/IP se utiliza en redes comerciales y domésticas, siendo también el protocolo primario de Internet. Son los protocolos TCP/IP los que especifican los

mecanismos de formateo, de direccionamiento y de enrutamiento que garantizan que nuestros mensajes sean entregados a los destinatarios correctos.

Mensajes.

En la primera etapa del viaje desde la computadora al destino, el mensaje instantáneo se convierte en un formato que puede transmitirse en la red. Todos los tipos de mensajes tienen que ser convertidos a bits, señales digitales codificadas en binario, antes de ser enviados a sus destinos. Esto es así sin importar el formato del mensaje original: texto, video, voz o datos informáticos. Una vez que el mensaje instantáneo se convierte en bits, está listo para ser enviado a la red para su remisión.

Dispositivos.

Para comenzar a entender la solidez y complejidad de las redes interconectadas que forman Internet, es necesario empezar por lo más básico. Tomemos el ejemplo del envío de mensajes de texto con un programa de mensajería instantánea en una computadora. Cuando pensamos en utilizar servicios de red, generalmente pensamos en utilizar una computadora para acceder a ellos. Pero una computadora es sólo un tipo de dispositivo que puede enviar y recibir mensajes por una red. Muchos otros tipos de dispositivos pueden conectarse a la red para participar en servicios de red. Entre esos dispositivos se encuentran teléfonos, cámaras, sistemas de música, impresoras y consolas de juegos.

Además de la computadora, hay muchos otros componentes que hacen posible que nuestros mensajes instantáneos sean direccionados a través de kilómetros de cables, cables subterráneos, ondas aéreas y estaciones de satélites que puedan existir entre los dispositivos de origen y de destino. Uno de los componentes críticos en una red de cualquier tamaño es el router. Un router une dos o más redes, como una red doméstica e Internet, y pasa información de una red a otra. Los routers en una red funcionan para asegurar que el mensaje llegue al destino de la manera más rápida y eficaz.

Medio.

Para enviar el mensaje instantáneo al destino, la computadora debe estar conectada a una red local inalámbrica o con cables. Las redes locales pueden

instalarse en casas o empresas, donde permiten a computadoras y otros dispositivos compartir información y utilizar una conexión común a Internet.

Las redes inalámbricas permiten el uso de dispositivos con redes en cualquier parte, en una oficina, en una casa e inclusive al aire libre. Fuera de la casa o la oficina, la red inalámbrica está disponible en zonas activas públicas como cafés, empresas, habitaciones de hoteles y aeropuertos.

Muchas de las redes instaladas utilizan cables para proporcionar conectividad. Ethernet es la tecnología de red con cable más común en la actualidad. Los hilos, llamados cables, conectan las computadoras a otros dispositivos que forman las redes. Las redes con cables son mejores para transmitir grandes cantidades de datos a alta velocidad y son necesarias para respaldar multimedia de calidad profesional.

Servicios.

Los servicios de red son programas de computación que respaldan la red humana. Distribuidos en toda la red, estos servicios facilitan las herramientas de comunicación en línea como e-mails, foros de discusión/boletines, salas de chat y mensajería instantánea. Por ejemplo: en el caso un servicio de mensajería instantánea proporcionado por dispositivos en la nube, debe ser accesible tanto para el emisor como para el receptor.

Las Reglas.

Aspectos importantes de las redes que no son dispositivos ni medios, son reglas o protocolos. Estas reglas son las normas o protocolos que especifican la manera en que se envían los mensajes, cómo se direccionan a través de la red y cómo se interpretan en los dispositivos de destino. Por ejemplo: en el caso de la mensajería instantánea Jabber, los protocolos XMPP, TCP e IP son importantes conjuntos de reglas que permiten que se realice la comunicación.

1.4 Redes múltiples de múltiples servicios.

El teléfono tradicional, la radio, la televisión y las redes de datos informáticos tienen su propia versión individual de los cuatro elementos básicos de la red. En el pasado, cada uno de estos servicios requería una tecnología diferente para emitir

su señal de comunicación particular. Además, cada servicio tiene su propio conjunto de reglas y estándares para garantizar la comunicación exitosa de su señal a través de un medio específico.

Redes convergentes

Los avances de la tecnología nos permiten consolidar esas redes dispersas en una única plataforma: una plataforma definida como una red convergente. El flujo de voz, vídeo y datos que viajan a través de la misma red elimina la necesidad de crear y mantener redes separadas (Ver Fig.1.6). En una red convergente todavía hay muchos puntos de contacto y muchos dispositivos especializados (por ejemplo: computadoras personales, teléfonos, televisores, asistentes personales y registradoras de puntos de venta minoristas) pero una sola infraestructura de red común.

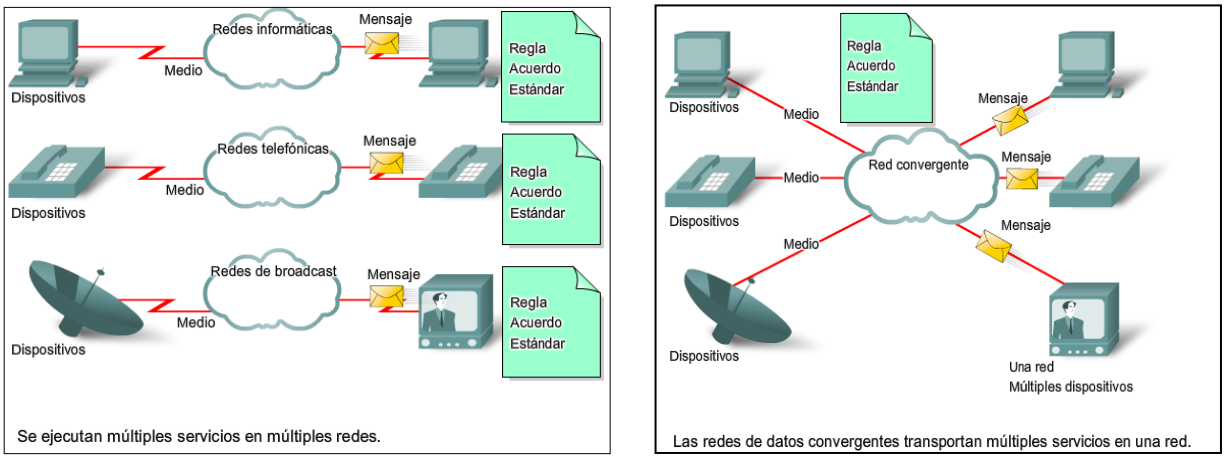


Fig.1.6 Redes múltiples.

Redes de información inteligentes.

La función de la red está evolucionando. La plataforma de comunicaciones inteligentes del futuro ofrecerá mucho más que conectividad básica y acceso a las aplicaciones. La convergencia de los diferentes tipos de redes de comunicación en una plataforma representa la primera fase en la creación de la red inteligente de información. En la actualidad nos encontramos en esta fase de evolución de la red. La próxima fase será consolidar no sólo los diferentes tipos de mensajes en

una única red, sino también consolidar las aplicaciones que generan, transmiten y aseguran los mensajes en los dispositivos de red integrados. No sólo la voz y el video se transmitirán mediante la misma red, sino que los dispositivos que realizan la conmutación de teléfonos y el broadcasting de videos serán los mismos dispositivos que enrutan los mensajes en la red. La plataforma de comunicaciones resultante proporcionará funcionalidad de aplicaciones de alta calidad a un costo reducido.

La velocidad a la que se desarrollan nuevas e interesantes aplicaciones de red convergentes se puede atribuir a la rápida expansión de Internet. Esta expansión creó una amplia audiencia y una base de consumo más grande, ya que puede enviarse cualquier mensaje, producto o servicio. Los procesos y mecanismos subyacentes que llevan a este crecimiento explosivo tienen como resultado una arquitectura de red más flexible y escalable. Como plataforma tecnológica que se puede aplicar a la vida, al aprendizaje, al trabajo y al juego en la red humana, la arquitectura de red de Internet se debe adaptar a los constantes cambios en los requisitos de seguridad y de servicio de alta calidad (Fig.1.7).

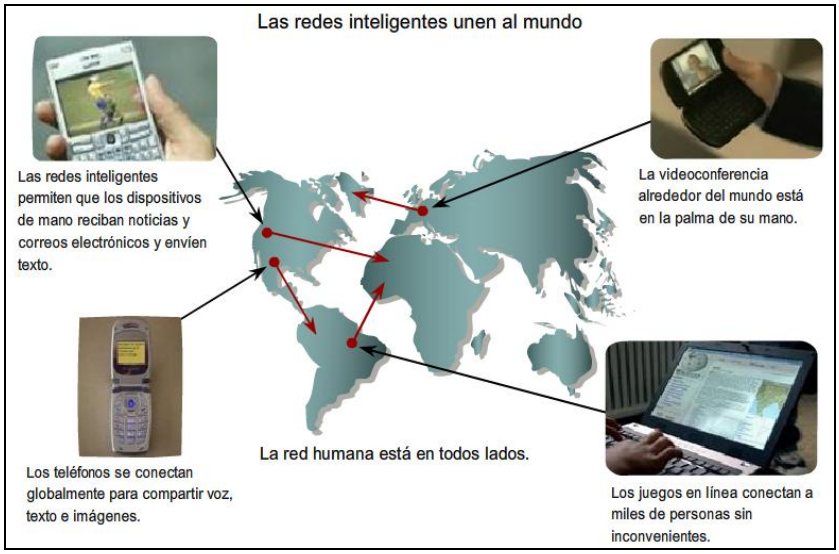


Fig.1.7 Las redes inteligentes unen al mundo.

1.5 Arquitectura de la red.

Las redes deben admitir una amplia variedad de aplicaciones y servicios, como así también funcionar con diferentes tipos de infraestructuras físicas. El término arquitectura de red, en este contexto, se refiere a las tecnologías que admiten la infraestructura y a los servicios y protocolos programados que pueden trasladar los mensajes en toda esa infraestructura. Debido a que Internet evoluciona, al igual que las redes en general, descubrimos que existen cuatro características básicas que la arquitectura subyacente necesita para cumplir con las expectativas de los usuarios: tolerancia a fallas, escalabilidad, calidad del servicio y seguridad.

a expectativa de que Internet está siempre disponible para millones de usuarios que confían en ella requiere de una arquitectura de red diseñada y creada con tolerancia a fallas. Una red tolerante a fallas es la que limita el impacto de una falla del software o hardware y puede recuperarse rápidamente cuando se produce dicha falla. Estas redes dependen de enlaces o rutas redundantes entre el origen y el destino del mensaje. Si un enlace o ruta falla, los procesos garantizan que los mensajes pueden enrutarse en forma instantánea en un enlace diferente transparente para los usuarios en cada extremo. Tanto las infraestructuras físicas como los procesos lógicos que direccionan los mensajes a través de la red están diseñados para adaptarse a esta redundancia. Ésta es la premisa básica de la arquitectura de redes actuales.

Una red escalable puede expandirse rápidamente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio enviado a los usuarios actuales. Miles de nuevos usuarios y proveedores de servicio se conectan a Internet cada semana. La capacidad de la red de admitir estas nuevas interconexiones depende de un diseño jerárquico en capas para la infraestructura física subyacente y la arquitectura lógica. El funcionamiento de cada capa permite a los usuarios y proveedores de servicios insertarse sin causar disrupción en toda la red. Los desarrollos tecnológicos aumentan constantemente las capacidades de transmitir el mensaje y el rendimiento de los componentes de la estructura física en cada capa. Estos desarrollos, junto con los nuevos métodos para identificar y localizar

usuarios individuales dentro de una internetwork, están permitiendo a Internet mantenerse al ritmo de la demanda de los usuarios.

Calidad de servicio (QoS).

Internet actualmente proporciona un nivel aceptable de tolerancia a fallas y escalabilidad para sus usuarios. Pero las nuevas aplicaciones disponibles para los usuarios en ínternetworks crean expectativas mayores para la calidad de los servicios enviados. Las transmisiones de voz y video en vivo requieren un nivel de calidad consistente y un envío ininterrumpido que no era necesario para las aplicaciones informáticas tradicionales. La calidad de estos servicios se mide con la calidad de experimentar la misma presentación de audio y video en persona. Las redes de voz y video tradicionales están diseñadas para admitir un único tipo de transmisión y, por lo tanto, pueden producir un nivel aceptable de calidad. Los nuevos requerimientos para admitir esta calidad de servicio en una red convergente cambian la manera en que se diseñan e implementan las arquitecturas de red.

Seguridad.

Internet evolucionó de una internetwork de organizaciones gubernamentales y educativas estrechamente controlada a un medio ampliamente accesible para la transmisión de comunicaciones personales y empresariales. Como resultado, cambiaron los requerimientos de seguridad de la red, como se muestra en la Fig.1.8.

Las expectativas de privacidad y seguridad que se originan del uso de ínternetworks para intercambiar información empresarial crítica y confidencial exceden lo que puede enviar la arquitectura actual. La rápida expansión de las áreas de comunicación que no eran atendidas por las redes de datos tradicionales aumenta la necesidad de incorporar seguridad en la arquitectura de red. Como resultado, se está dedicando un gran esfuerzo a esta área de investigación y desarrollo. Mientras tanto, se están implementando muchas herramientas y

procedimientos para combatir los defectos de seguridad inherentes en la arquitectura de red.

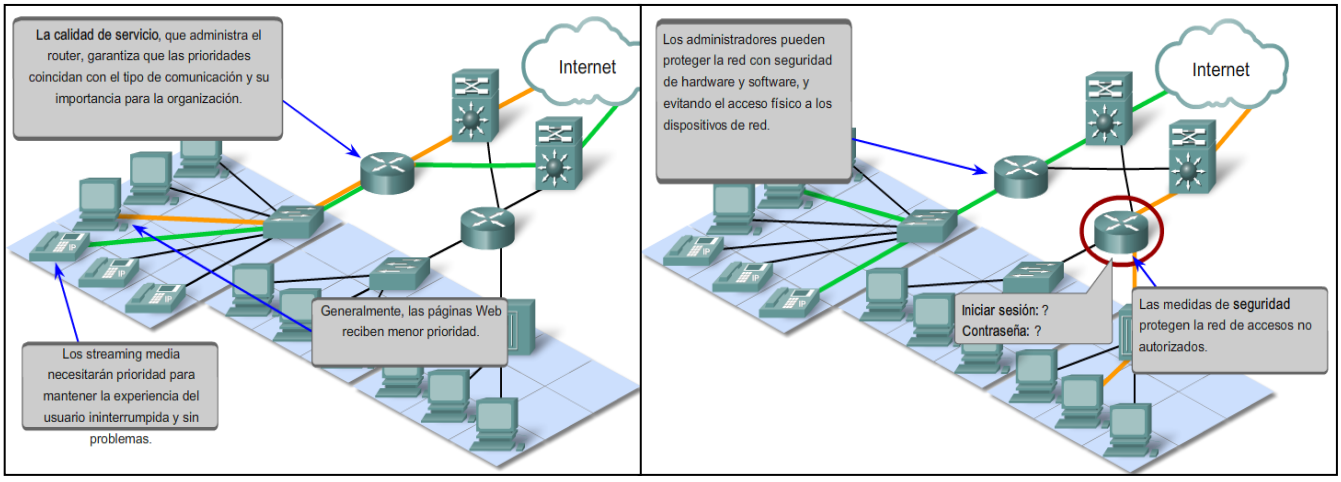


Fig.1.8 Calidad de servicio y seguridad.

Internet, en sus comienzos, era el resultado de una investigación respaldada por el Departamento de Defensa de Estados Unidos (DoD). Su objetivo principal fue tener un medio de comunicación que pudiera soportar la destrucción de numerosos sitios e instalaciones de transmisión sin interrumpir el servicio. Esto implica que la tolerancia a fallas era el foco del esfuerzo del trabajo de diseño de internetwork inicial. Los primeros investigadores de red observaron las redes de comunicación existentes, que en sus comienzos se utilizaban para la transmisión de tráfico de voz, para determinar qué podía hacerse para mejorar el nivel de tolerancia a fallas.

Redes orientadas a la conexión conmutada por circuito.

Para comprender el desafío con el que se enfrentaron los investigadores del DoD, es necesario observar cómo funcionaban los sistemas telefónicos. Cuando una persona realiza una llamada utilizando un teléfono tradicional, la llamada primero pasa por un proceso de configuración en el cual se identifican todas las conmutaciones telefónicas entre la persona y el teléfono al que está llamando. Se

crea una ruta temporal o circuito a través de las distintas ubicaciones de conmutación a utilizar durante la duración de la llamada telefónica. Si falla algún enlace o dispositivo que participa en el circuito, la llamada se cae. Para volver a conectarse, se debe realizar una nueva llamada y crear un nuevo circuito entre el teléfono de origen y el de destino. Este tipo de red orientada a la conexión se llama red conmutada por circuito. Las primeras redes conmutadas por circuito no recreaban en forma dinámica los circuitos descartados. Para recuperarse de una falla, se deben iniciar nuevas llamadas y crear nuevos circuitos de extremo a extremo.

Muchas redes conmutadas por circuitos otorgan prioridad al mantenimiento de conexiones de circuitos (Fig.1.9) existentes a expensas de nuevas solicitudes de circuitos. En este tipo de red orientada a la conexión, una vez establecido el circuito, aunque no exista comunicación entre las personas en ningún extremo de la llamada, el circuito permanece conectado y los recursos se reservan hasta que una de las partes desconecta la llamada. Debido a que existe una determinada capacidad para crear nuevos circuitos, es posible que a veces reciba un mensaje de que todos los circuitos están ocupados y no pueda realizar la llamada. El costo que implica crear muchas rutas alternativas con capacidad suficiente para admitir un gran número de circuitos simultáneos y las tecnologías necesarias para recrear en forma dinámica los circuitos descartados en caso de falla, llevaron al DoD a considerar otros tipos de redes.

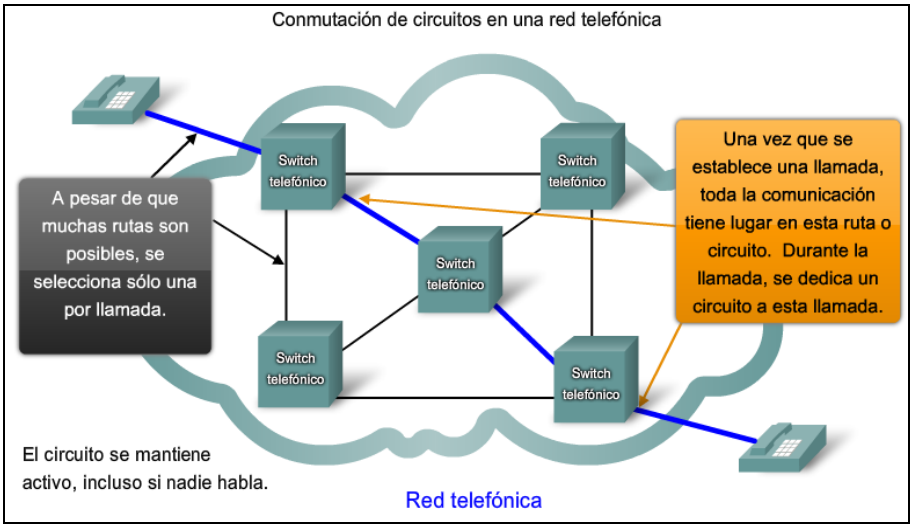


Fig.1.9 Conmutación de circuitos en una red telefónica.

Redes sin conexión conmutada por paquetes.

En la búsqueda de una red que pueda soportar la pérdida de una cantidad significativa de sus servicios de transmisión y conmutación, los primeros diseñadores de Internet reevaluaron las investigaciones iniciales acerca de las redes conmutadas por paquetes. La premisa para este tipo de redes es que un simple mensaje puede dividirse en múltiples bloques de mensajes. Los bloques individuales que contienen información de direccionamiento indican tanto su punto de origen como su destino final. Utilizando esta información incorporada, se pueden enviar por la red a través de diversas rutas esos bloques de mensajes, denominados paquetes, y se pueden rearmar como el mensaje original una vez que llegan a destino.

Utilización de paquetes

Los dispositivos dentro de la misma red no tienen en cuenta el contenido de los paquetes individuales, sólo es visible la dirección del destino final y del próximo dispositivo en la ruta hacia ese destino. No se genera ningún circuito reservado entre emisor y receptor. Cada paquete se envía en forma independiente desde una ubicación de conmutación a otra. En cada ubicación, se decide qué ruta utilizar para enviar el paquete al destino final. Si una ruta utilizada anteriormente ya no está disponible, la función de enrutamiento puede elegir en forma dinámica la próxima ruta disponible. Debido a que los mensajes se envían por partes, en lugar de hacerlo como un mensaje completo y único, los pocos paquetes que pueden perderse en caso de que se produzca una falla pueden volver a transmitirse a destino por una ruta diferente. En muchos casos, el dispositivo de destino no tiene en cuenta que se ha producido una falla o reenrutamiento.

Los investigadores del Departamento de Defensa (DoD) se dieron cuenta de que una red sin conexión conmutada por paquetes tenía las características necesarias para admitir una arquitectura de red resistente y tolerante a fallas. En una red conmutada por paquetes no existe la necesidad de un circuito reservado y simple de extremo a extremo. Cualquier parte del mensaje puede enviarse a través de la red utilizando una ruta disponible. Los paquetes que contienen las partes de los

mensajes de diferentes orígenes pueden viajar por la red al mismo tiempo. El problema de los circuitos inactivos o no utilizados desaparece; todos los recursos disponibles pueden utilizarse en cualquier momento para enviar paquetes al destino final. Al proporcionar un método para utilizar dinámicamente rutas redundantes sin intervención del usuario, Internet se ha vuelto un método de comunicación tolerante a fallas y escalable.

Redes orientadas a la conexión

Aunque las redes sin conexión conmutada por paquetes (Fig. 1.10) cubren las necesidades de los DoD y siguen siendo la infraestructura primaria de la Internet actual, hay algunos beneficios en un sistema orientado a la conexión como el sistema telefónico conmutado por circuito. Debido a que los recursos de las diferentes ubicaciones de conmutación están destinados a proporcionar un número determinado de circuitos, pueden garantizarse la calidad y consistencia de los mensajes transmitidos en una red orientada a la conexión. Otro beneficio es que el proveedor del servicio puede cargar los usuarios de la red durante el período de tiempo en que la conexión se encuentra activa. La capacidad de cargar los usuarios para conexiones activas a través de la red es una premisa fundamental de la industria del servicio de telecomunicaciones.

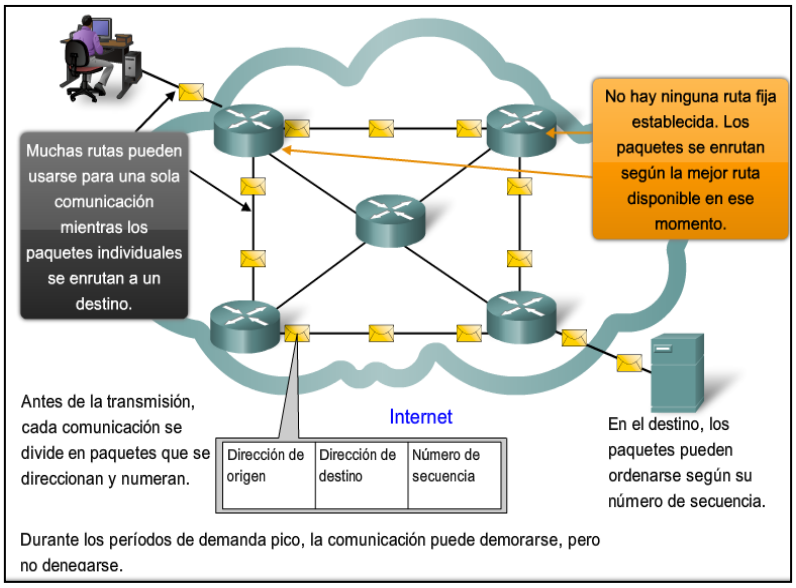


Fig.1.10 Conmutación de paquetes en una red de datos.

1.6 Arquitectura de la red escalable.

El hecho de que Internet se expanda a esta velocidad, sin afectar seriamente el rendimiento de usuarios individuales, es una función del diseño de los protocolos y de las tecnologías subyacentes sobre la cual se construye. Internet, hecho de una colección de redes públicas y privadas interconectadas, tiene una estructura jerárquica en capas para servicios de direccionamiento, designación y conectividad. En cada nivel o capa de la jerarquía, los operadores de red individual mantienen relaciones entre pares con otros operadores en el mismo nivel. Como resultado, el tráfico de redes destinado para servicios regionales y locales no necesita cruzar a un punto central para su distribución. Los servicios comunes pueden duplicarse en diferentes regiones, manteniendo el tráfico de las redes backbone de nivel superior.

Aunque no existe una organización que regule Internet, los operadores de las diferentes redes individuales que proporcionan la conectividad de Internet cooperan para cumplir con los protocolos y estándares aceptados.

La adherencia a los estándares permite a los fabricantes de hardware y software concentrarse en las mejoras del producto en áreas de rendimiento y capacidad, sabiendo que los nuevos productos pueden integrarse y mejorar la infraestructura existente.

La arquitectura de Internet actual, altamente escalable como se muestra en la Fig. 1.11, no siempre puede mantener el ritmo de la demanda del usuario. Los nuevos protocolos y estructuras de direccionamiento están en desarrollo para cumplir con el ritmo acelerado al cual se agregan los servicios y aplicaciones de Internet.

.

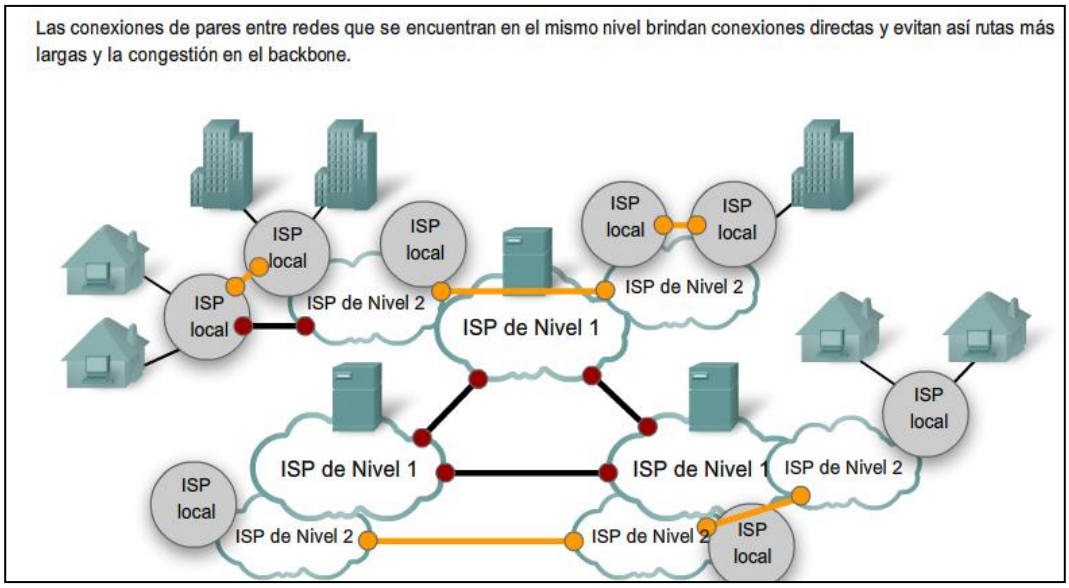


Fig.1.11 Estructura de internet: Una red de redes

1.7 provisión de calidad de servicio.

Las redes deben proporcionar servicios seguros, predecibles, mensurables y, a veces, garantizados. La arquitectura de red conmutada por paquetes no garantiza que todos los paquetes que conforman un mensaje en particular lleguen a tiempo, en el orden correcto, ni aun garantizan la llegada.

Las redes también necesitan mecanismos para administrar el tráfico de redes congestionado. La congestión se genera cuando la demanda de recursos de red supera la capacidad disponible.

Si todas las redes tuvieran recursos infinitos no habría necesidad de utilizar mecanismos QoS para garantizar la calidad de servicio. Desafortunadamente, éste no es el caso. Existen algunas restricciones en los recursos de red que no pueden evitarse. Las restricciones incluyen limitaciones tecnológicas, costos y disponibilidad local del servicio de alto ancho de banda. El ancho de banda es la medida de la capacidad de transmisión de datos de la red. Cuando se producen intentos de comunicaciones simultáneas en la red, la demanda de ancho de banda puede exceder su disponibilidad. La solución obvia para esta situación sería aumentar la cantidad de ancho de banda disponible. Pero debido a las restricciones anteriormente mencionadas, esto no siempre es posible.

En la mayoría de los casos, cuando el volumen de paquetes es mayor de lo que se puede transportar en la red, los dispositivos colocan los paquetes en cola en la memoria hasta que haya recursos disponibles para transmitirlos. Los paquetes en cola provocan retrasos. Si el número de paquetes en cola continúa aumentando, las colas de la memoria se llenan y los paquetes se descartan.

El secreto para llegar a una solución exitosa de calidad de aplicación de extremo a extremo es lograr la Calidad de servicio (QoS) necesaria administrando los parámetros de pérdida de paquetes o de retraso en una red. Por lo tanto, asegurar la QoS requiere de un grupo de técnicas para administrar la utilización de los recursos de red. Para mantener una buena calidad de servicio para las aplicaciones que lo requieren, es necesario priorizar los tipos de paquetes de datos que deben enviarse a expensas de otros tipos de paquetes que puedan retrasarse o descartarse.

Clasificación.

Lo ideal es asignar una prioridad exacta para cada tipo de comunicación. En la actualidad, esto no resulta práctico y posible. Por lo tanto, clasificamos las aplicaciones en categorías según la calidad específica de requisitos de servicios.

Para crear clasificaciones de datos QoS, utilizamos una combinación de características de comunicación y la importancia relativa asignada a la aplicación. Luego incluimos todos los datos en la misma clasificación en base a las mismas reglas. Por ejemplo, la comunicación sensible al tiempo o importante debería clasificarse en forma diferente de la comunicación que puede esperar o es de menor importancia.

Asignación de prioridades.

Las características de la información que se comunica también afectan su administración. Por ejemplo, el envío de una película utiliza una importante cantidad de recursos de red cuando se envía en forma continua, sin interrupción. Otros tipos de servicios, los e-mails, por ejemplo, no resultan tan demandantes en la red. En una empresa, el administrador puede decidir asignar la mayor parte de

los recursos de red a la película, considerando que ésta es la prioridad para los clientes. El administrador puede decidir que el impacto será mínimo si los usuarios de e-mails tienen que esperar algunos segundos más para que llegue. En otra empresa la calidad del stream de vídeo no es tan importante como la información de control de procesos críticos que operan las máquinas de fabricación.

Los mecanismos de QoS permiten el establecimiento de estrategias de administración de cola que implementan prioridades para las diferentes clasificaciones de los datos de aplicación. Sin el diseño y la implementación correctos de los mecanismos de QoS, los paquetes de datos se descartan sin considerar las características de la aplicación ni la prioridad. Algunas de las decisiones prioritarias para una organización pueden ser:

- Comunicaciones sensibles al tiempo: aumentan la prioridad por servicios como el teléfono o la distribución de vídeos.
- Comunicaciones no sensibles al tiempo: disminuyen la prioridad de recuperación de páginas Web o de correos electrónicos.
- Mucha importancia para la empresa: aumenta la prioridad de control de producción o de datos de transacciones comerciales.
- Comunicación indeseable: disminuye la prioridad o bloquea la actividad no deseada como la transferencia de archivos entre pares o el entretenimiento en vivo.

La Calidad de servicio que puede ofrecer una red es un tema vital y, en algunas situaciones, es crucial (Fig. 1.12). Imagine las consecuencias si se descarta una llamada de pedido de ayuda a un centro de emergencias, o si se pierde la señal de control de una pieza automatizada de maquinaria pesada. Una responsabilidad clave para los administradores de red en una organización es establecer una política de calidad de servicio para asegurar que se apliquen los mecanismos para cumplir los objetivos.

Fig.1.12 La calidad de servicio es importante.

1.8 Provisión de seguridad de red.

La infraestructura de red, los servicios y los datos contenidos en las computadoras conectadas a la red son activos comerciales y personales muy importantes. Comprometer la integridad de estos activos puede ocasionar serias repercusiones financieras y comerciales.

Algunas de las consecuencias de la ruptura en la seguridad de la red son:

- Interrupciones de red que impiden la realización de comunicaciones y de transacciones, con la consecuente pérdida de negocios,
- Mal direccionamiento y pérdida de fondos personales o comerciales,
- Propiedad intelectual de la empresa (ideas de investigación, patentes o diseños) que son robados y utilizados por la competencia, o
- Detalles de contratos con clientes que se divulgan a los competidores o son hechos públicos, generando una pérdida de confianza del mercado de la industria.

La falta de confianza pública en la privacidad, confidencialidad y niveles de integridad de los negocios puede derivar en la pérdida de ventas y, finalmente, en la quiebra de la empresa. Existen dos tipos de cuestiones de seguridad de la red

que se deben tratar a fin de evitar serias consecuencias: seguridad de la infraestructura de la red y seguridad del contenido.

Asegurar la infraestructura de la red incluye la protección física de los dispositivos que proporcionan conectividad de red y evitan el acceso no autorizado al software de administración que reside en ellos.

La seguridad del contenido se refiere a la protección de la información contenida en los paquetes que se transmiten en la red y la información almacenada en los dispositivos conectados a ésta. Al transmitir la información en Internet u otra red, los dispositivos y las instalaciones por las que viajan los paquetes desconocen el contenido de los paquetes individuales. Se deben implementar herramientas para proporcionar seguridad al contenido de los mensajes individuales sobre los protocolos subyacentes que rigen la forma en que los paquetes se formatean, direccionan y envían. Debido a que el reensamblaje y la interpretación del contenido se delegan a programas que se ejecutan en sistemas individuales de origen y destino, muchos de los protocolos y herramientas de seguridad deben implementarse también en esos sistemas.

Las medidas de seguridad que se deben tomar en una red son:

- Evitar la divulgación no autorizada o el robo de información,
- Evitar la modificación no autorizada de información, y
- Evitar la denegación de servicio.

Garantizar la confidencialidad.

La privacidad de los datos se logra permitiendo que lean los datos solamente los receptores autorizados y designados (individuos, procesos o dispositivos).

Un sistema seguro de autenticación de usuarios, el cumplimiento de las contraseñas difíciles de adivinar y el requerimiento a los usuarios para que las cambien frecuentemente ayudan a restringir el acceso a las comunicaciones y a los datos almacenados en los dispositivos adjuntos de la red. Cuando corresponda, el contenido encriptado asegura la confidencialidad y reduce las posibilidades de divulgación no autorizada o robo de información.

Mantener la integridad de las comunicaciones.

La integración de datos significa que la información no se alteró durante la transmisión de origen a destino. La integración de datos puede verse comprometida cuando al dañarse la información, ya sea en forma intencional o accidental, antes de que el receptor correspondiente la reciba.

La integridad de origen es la confirmación de que se validó la identidad del emisor. Se compromete la integridad del origen cuando un usuario o dispositivo falsifica su identidad y proporciona información incorrecta al destinatario.

El uso de firmas digitales, algoritmos de hash y mecanismos de checksum son formas de proporcionar integridad de origen y de datos a través de la red para evitar la modificación no autorizada de información. (Ver Fig. 1.13)

Garantizar disponibilidad.

La garantía de confidencialidad e integridad son irrelevantes si los recursos de red están sobrecargados o no disponibles. Disponibilidad significa tener la seguridad de acceder en forma confiable y oportuna a los servicios de datos para usuarios autorizados. Los recursos pueden no estar disponibles durante un ataque de Denegación de servicio (DoS) o por la propagación de un virus de computadora. Los dispositivos firewall de red, junto con los software antivirus de los equipos de escritorio y de los servidores pueden asegurar la confiabilidad y solidez del sistema para detectar, repeler y resolver esos ataques. La creación de infraestructuras de red completamente redundantes, con pocos puntos de error, puede reducir el impacto de esas amenazas.

El resultado de la implementación de medidas para mejorar tanto la calidad del servicio como la seguridad de las comunicaciones de red es un aumento en la complejidad de la plataforma de red subyacente. Debido a que Internet continúa expandiéndose para ofrecer más y nuevos servicios, su futuro depende de las nuevas y más sólidas arquitecturas en desarrollo que incluyen estas cuatro características: tolerancia a fallas, escalabilidad, calidad del servicio y seguridad.

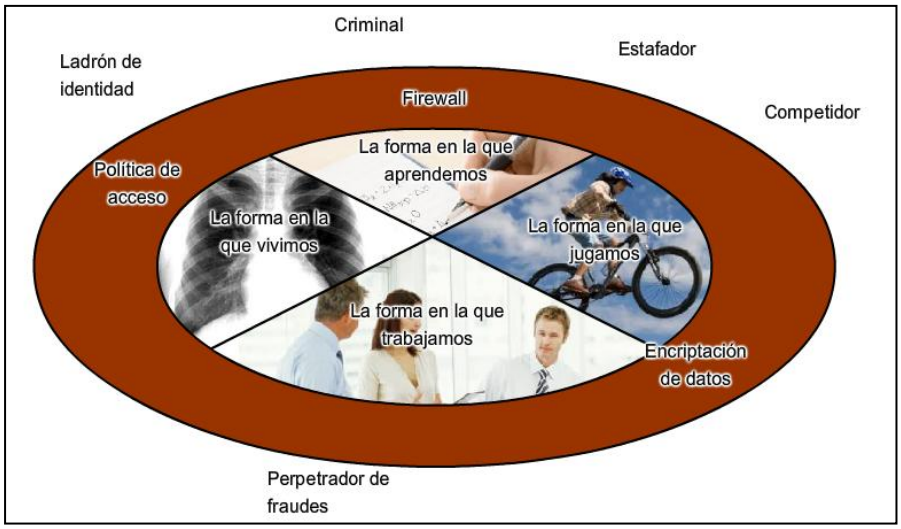


Fig.1.13 Las comunicaciones y la información que deseamos, sean privadas y estén protegidas de quienes las usan de manera no autorizada.

1.9 Componentes de la red.

La ruta que toma un mensaje desde el origen hasta el destino puede ser tan sencilla como un solo cable que conecta una computadora con otra o tan compleja como una red que literalmente abarca el mundo. Esta infraestructura de red es la plataforma que respalda la red humana. Proporciona el canal estable y confiable por el cual se producen las comunicaciones.

Los dispositivos y los medios son los elementos físicos o hardware de la red. El hardware es generalmente el componente visible de la plataforma de red, como una computadora portátil o personal, un switch, o el cableado que se usa para conectar estos dispositivos. A veces, puede que algunos componentes no sean visibles. En el caso de los medios inalámbricos, los mensajes se transmiten a través del aire utilizando radio frecuencia invisible u ondas infrarrojas.

Los servicios y procesos son los programas de comunicación, denominados software, que se ejecutan en los dispositivos conectados a la red. Un servicio de red proporciona información en respuesta a una solicitud. Los servicios incluyen una gran cantidad de aplicaciones de red comunes que utilizan las personas a diario, como los servicios de e-mail hosting y los servicios de Web hosting. Los procesos proporcionan la funcionalidad que direcciona y traslada mensajes a

través de la red. Los procesos son menos obvios para nosotros, pero son críticos para el funcionamiento de las redes.

Los dispositivos de red con los que la gente está más familiarizada se denominan dispositivos finales. Estos dispositivos constituyen la interfaz entre la red humana y la red de comunicación subyacente. Algunos ejemplos de dispositivos finales son:

- Computadoras (estaciones de trabajo, computadoras portátiles, servidores de archivos, servidores Web)
- Impresoras de red
- Teléfonos VoIP
- Cámaras de seguridad
- Dispositivos móviles de mano (como escáneres de barras inalámbricos, asistentes digitales personales (PDA))

En el contexto de una red, los dispositivos finales se denominan host. Un dispositivo host puede ser el origen o el destino de un mensaje transmitido a través de la red. Para distinguir un host de otro, cada host en la red se identifica por una dirección. Cuando un host inicia una comunicación, utiliza la dirección del host de destino para especificar dónde debe ser enviado el mensaje.

En las redes modernas, un host puede funcionar como un cliente, como un servidor o como ambos. El software instalado en el host determina qué rol representa en la red.

Los servidores son hosts que tienen software instalado que les permite proporcionar información y servicios, como e-mail o páginas Web, a otros hosts en la red.

Los clientes son hosts que tienen software instalado que les permite solicitar y mostrar la información obtenida del servidor.

Además de los dispositivos finales con los cuales la gente está familiarizada, las redes dependen de dispositivos intermediarios para proporcionar conectividad y para trabajar detrás de escena y garantizar que los datos fluyan a través de la red. Estos dispositivos conectan los hosts individuales a la red y pueden conectar

varias redes individuales para formar una internetwork. Los siguientes son ejemplos de dispositivos de red intermediarios:

- dispositivos de acceso a la red (hubs, switches y puntos de acceso inalámbricos),
- dispositivos de Internetworking (routers),
- servidores de comunicación y módems, y
- dispositivos de seguridad (firewalls).

La administración de datos mientras fluyen a través de la red también es una función de los dispositivos intermediarios. Estos dispositivos utilizan la dirección host de destino, conjuntamente con información sobre las interconexiones de la red, para determinar la ruta que deben tomar los mensajes a través de la red. Los procesos que se ejecutan en los dispositivos de red intermediarios realizan las siguientes funciones:

- Regenerar y retransmitir señales de datos,
- Mantener información sobre qué rutas existen a través de la red y de la internetwork,
- Notificar a otros dispositivos los errores y las fallas de comunicación,
- Direccionar datos por rutas alternativas cuando existen fallas en un enlace,
- Clasificar y direccionar mensajes según las prioridades de qos (calidad de servicio), y
- Permitir o denegar el flujo de datos en base a configuraciones de seguridad.

Medios de red.

La comunicación a través de una red es transportada por un medio (Fig. 1.14). El medio proporciona el canal por el cual viaja el mensaje desde el origen hasta el destino.

Las redes modernas utilizan principalmente tres tipos de medios para interconectar los dispositivos y proporcionar la ruta por la cual pueden transmitirse los datos. Estos medios son:

- Hilos metálicos dentro de los cables,
- Fibras de vidrio o plásticas (cable de fibra óptica), y

- Transmisión inalámbrica.

La codificación de señal que se debe realizar para que el mensaje sea transmitido es diferente para cada tipo de medio. En los hilos metálicos, los datos se codifican dentro de impulsos eléctricos que coinciden con patrones específicos. Las transmisiones por fibra óptica dependen de pulsos de luz, dentro de intervalos de luz visible o infrarroja. En las transmisiones inalámbricas, los patrones de ondas electromagnéticas muestran los distintos valores de bits.

Los diferentes tipos de medios de red tienen diferentes características y beneficios. No todos los medios de red tienen las mismas características ni son adecuados para el mismo fin. Los criterios para elegir un medio de red son:

- La distancia en la cual el medio puede transportar exitosamente una señal,
- El ambiente en el cual se instalará el medio,
- La cantidad de datos y la velocidad a la que se deben transmitir, y
- El costo del medio y de la instalación.

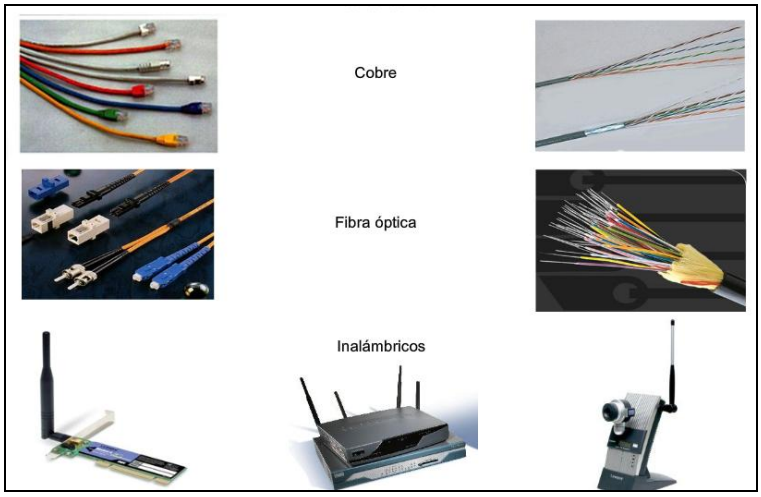


Fig.1.14 Medios de red.

1.10 Redes de area local.

Las infraestructuras de red pueden variar en gran medida en términos de:

- El tamaño del área cubierta,
- La cantidad de usuarios conectados, y
- La cantidad y tipos de servicios disponibles.

Una red individual generalmente cubre una única área geográfica y proporciona servicios y aplicaciones a personas dentro de una estructura organizacional común, (en la Fig. 1.15) una empresa, un campus o una región. Este tipo de red se denomina Red de área local (LAN). Una LAN por lo general está administrada por una organización única. El control administrativo que rige las políticas de seguridad y control de acceso está implementado en el nivel de red.

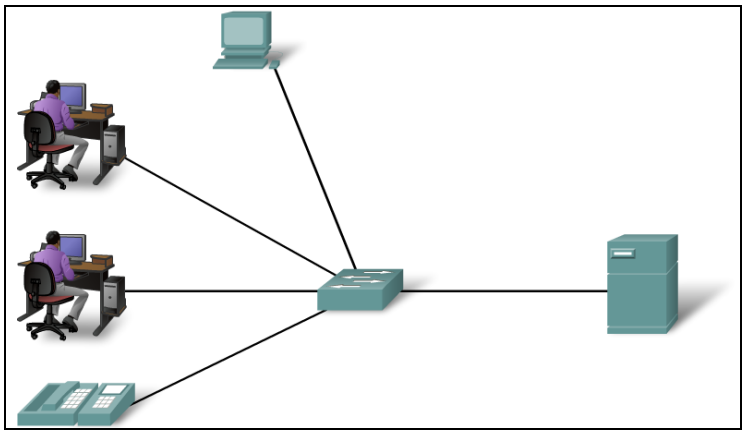


Fig.1.15 Una red que abastece un hogar, un edificio o un campus es considerada una Red de Área Local (LAN).

1.11 Redes de Área Ampliada.

Cuando una compañía o una organización tiene ubicaciones separadas por grandes distancias geográficas, es posible que deba utilizar un proveedor de servicio de telecomunicaciones (TSP) para interconectar las LAN en las distintas ubicaciones. Los proveedores de servicios de telecomunicaciones operan grandes redes regionales que pueden abarcar largas distancias. Tradicionalmente, los TSP transportaban las comunicaciones de voz y de datos en redes separadas. Cada vez más, estos proveedores ofrecen a sus subscriptores servicios de red convergente de información.

Por lo general, las organizaciones individuales alquilan las conexiones a través de una red de proveedores de servicios de telecomunicaciones. Estas redes que conectan las LAN en ubicaciones separadas geográficamente se conocen como Redes de área amplia (WAN). Aunque la organización mantiene todas las políticas y la administración de las LAN en ambos extremos de la conexión, las políticas dentro de la red del proveedor del servicio de comunicaciones son controladas por el TSP.

Las WAN (Fig. 1.16) utilizan dispositivos de red diseñados específicamente para realizar las interconexiones entre las LAN. Dada la importancia de estos dispositivos para la red, la configuración, instalación y mantenimiento de éstos son aptitudes complementarias de la función de una red de la organización.

Las LAN y WAN son de mucha utilidad para las organizaciones individuales. Conectan a los usuarios dentro de la organización. Permiten gran cantidad de formas de comunicación que incluyen intercambio de e-mails, capacitación corporativa y acceso a recursos.

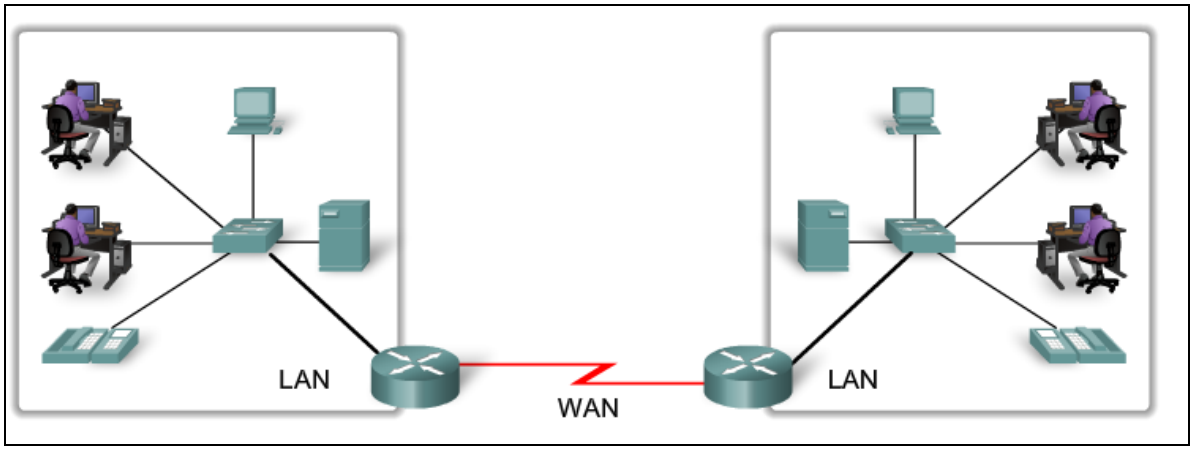


Fig.1.16 Las LAN separadas por una distancia geográfica están conectadas por una red que se conoce como Red de Área Extendida.

1.12 Internet una red de redes.

Aunque existen beneficios por el uso de una LAN o WAN, la mayoría de los usuarios necesitan comunicarse con un recurso u otra red, fuera de la organización local.

Aunque existen beneficios por el uso de una LAN o WAN, la mayoría de los usuarios necesitan comunicarse con un recurso u otra red, fuera de la organización local.

Los ejemplos de este tipo de comunicación incluyen:

- Enviar un correo electrónico a un amigo en otro país,
- Acceder a noticias o productos de un sitio web,
- Obtener un archivo de la computadora de un vecino,
- Mensajería instantánea con un pariente de otra ciudad, y
- Seguimiento de la actividad de un equipo deportivo favorito a través del teléfono celular.

Internetwork.

Una malla global de redes interconectadas (internetworks) cubre estas necesidades de comunicación humanas. Algunas de estas redes interconectadas pertenecen a grandes organizaciones públicas o privadas, como agencias gubernamentales o empresas industriales, y están reservadas para su uso exclusivo. La internetwork más conocida, ampliamente utilizada y a la que accede el público en general es Internet.

Internet se crea por la interconexión de redes que pertenecen a los Proveedores de servicios de Internet (ISP). Estas redes ISP se conectan entre sí para proporcionar acceso a millones de usuarios en todo el mundo. Garantizar la comunicación efectiva a través de esta infraestructura diversa requiere la aplicación de tecnologías y protocolos consistentes y reconocidos comúnmente, como también la cooperación de muchas agencias de administración de redes.

Intranet.

El término intranet se utiliza generalmente para referirse a una conexión privada de algunas LAN y WAN que pertenecen a una organización y que está diseñada para que puedan acceder solamente los miembros y empleados de la organización u otros que tengan autorización (Fig. 1.17).

Nota: Es posible que los siguientes términos sean sinónimos: internetwork, red de datos y red. Una conexión de dos o más redes de datos forma una internetwork: una red de redes. También es habitual referirse a una internetwork como una red de datos o simplemente como una red, cuando se consideran las comunicaciones a alto nivel. El uso de los términos depende del contexto y del momento, a veces los términos pueden ser intercambiados.

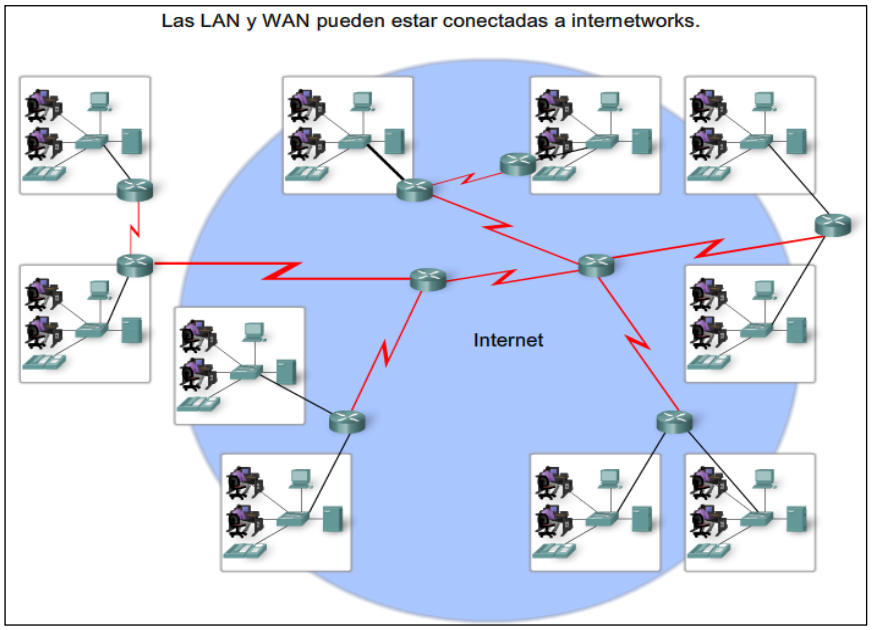


Fig.1.17 Las LAN y WAN pueden estar conectadas a ínternetworks.

1.13 Representaciones de red.

Cuando se transporta información compleja como la conectividad de red y el funcionamiento de una gran internetwork, es de mucha utilidad utilizar representaciones visuales y gráficos como los mostrados en la Fig. 1.18. Como cualquier otro idioma, el lenguaje de interconexión de redes utiliza un grupo común de símbolos para representar los distintos dispositivos finales, los dispositivos de red y los medios. La capacidad de reconocer las representaciones lógicas de los componentes físicos de networking es fundamental para poder visualizar la organización y el funcionamiento de una red. Durante todo este curso y pruebas de laboratorio, aprenderá cómo funcionan estos dispositivos y cómo se realizan con ellos tareas básicas de configuración.

Además de estas representaciones, se utiliza terminología especializada cuando se analiza la manera en que se conectan unos con otros. Algunos términos importantes para recordar son:

Tarjeta de interfaz de red (NIC): una NIC o adaptador LAN proporciona la conexión física con la red en la computadora personal u otro dispositivo host. El medio que conecta la computadora personal con el dispositivo de red se inserta directamente en la NIC.

Puerto físico: conector o toma en un dispositivo de red en el cual el medio se conecta con un host o con otro dispositivo de red.

Interfaz: puertos especializados de un dispositivo de Internetworking que se conecta con redes individuales. Puesto que los routers se utilizan para interconectar redes, los puertos de un router se conocen como interfaces de red.

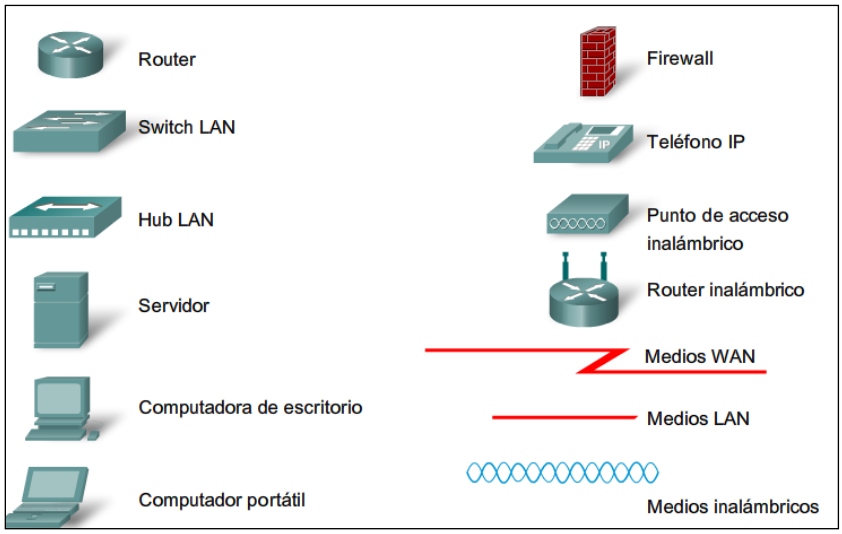


Fig.1.18 Símbolos comunes de las redes de datos.

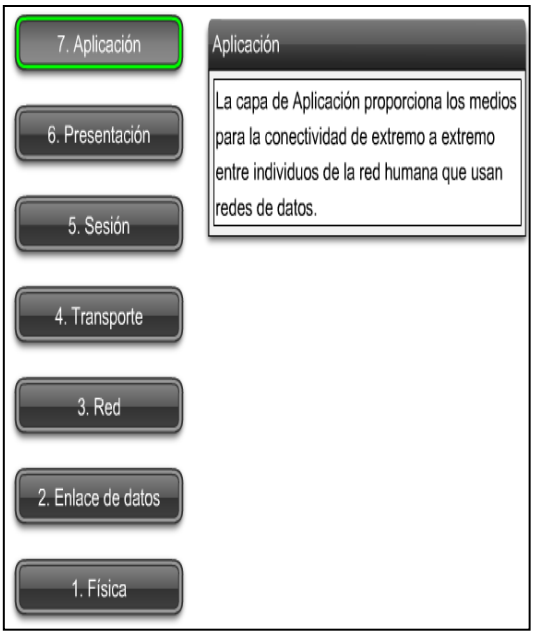
1.14 Modelo OSI.

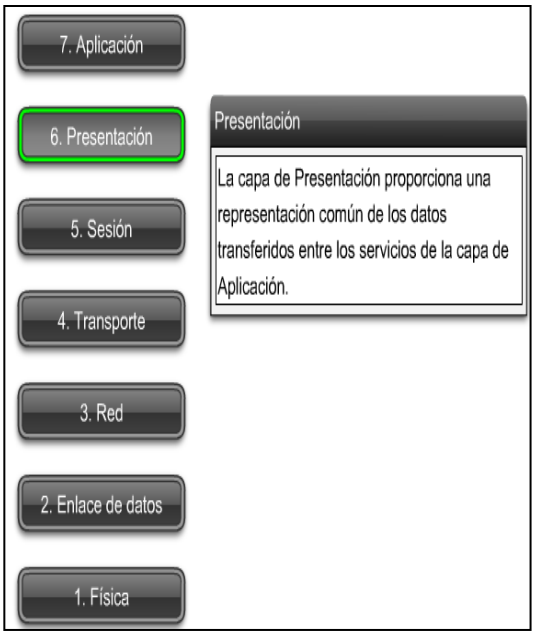
Inicialmente, el modelo OSI fue diseñado por la Organización Internacional para la Estandarización (ISO, International Organization for Standardization) para proporcionar un marco sobre el cual crear una suite de protocolos de sistemas abiertos. La visión era que este conjunto de protocolos se utilizara para desarrollar una red internacional que no dependiera de sistemas propietarios.

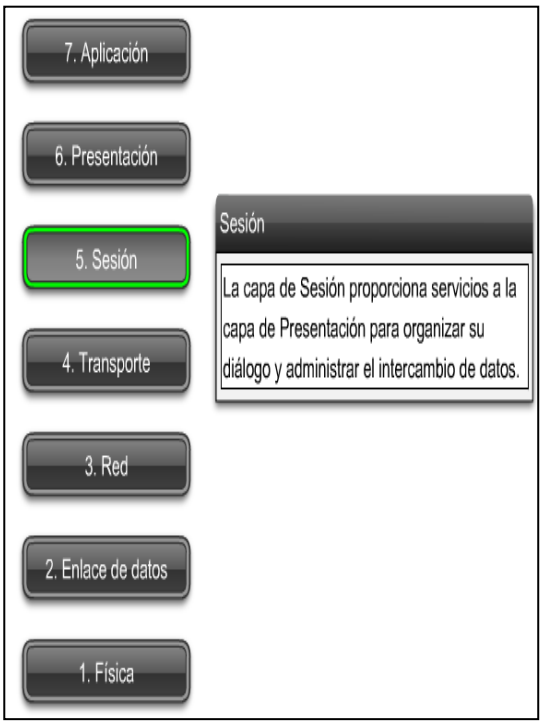
Lamentablemente, la velocidad a la que fue adoptada la Internet basada en TCP/IP y la proporción en la que se expandió ocasionaron que el desarrollo y la aceptación de la suite de protocolos OSI quedaran atrás. Aunque pocos de los protocolos desarrollados mediante las especificaciones OSI son de uso masivo en la actualidad, el modelo OSI de siete capas ha realizado aportes importantes para el desarrollo de otros protocolos y productos para todos los tipos de nuevas redes.

Como modelo de referencia, el modelo OSI proporciona una amplia lista de funciones y servicios que pueden producirse en cada capa. También describe la interacción de cada capa con las capas directamente por encima y por debajo de él. Aunque el contenido de esta tesis se estructurará en torno al modelo OSI, el eje del análisis serán los protocolos identificados en el stack de protocolos TCP/IP.

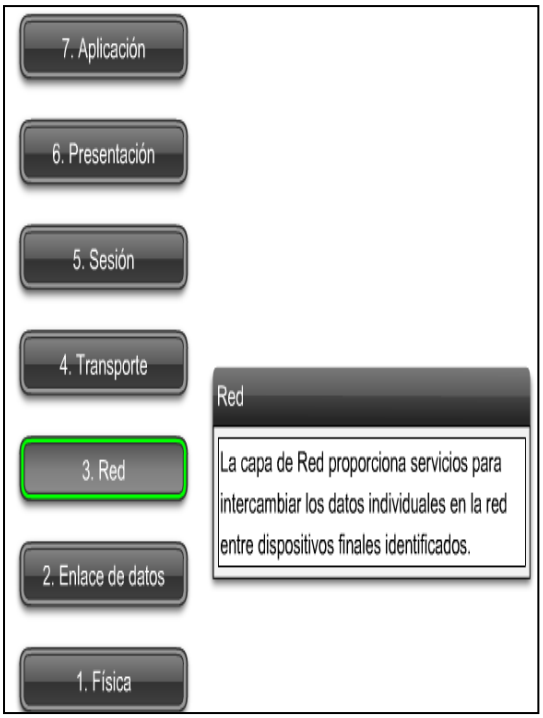
Tenga en cuenta que, mientras las capas del modelo TCP/IP se mencionan sólo por el nombre, las siete capas del modelo OSI (Fig. 1.19) se mencionan con frecuencia por número y no por nombre.






7. Aplicación
6. Presentación
5. Sesión
4. Transporte
3. Red
2. Enlace de datos
1. Física
Sesión
La capa de Sesión proporciona servicios a la capa de Presentación para organizar su diálogo y administrar el intercambio de datos.


7. Aplicación
6. Presentación
5. Sesión
4. Transporte
3. Red
2. Enlace de datos
1. Física
Transporte
La capa de Transporte define los servicios para segmentar, transferir y reensamblar los datos para las comunicaciones individuales entre dispositivos finales.


7. Aplicación
6. Presentación
5. Sesión
4. Transporte
3. Red
2. Enlace de datos
1. Física
Red
La capa de Red proporciona servicios para intercambiar los datos individuales en la red entre dispositivos finales identificados.

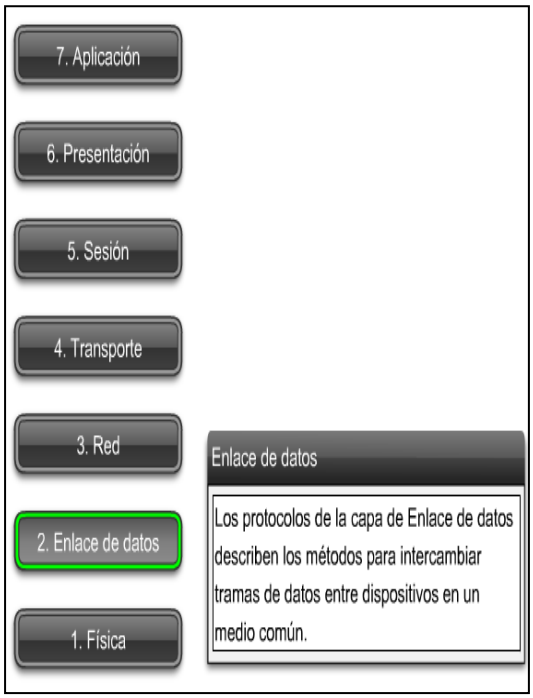

7. Aplicación
6. Presentación
5. Sesión
4. Transporte
3. Red
2. Enlace de datos
1. Física
Enlace de datos
Los protocolos de la capa de Enlace de datos describen los métodos para intercambiar tramas de datos entre dispositivos en un medio común.

Fig.1.19 Capas del Modelo OSI

1.15 Comparación del Modelo OSI y el modelo TCP/IP.

Los protocolos que forman la suite de protocolos TCP/IP pueden describirse en términos del modelo de referencia OSI. En el modelo OSI, la capa Acceso a la red y la capa Aplicación del modelo TCP/IP están subdivididas (Fig. 1.20) para describir funciones discretas que deben producirse en estas capas.

En la capa Acceso a la red, la suite de protocolos TCP/IP no especifica cuáles protocolos utilizar cuando se transmite por un medio físico; sólo describe la transferencia desde la capa de Internet a los protocolos de red física. Las Capas OSI 1 y 2 analizan los procedimientos necesarios para tener acceso a los medios y los medios físicos para enviar datos por una red.

Los paralelos clave entre dos modelos de red se producen en las Capas 3 y 4 del modelo OSI. La Capa 3 del modelo OSI, la capa Red, se utiliza casi universalmente para analizar y documentar el rango de los procesos que se producen en todas las redes de datos para direccionar y enrutar mensajes a través de una internetwork. El Protocolo de Internet (IP) es el protocolo de la suite TCP/IP que incluye la funcionalidad descrita en la Capa 3.

La Capa 4, la capa Transporte del modelo OSI, con frecuencia se utiliza para describir servicios o funciones generales que administran conversaciones individuales entre los hosts de origen y de destino. Estas funciones incluyen acuse de recibo, recuperación de errores y secuenciamiento. En esta capa, los protocolos TCP/IP, Protocolo de control de transmisión (TCP) y Protocolo de datagramas de usuario (UDP) proporcionan la funcionalidad necesaria.

La capa de aplicación TCP/IP incluye una cantidad de protocolos que proporcionan funcionalidad específica para una variedad de aplicaciones de usuario final. Las Capas 5, 6 y 7 del modelo OSI se utilizan como referencias para proveedores y programadores de software de aplicación para fabricar productos que necesitan acceder a las redes para establecer comunicaciones.

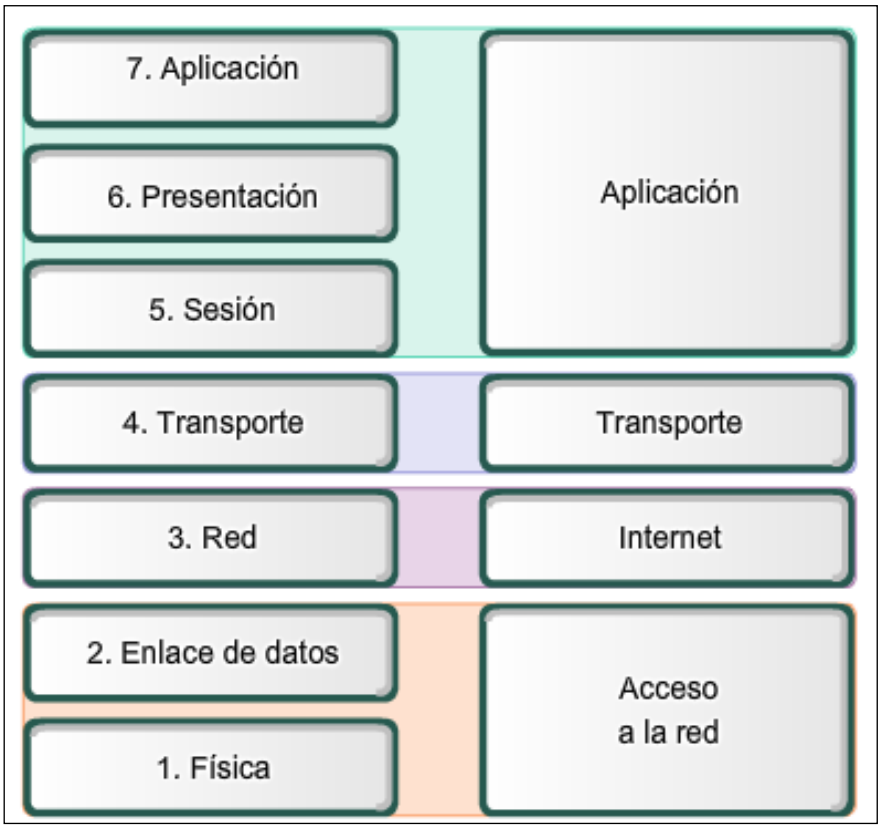


Fig.1.20 Comparación del Modelo OSI y el modelo TCP/IP

1.16 Direccionamiento en la red.

El modelo OSI describe los procesos de codificación, formateo, segmentación y encapsulación de datos para transmitir por la red. Un flujo de datos que se envía desde un origen hasta un destino se puede dividir en partes y entrelazar con los mensajes que viajan desde otros hosts hacia otros destinos. Miles de millones de estas partes de información viajan por una red en cualquier momento. Es muy importante que cada parte de los datos contenga suficiente información de identificación para llegar al destino correcto.

Existen varios tipos de direcciones que deben incluirse para entregar satisfactoriamente los datos desde una aplicación de origen que se ejecuta en un host hasta la aplicación de destino correcta que se ejecuta en otro. Al utilizan el modelo OSI como guía, se pueden observar las distintas direcciones e identificadores necesarios en cada capa, como se muestra en la Fig. 1.21.

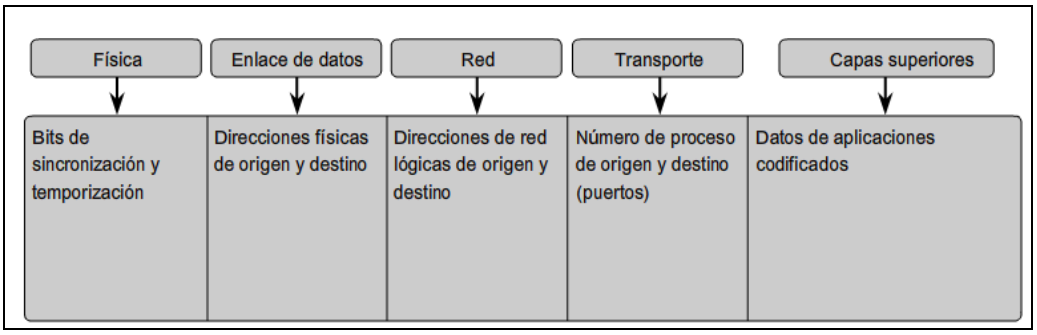


Fig.1.21Direccionamiento de la red.

Los protocolos de Capa 3 están diseñados principalmente para mover datos desde una red local a otra red local dentro de una internetwork. Mientras las direcciones de Capa 2 sólo se utilizan para comunicar entre dispositivos de una red local única, las direcciones de Capa 3 deben incluir identificadores que permitan a dispositivos de red intermediarios ubicar hosts en diferentes redes. En la suite de protocolos TCP/IP, cada dirección IP host contiene información sobre la red en la que está ubicado el host.

En los límites de cada red local, un dispositivo de red intermediario, por lo general un router, desencapsula la trama para leer la dirección host de destino contenida en el encabezado del paquete, la PDU de Capa 3. Los routers utilizan la porción

del identificador de red de esta dirección para determinar qué ruta utilizar para llegar al host de destino (Fig. 1.22) Una vez que se determina la ruta, el router encapsula el paquete en una nueva trama y lo envía por su trayecto hacia el dispositivo final de destino. Cuando la trama llega a su destino final, la trama y los encabezados del paquete se eliminan y los datos se suben a la Capa 4.

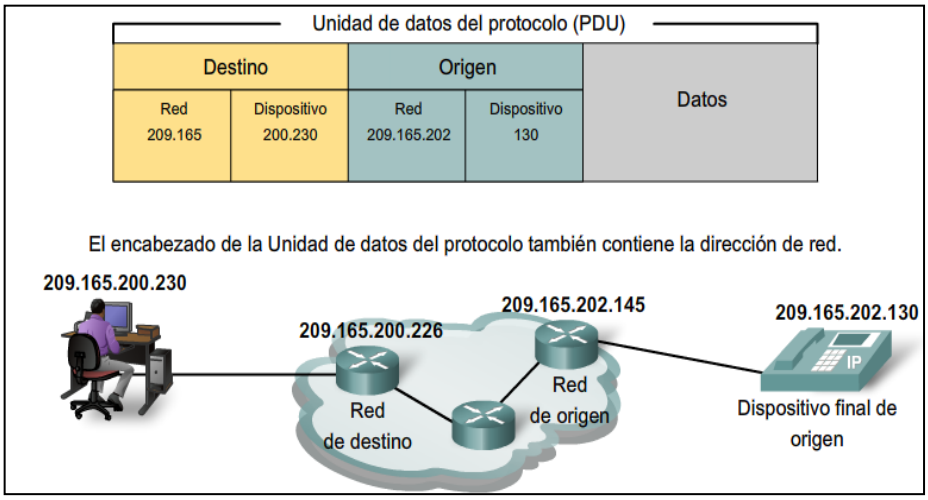


Fig.1.22 Ubicación de las partes en la red correcta.

En la Capa 4, la información contenida en el encabezado de la PDU no identifica un host de destino o una red de destino. Lo que sí identifica es el proceso o servicio específico que se ejecuta en el dispositivo host de destino que actuará en los datos que se entregan. Los hosts, sean clientes o servidores en Internet, pueden ejecutar múltiples aplicaciones de red simultáneamente. La gente que utiliza computadoras personales generalmente tiene un cliente de correo electrónico que se ejecuta al mismo tiempo que el explorador Web, un programa de mensajería instantánea, algún streaming media y, tal vez, incluso algún juego. Todos estos programas ejecutándose en forma separada son ejemplos de procesos individuales.

Ver una página Web invoca al menos un proceso de red. Hacer clic en un hipervínculo hace que un explorador Web se comunique con un servidor Web. Al mismo tiempo, en segundo plano, es posible que cliente de correo electrónico esté

enviando o recibiendo un e-mail y un colega o amigo enviando un mensaje instantáneo.

Piense en una computadora que tiene sólo una interfaz de red. Todos los streams de datos creados por las aplicaciones que se están ejecutando en la PC ingresan y salen a través de esa sola interfaz, sin embargo los mensajes instantáneos no emergen en el medio del documento del procesador de textos o del e-mail que se ve en un juego.

Esto es así porque los procesos individuales que se ejecutan en los hosts de origen y de destino se comunican entre sí. Cada aplicación o servicio es representado por un número de puerto en la Capa 4. Un diálogo único entre dispositivos se identifica con un par de números de puerto de origen y de destino de Capa 4 que son representativos de las dos aplicaciones de comunicación. (ver Fig. 1.23) Cuando los datos se reciben en el host, se examina el número de puerto para determinar qué aplicación o proceso es el destino correcto de los datos.

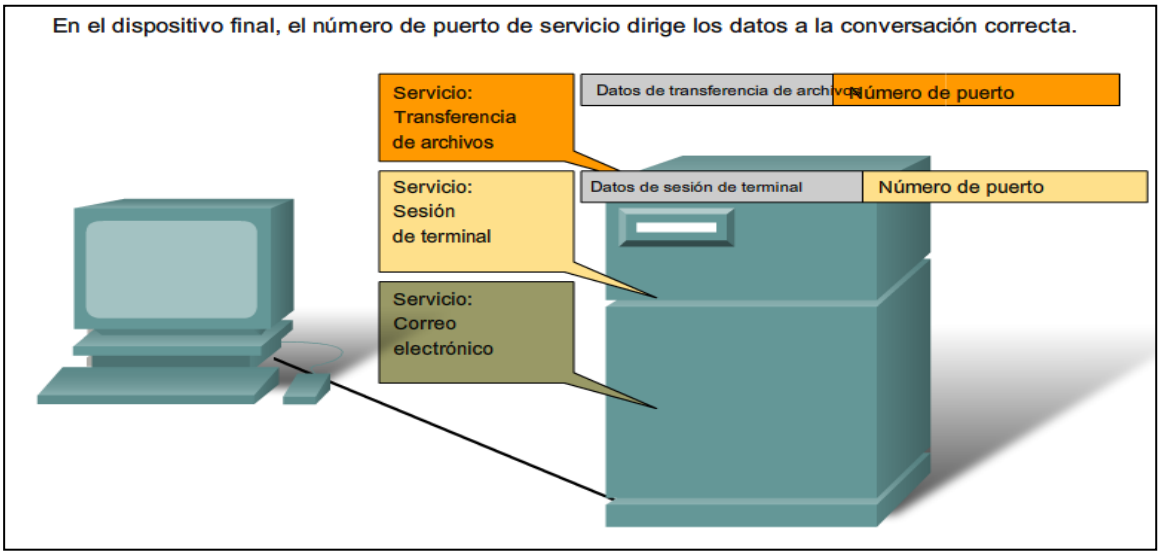


Fig.1.23 En el dispositivo final, el número de puerto de servicio dirige los datos a la conversación correcta.

CAPÍTULO 2.
ATAQUES MÁS COMUNES Y SEGURIDAD PERIMETRAL.

Debido a que el uso de Internet se encuentra en aumento, cada vez más compañías permiten a sus socios y proveedores acceder a sus sistemas de información. Por lo tanto, es fundamental saber qué recursos de la compañía necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información. Los mismos procedimientos se aplican cuando se permite el acceso a la compañía a través de Internet.

Además, debido a la tendencia creciente hacia un estilo de vida nómada de hoy en día, el cual permite a los empleados conectarse a los sistemas de información casi desde cualquier lugar, se pide a los empleados que lleven consigo parte del sistema de información fuera de la infraestructura segura de la compañía.

Los riesgos, en términos de seguridad, se caracterizan por lo general mediante la siguiente ecuación.

$$\text{Risque} = \frac{\text{Menace x Vulnérabilité}}{\text{Contre-mesure}}$$

La **amenaza** representa el tipo de acción que tiende a ser dañina, mientras que la **vulnerabilidad** (conocida a veces como *falencias (flaws)* o *brechas (breaches)*) representa el grado de exposición a las amenazas en un contexto particular. Finalmente, la **contramedida** representa todas las acciones que se implementan para prevenir la amenaza.

Las contramedidas que deben implementarse no sólo son soluciones técnicas, sino también reflejan la capacitación y la toma de conciencia por parte del usuario, además de reglas claramente definidas.

Para que un sistema sea seguro, deben identificarse las posibles amenazas y por lo tanto, conocer y prever el curso de acción del enemigo. Por tanto, el objetivo de este informe es brindar una perspectiva general de las posibles motivaciones de los hackers, categorizarlas, y dar una idea de cómo funciona para conocer la mejor forma de reducir el riesgo de intrusiones.

Generalmente, los sistemas de información incluyen todos los datos de una compañía y también en el material y los recursos de software que permiten a una compañía almacenar y hacer circular estos datos. Los sistemas de información son fundamentales para las compañías y deben ser protegidos.

Generalmente, la seguridad informática consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

La seguridad informática se resume, por lo general, en cinco objetivos principales:

- **Integridad**: garantizar que los datos sean los que se supone que son
- **Confidencialidad**: asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian
- **Disponibilidad**: garantizar el correcto funcionamiento de los sistemas de información
- **Evitar el rechazo**: garantizar de que no pueda negar una operación realizada.
- **Autenticación**: asegurar que sólo los individuos autorizados tengan acceso a los recursos

La **confidencialidad** consiste en hacer que la información sea ininteligible para aquellos individuos que no estén involucrados en la operación.

La verificación de la **integridad** de los datos consiste en determinar si se han alterado los datos durante la transmisión (accidental o intencionalmente.

El objetivo de la **disponibilidad** es garantizar el acceso a un servicio o a los recursos.

Evitar el repudio de información constituye la garantía de que ninguna de las partes involucradas pueda negar en el futuro una operación realizada.

La autenticación consiste en la confirmación de la identidad de un usuario; es decir, la garantía para cada una de las partes de que su interlocutor es realmente quien dice ser. Un control de acceso permite (por ejemplo gracias a una contraseña codificada) garantizar el acceso a recursos únicamente a las personas autorizadas.

2.1 Cómo implementar una política de seguridad.

Generalmente, la seguridad de los sistemas informáticos se concentra en garantizar el derecho a acceder a datos y recursos del sistema configurando los mecanismos de autentificación y control que aseguran que los usuarios de estos recursos sólo posean los derechos que se les han otorgado.

Los mecanismos de seguridad pueden sin embargo, causar inconvenientes a los usuarios. Con frecuencia, las instrucciones y las reglas se vuelven cada vez más complicadas a medida que la red crece. Por consiguiente, la seguridad informática debe estudiarse de modo que no evite que los usuarios desarrollen usos necesarios y así puedan utilizar los sistemas de información en forma segura.

Por esta razón, uno de los primeros pasos que debe dar una compañía es definir una política de seguridad que pueda implementar en función a las siguientes cuatro etapas:

- Identificar las necesidades de seguridad y los riesgos informáticos que enfrenta la compañía así como sus posibles consecuencias
- Proporcionar una perspectiva general de las reglas y los procedimientos que deben implementarse para afrontar los riesgos identificados en los diferentes departamentos de la organización
- Controlar y detectar las vulnerabilidades del sistema de información, y mantenerse informado acerca de las falencias en las aplicaciones y en los materiales que se usan
- Definir las acciones a realizar y las personas a contactar en caso de detectar una amenaza.

La política de seguridad comprende todas las reglas de seguridad que sigue una organización (en el sentido general de la palabra). Por lo tanto, la administración de la organización en cuestión debe encargarse de definirla, ya que afecta a todos los usuarios del sistema.

En este sentido, no son sólo los administradores de informática los encargados de definir los derechos de acceso sino sus superiores. El rol de un administrador de informática es el de asegurar que los recursos de informática y los derechos de

acceso a estos recursos coincidan con la política de seguridad definida por la organización.

Es más, dado que el/la administrador/a es la única persona que conoce perfectamente el sistema, deberá proporcionar información acerca de la seguridad a sus superiores, eventualmente aconsejar a quienes toman las decisiones con respecto a las estrategias que deben implementarse, y constituir el punto de entrada de las comunicaciones destinadas a los usuarios en relación con los problemas y las recomendaciones de seguridad.

La seguridad informática de una compañía depende de que los empleados (usuarios) aprendan las reglas a través de sesiones de capacitación y de concientización. Sin embargo, la seguridad debe ir más allá del conocimiento de los empleados y cubrir las siguientes áreas:

- Un mecanismo de seguridad física y lógica que se adapte a las necesidades de la compañía y al uso de los empleados
- Un procedimiento para administrar las actualizaciones
- Una estrategia de realización de copias de seguridad (backup) planificada adecuadamente
- Un plan de recuperación luego de un incidente
- Un sistema documentado actualizado

Las causas de inseguridad

Generalmente, la inseguridad se puede dividir en dos categorías:

- Un estado de inseguridad activo; es decir, la falta de conocimiento del usuario acerca de las funciones del sistema, algunas de las cuales pueden ser dañinas para el sistema (por ejemplo, no desactivar los servicios de red que el usuario no necesita)
- Un estado de inseguridad pasivo; es decir, la falta de conocimiento de las medidas de seguridad disponibles (por ejemplo, cuando el administrador usuario de un sistema no conocen los dispositivos de seguridad con los que cuentan).

La etapa de **definición** de las necesidades de seguridad es el primer paso hacia la implementación de una política de seguridad.

El objetivo es determinar las necesidades de organización mediante la redacción de un inventario del sistema de información y luego estudiar los diferentes riesgos y las distintas amenazas que representan para implementar una política de seguridad apropiada.

La etapa de definición se compone entonces de tres etapas:

- Identificación de las necesidades
- Análisis de los riesgos
- Definición de la política de seguridad

Identificación de las necesidades.

La etapa de identificación de las necesidades consiste en realizar en primer lugar un inventario del sistema de información, en particular de la siguiente información:

- Personas y funciones
- Materiales, servidores y los servicios que éstos brindan
- Esquematización de la red (esquema de direcciones, topologías físicas y lógicas, etc.)
- Lista de los nombres de dominio de la empresa.
- Infraestructura de la comunicación (routers, conmutadores, etc.)
- Información delicada.

Análisis de los riesgos.

La etapa de análisis de riesgos consiste en relevar los diferentes riesgos que se advierten, estimar sus probabilidades y, por último, estudiar su impacto.

La mejor forma de analizar el impacto de una amenaza consiste en calcular el costo de los daños que causaría (por ejemplo, un ataque a un servidor o un daño de los datos de vital importancia de la compañía).

Partiendo de esta base, sería interesante confeccionar una tabla de riesgos y de sus potencialidades (es decir, la probabilidad de que existan) dándoles niveles escalonados de acuerdo con una escala que debe definirse. Por ejemplo:

- Infundado (o improbable): la amenaza es insostenible
- Débil: la amenaza tiene pocas probabilidades de existir
- Moderada: la amenaza es real
- Alta: la amenaza tiene muchas probabilidades de existir.

Cómo definir la política de seguridad.

La política de seguridad es el documento de referencia que define los objetivos de seguridad y las medidas que deben implementarse para tener la certeza de alcanzar estos objetivos.

La política de seguridad define un número de reglas, procedimientos y prácticas óptimas que aseguren un nivel de seguridad que esté a la altura de las necesidades de la organización.

Este documento se debe presentar como un proyecto que incluya a todos, desde los usuarios hasta el rango más alto de la jerarquía, para ser aceptado por todos. Una vez redactada la política de seguridad, se deben enviar a los empleados las cláusulas que los impliquen para que la política de seguridad tenga el mayor impacto posible.

Etapa de implementación.

La etapa de implementación consiste en establecer los métodos y mecanismos diseñados para que el sistema de información sea seguro, y aplicar las reglas definidas en la política de seguridad.

Los principales mecanismos que se usan para asegurar una red contra intrusiones son los sistemas firewall. Sin embargo, este tipo de mecanismos no protege la confidencialidad de los datos que circulan en la red.

Por lo tanto, en la mayoría de los casos, es necesario usar algoritmos criptográficos, los cuales garantizan la confidencialidad del intercambio.

La configuración de una red virtual privada (VPN, por sus siglas en inglés) puede proporcionar seguridad adicional, ya que toda la información se halla codificada.

2.2 El concepto de auditoría.

Una auditoría de seguridad consiste en apoyarse en un tercero de confianza (generalmente una compañía que se especializada en la seguridad informática) para validar las medidas de protección que se llevan a cabo, sobre la base de la política de seguridad.

El objetivo de la auditoría es verificar que cada regla de la política de seguridad se aplique correctamente y que todas las medidas tomadas conformen un todo coherente.

Una auditoría de seguridad garantiza que el conjunto de disposiciones tomadas por la empresa se consideren seguras.

Prueba de intrusión.

Las pruebas de intrusión (abreviado como *pen tests [penetration tests, pruebas de penetración]*) consisten en probar los métodos de protección del sistema de información sometiendo el sistema a una situación real.

Generalmente, se utilizan dos métodos:

- El método de la caja negra, el cual consiste en intentar penetrar en la red sin tener conocimientos del sistema para generar una situación realista
- El método de la caja blanca que consiste en intentar penetrar en el sistema conociéndolo por completo para poner a prueba al máximo los límites de seguridad de la red

Es necesario el consentimiento (preferentemente por escrito) del nivel más alto de la jerarquía antes de realizar estas pruebas, debido a que pueden causar daños y a que los métodos utilizados se consideran ilegales sin la autorización expresa del propietario del sistema.

Una prueba de intrusión representa una buena forma de aumentar la conciencia de las personas involucradas en el proyecto cuando éste muestra una falencia. Por otro lado, no garantiza la seguridad del sistema, ya que quienes realizan las pruebas pueden obviar vulnerabilidades. Las auditorías de seguridad constituyen un método más eficaz para garantizar un nivel de seguridad superior en el

sistema, ya que en éstas se tiene en cuenta elementos organizacionales y humanos, y se analiza la seguridad en forma interna.

2.3 Etapa de detección de incidentes

Para ser completamente fiable, un sistema de información seguro debe aplicar medidas que permitan detectar incidentes.

Por consiguiente, existen sistemas de detección de intrusiones (o *IDS, por sus siglas en inglés*) que controlan la red y pueden activar una alarma cuando una solicitud resulta sospechosa o no cumple con la política de seguridad.

El uso de estas sondas investigativas y los parámetros relativos a éstas deben estudiarse cuidadosamente, ya que este tipo de mecanismo puede generar muchas falsas alarmas.

Es fundamental identificar las necesidades de seguridad de una organización para establecer las medidas que permitirán a dicha organización evitar una situación catastrófica, como una intrusión, una falla en los equipos o incluso un daño por filtración de agua. No obstante, es imposible evitar por completo todo tipo de riesgos, por lo que todas las empresas deben estar preparadas para experimentar algún día una situación catastrófica.

En estas circunstancias, resulta fundamental una reacción rápida, ya que una máquina afectada hace peligrar el sistema de información de la compañía en su totalidad. Además, cuando el compromiso provoca el mal funcionamiento del servicio, una interrupción prolongada puede aparejar pérdidas económicas. Por último, en los casos en los que se ha alterado un sitio web (modificación de páginas) la reputación de la compañía está en juego.

Etapa de reacción.

Generalmente, la etapa de reacción es la que menos se toma en cuenta en los proyectos de seguridad informática. Esta etapa consiste en prever eventos y planificar las medidas que deben tomarse si surge un problema.

En el caso de una intrusión, por ejemplo, el administrador de sistemas puede reaccionar de una de las siguientes maneras:

- Obtener la dirección del hacker y contraatacar
- Cortar el suministro eléctrico de la máquina
- Desconectar la máquina de la red
- Reinstalar el sistema.

El problema es que cada una de estas acciones puede resultar más perjudicial (particularmente en términos de costos) que la intrusión en sí misma. En efecto, si el funcionamiento de la máquina comprometida es fundamental para el funcionamiento del sistema de información o si se trata de un sitio web de ventas online, una interrupción prolongada del servicio podría ser catastrófica.

A su vez, en este tipo de situaciones es importante establecer pruebas en caso de que se realice una investigación judicial. De lo contrario, si la máquina comprometida se ha usado para realizar otro ataque, la compañía corre el riesgo de ser considerada responsable.

La implementación de un plan de recuperación de desastres permite a la organización evitar que el desastre empeore y tener la certeza de que todas las medidas tomadas para establecer pruebas se aplicarán correctamente.

Asimismo, un plan contra desastres desarrollado correctamente define las responsabilidades de cada individuo y evita que se emitan órdenes y contraórdenes, que impliquen una pérdida de tiempo.

Restauración.

En el plan de recuperación, se debe especificar en detalle cómo hacer que el sistema comprometido vuelva a funcionar correctamente. Es necesario tomar en cuenta los siguientes elementos:

- **Anotar la fecha de intrusión**: conocer la fecha aproximada en la que se ha comprometido la máquina permite a la organización evaluar el nivel de riesgo de intrusión para el resto de la red y el grado de compromiso de la maquina.
- **Restringir el compromiso**: tomar las medidas necesarias para que el compromiso no se expanda

- Estrategia de seguridad: si la compañía tiene una estrategia de seguridad, se recomienda comparar los cambios que se realizaron a los datos del sistema comprometido con los datos supuestamente fiables. Si los datos están infectados con un virus[1] o un troyano[2], la restauración de éstos puede expandir aún más el daño.

[1] **Un virus** es un pequeño programa informático que se encuentra dentro de otro programa que, una vez ejecutado, se carga solo en la memoria y cumple instrucciones programadas por su creador. La definición de un virus podría ser la siguiente:
"Cualquier programa de informática que puede infectar a otro programa alterándolo gravemente y que puede reproducirse".
El nombre real que corresponde a los virus es Código Auto Propagado pero por analogía con el campo de la medicina, se les dio el nombre de "virus".
Los virus residentes en la memoria (también llamados TSR por Terminate and Stay Resident (Terminar y permanecer residente en la memoria) se cargan en la RAM del ordenador para infectar los archivos ejecutables abiertos por el usuario. Los virus no residentes, una vez ejecutados, infectan programas que se encuentran en el disco duro.
Los efectos de un virus varían desde la simple visualización de una pelota de ping pong rebotando por toda la pantalla hasta un virus que elimina datos: éste es el tipo de virus más destructivo que existe. Al haber una amplia variedad con efectos muy variados, los virus no se clasifican según el tipo de daño que causan, sino de acuerdo con la forma en que se propagan e infectan ordenadores.
Por este motivo es que existen diferentes tipos de virus:
- Los gusanos son virus que se pueden propagar a través de una red.
- Los Troyanos son virus que crean un fallo en el ordenador (generalmente para que su diseñador acceda al sistema infectado y lo controle).
- Las bombas lógicas son virus que se pueden activar por un evento específico (por ejemplo, la fecha del sistema o por activación remota).

En los últimos años, ha surgido un nuevo fenómeno, el de los fraudes, es decir, avisos recibidos a través de correos electrónicos (por ejemplo, un informe sobre la aparición de un nuevo virus destructivo o la posibilidad de ganar un teléfono movil gratis). Los mensajes tienen una nota que indica al destinatario reenviar el mensaje a todas las personas que conoce. El propósito de esto es obstruir el tráfico de la red y propagar información falsa

[2] **Un Troyano** es un programa de informática que produce operaciones malintencionadas sin el conocimiento del usuario. El nombre "Troyano" proviene de una leyenda contada por los griegos en la Ilíada (escrita por Homero) sobre el bloqueo de la ciudad de Troya.
Según la leyenda, a los griegos, que no lograban traspasar las defensas de la ciudad de Troya, se les ocurrió la idea de abandonar el bloqueo y, en cambio, entregar una ofrenda a la ciudad: el regalo consistía en un caballo de madera gigante.
Los habitantes de Troya (Troyanos) aceptaron el regalo aparentemente inofensivo sin sospechar nada, y lo introdujeron dentro de los muros de la ciudad. Pero el caballo estaba lleno de soldados que esperaron a que la población se durmiera para salir del interior del caballo, abrir las puertas de la ciudad para facilitar la entrada del resto del ejército.
Volviendo al campo de la informática, se denomina Troyano a un programa oculto dentro de otro que ejecuta comandos furtivamente y que, por lo general, abre el acceso al ordenador y lo opera abriendo una puerta trasera. Por esta razón, a veces se lo conoce como Troyano por la analogía con los ciudadanos de Troya.
Similar a un virus, un Troyano es un código malicioso que se encuentra en un programa sano (por ejemplo, un comando falso para crear una lista de archivos que los destruye en lugar de mostrar la lista).
Un Troyano puede, por ejemplo:
- robar contraseñas
- copiar fechas confidenciales
- realizar cualquier otra operación maliciosa
- etc.

Y aún peor, este programa puede crear una infracción intencional de seguridad dentro de la red para que los usuarios externos puedan acceder a áreas protegidas de esa red.
Los Troyanos más comunes abren puertos en la máquina que permiten al diseñador tener acceso al ordenador a través de la red abriendo una puerta trasera. Por esta razón se usa frecuentemente el término puerta trasera u orificio trasero.

- Establecer pruebas: por razones legales, es necesario guardar los archivos de registro diario del sistema corrompido para poder restituirlos en caso de una investigación judicial
- Cómo configurar un sitio de reemplazo: en lugar de reinstalar el sistema comprometido, es preferible desarrollar y activar a tiempo un sitio de reemplazo que permita que el servicio continúe activo cuando sea necesario.

Práctica del plan contra desastres.

De la misma forma en que los simulacros de incendio son fundamentales para repasar un plan de escape en caso de incendio, la práctica del plan contra desastres permite a una organización confirmar que el plan funciona y garantizar que todas las personas involucradas sepan qué hacer.

2.4 ¿Qué es la seguridad de redes?

La seguridad de redes es un nivel de seguridad que garantiza que el funcionamiento de todas las máquinas de una red sea óptimo y que todos los usuarios de estas máquinas posean los derechos que les han sido concedidos:

Esto puede incluir:

- Evitar que personas no autorizadas intervengan en el sistema con fines malignos
- Evitar que los usuarios realicen operaciones involuntarias que puedan dañar el sistema
- Asegurar los datos mediante la previsión de fallas
- Garantizar que no se interrumpan los servicios

Las causas de inseguridad.

Generalmente, la inseguridad puede dividirse en dos categorías:

- Un **estado de inseguridad activo**, es decir, la falta de conocimiento del usuario acerca de las funciones del sistema, algunas de las cuales pueden

ser dañinas para el sistema (por ejemplo, no desactivar los servicios de red que el usuario no necesita)

- un **estado pasivo de inseguridad**; es decir, cuando el administrador (o el usuario) de un sistema no está familiarizado con los mecanismos de seguridad presentes en el sistema.

El objetivo de los atacantes.

Los atacantes (también denominados "piratas" o "hackers") pueden tener muchos motivos:

- La atracción hacia lo prohibido
- El deseo de obtener dinero (por ejemplo, violando el sistema de un banco)
- La reputación (impresionar a sus amigos)
- El deseo de hacer daño (destruir datos, hacer que un sistema no funcione)

El comportamiento del atacante.

Frecuentemente, el objetivo de los atacantes es controlar una máquina para poder llevar a cabo acciones deseadas. Existen varias formas de lograr esto:

- Obteniendo información que puede utilizarse en ataques
- Explotando las vulnerabilidades del sistema
- Forzando un sistema para irrumpir en él

¿Cómo es posible protegerse?

- Manténganse informado
- Conozca su sistema operativo
- Limite el acceso a la red (firewall)
- Limite el número de puntos de entrada (puertos)
- Defina una política de seguridad interna (contraseñas, activación de archivos ejecutables)
- Haga uso de utilidades de seguridad (registro)

2.5 Firewall

Cada ordenador que se conecta a internet (y, básicamente, a cualquier red de ordenadores) puede ser víctima del ataque de un hacker. La metodología que generalmente usan los hackers consiste en analizar la red (mediante el envío aleatorio de paquetes de datos) en busca de un ordenador conectado. Una vez que encuentra un ordenador, el hacker busca un punto débil en el sistema de seguridad para explotarlo y tener acceso a los datos de la máquina.

Por muchas razones, esta amenaza es aún mayor cuando la máquina está permanente conectada a internet:

- Es probable que la máquina elegida esté conectada pero no controlada.
- Generalmente, la máquina conectada que se elige posee un ancho de banda más elevado.
- La máquina elegida no cambia las direcciones IP o lo hace muy ocasionalmente.

Por lo tanto, es necesario que tanto las redes de las compañías como los usuarios de internet con conexiones por cable o ADSL se protejan contra intrusiones en la red instalando un dispositivo de protección.

¿Qué es un Firewall?

Un firewall como el que se muestra en la fig.2.1 es un sistema que protege a un ordenador o a una red de ordenadores contra intrusiones provenientes de redes de terceros (generalmente desde internet). Un sistema de firewall filtra paquetes de datos que se intercambian a través de internet. Por lo tanto, se trata de una pasarela de filtrado que comprende al menos las siguientes interfaces de red:

- Una interfaz para la red protegida (red interna)
- Una interfaz para la red externa.

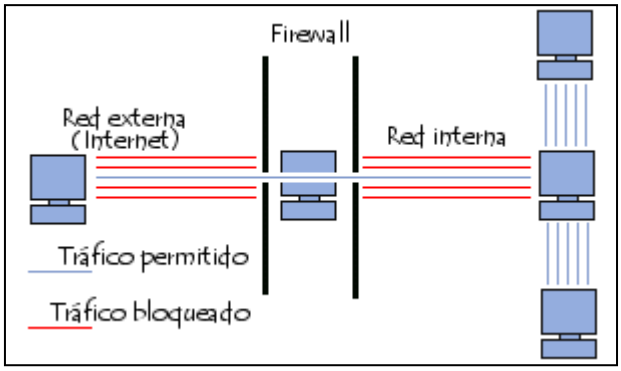


Fig. 2.1 Sistema Firewall.

El sistema firewall es un sistema de software, a menudo sustentado por un hardware de red dedicada, que actúa como intermediario entre la red local[3] (u ordenador local) y una o más redes externas. Un sistema de firewall puede instalarse en ordenadores que utilicen cualquier sistema siempre y cuando:

- La máquina tenga capacidad suficiente como para procesar el tráfico
- El sistema sea seguro
- No se ejecute ningún otro servicio más que el servicio de filtrado de paquetes en el servidor

En caso de que el sistema de firewall venga en una caja negra (llave en mano), se aplica el término "aparato".

Cómo funciona un sistema Firewall.

Un sistema firewall contiene un conjunto de reglas predeterminadas que le permiten al sistema:

- Autorizar la conexión (*permitir*)
- Bloquear la conexión (*denegar*)
- Rechazar el pedido de conexión sin informar al que lo envió (*negar*)

Todas estas reglas implementan un método de filtrado que depende de la **política de seguridad** adoptada por la organización. Las políticas de seguridad se dividen generalmente en dos tipos que permiten:

[3] Refererirse al capitulo 1

- La autorización de sólo aquellas comunicaciones que se autorizaron explícitamente:

  "todo lo que no se ha autorizado explícitamente está prohibido"
- El rechazo de intercambios que fueron prohibidos explícitamente

El primer método es sin duda el más seguro. Sin embargo, impone una definición precisa y restrictiva de las necesidades de comunicación.

2.6 Filtrado de paquetes Stateless[4].

Un sistema de firewall opera según el principio del filtrado simple de paquetes, o *filtrado de paquetes stateless*. Analiza el encabezado de cada paquete de datos (*datagrama*) que se ha intercambiado entre un ordenador de red interna y un ordenador externo.

Así, los paquetes de datos que se han intercambiado entre un ordenador con red externa y uno con red interna pasan por el firewall y contienen los siguientes encabezados, los cuales son analizados sistemáticamente por el firewall:

- La dirección IP del ordenador que envía los paquetes
- La dirección IP del ordenador que recibe los paquetes
- El tipo de paquete (TCP, UDP, etc.)
- El número de puerto (recordatorio: un puerto es un número asociado a un servicio o a una aplicación de red).

Las direcciones IP (como se muestra en la tabla 1) que los paquetes contienen permiten identificar el ordenador que envía los paquetes y el ordenador de destino, mientras que el tipo de paquete y el número de puerto indican el tipo de servicio que se utiliza.

La tabla 1 proporciona ejemplos de reglas del firewall:

Regla	Acción	IP fuente	IP destino	Protocolo	Puerto fuente	Puerto destino
1	Aceptar	192.168.10.20	194.154.192.3	tcp	cualquiera	25
2	Aceptar	cualquiera	192.168.10.3	tcp	cualquiera	80
3	Aceptar	192.168.10.0/24	cualquiera	tcp	cualquiera	80

[4] Un servidor sin estado es un servidor que trata cada petición como una organización independiente de transacciones que no está relacionado con la petición anterior.

4	Negar	cualquiera	cualquiera	cualquiera	cualquiera	cualquiera

Los puertos reconocidos[5] (cuyos números van del 0 al 1023) están asociados con servicios ordinarios (por ejemplo, los puertos 25 y 110 están asociados con el correo electrónico y el puerto 80 con la Web). La mayoría de los dispositivos de firewall se configuran al menos para filtrar comunicaciones de acuerdo con el puerto que se usa. Normalmente, se recomienda bloquear todos los puertos que no son fundamentales (según la política de seguridad vigente).

Por ejemplo, el puerto 23 a menudo se bloquea en forma predeterminada mediante dispositivos de firewall, ya que corresponde al protocolo TELNET, el cual permite a una persona emular el acceso terminal a una máquina remota para ejecutar comandos a distancia. Los datos que se intercambian a través de TELNET no están codificados. Esto significa que es probable que un hacker observe la actividad de la red y robe cualquier contraseña que no esté codificada. Generalmente, los administradores prefieren el protocolo SSH, el cual tiene la reputación de ser seguro y brinda las mismas funciones que TELNET.

2.7 Filtrado Dinámico.

El Filtrado de paquetes Stateless sólo intenta examinar los paquetes IP independientemente, lo cual corresponde al nivel 3 del modelo OSI (Interconexión de sistemas abiertos). Sin embargo, la mayoría de las conexiones son admitidas por el protocolo TCP, el cual administra sesiones, para tener la seguridad de que todos los intercambios se lleven a cabo en forma correcta. Asimismo, muchos servicios (por ejemplo, FTP) inician una conexión en un puerto estático. Sin

[5] Diversos programas TCP/IP pueden ejecutarse simultáneamente en Internet (por ejemplo, pueden abrirse diferentes navegadores de manera simultánea o navegar por páginas HTML mientras se descarga un archivo de un FTP). Cada uno de estos programas funciona con un protocolo. A veces el equipo debe poder distinguir las diferentes fuentes de datos.
Por lo tanto, para facilitar este proceso, a cada una de estas aplicaciones puede serle asignada una dirección única en equipo, codificada en 16 bits: un puerto (por consiguiente, la combinación de dirección IP + puerto es una dirección única en el mundo denominada socket).
De esta manera, la dirección IP sirve para identificar de manera única un equipo en la red mientras que el número de puerto especifica la aplicación a la que se dirigen los datos. Así, cuando el equipo recibe información que va dirigida a un puerto, los datos se envían a la aplicación relacionada. Si se trata de una solicitud enviada a la aplicación, la aplicación se denomina aplicación servidor. Si se trata de una respuesta, entonces hablamos de una aplicación cliente.

embargo, abren un puerto en forma dinámica (es decir, aleatoria) para establecer una sesión entre la máquina que actúa como servidor y la máquina cliente.

De esta manera, con un filtrado de paquetes stateless, es imposible prever cuáles puertos deberían autorizarse y cuáles deberían prohibirse Para solucionar este problema, el sistema de **filtrado dinámico de paquetes** se basa en la inspección de las capas 3 y 4 del modelo OSI, lo que permite controlar la totalidad de las transacciones entre el cliente y el servidor. El término que se usa para denominar este proceso es "**inspección stateful**" o "*filtrado de paquetes stateful*".

Un dispositivo de firewall con "inspección stateful" puede asegurar el control de los intercambios. Esto significa que toma en cuenta el estado de paquetes previos cuando se definen reglas de filtrado. De esta manera, desde el momento en que una máquina autorizada inicia una conexión con una máquina ubicada al otro lado del firewall, todos los paquetes que pasen por esta conexión serán aceptados implícitamente por el firewall.

El hecho de que el filtrado dinámico sea más efectivo que el filtrado básico de paquetes no implica que el primero protegerá el ordenador contra los hackers que se aprovechan de las vulnerabilidades de las aplicaciones. Aún así, estas vulnerabilidades representan la mayor parte de los riesgos de seguridad.

Filtrado de aplicaciones.

El filtrado de aplicaciones permite filtrar las comunicaciones de cada aplicación. El filtrado de aplicaciones opera en el nivel 7 (capa de aplicaciones) del modelo OSI, a diferencia del filtrado simple de paquetes (nivel 4). El filtrado de aplicaciones implica el conocimiento de los protocolos utilizados por cada aplicación.

Como su nombre lo indica, el filtrado de aplicaciones permite filtrar las comunicaciones de cada aplicación. El filtrado de aplicaciones implica el conocimiento de las aplicaciones en la red y un gran entendimiento de la forma en que en ésta se estructuran los datos intercambiados (puertos, etc.).

Un firewall que ejecuta un filtrado de aplicaciones se denomina generalmente "pasarela de aplicaciones" o ("proxy"), ya que actúa como relé entre dos redes mediante la intervención y la realización de una evaluación completa del contenido

en los paquetes intercambiados. Por lo tanto, el proxy actúa como intermediario entre los ordenadores de la red interna y la red externa, y es el que recibe los ataques. Además, el filtrado de aplicaciones permite la destrucción de los encabezados que preceden los mensajes de aplicaciones, lo cual proporciona una mayor seguridad.

Este tipo de firewall es muy efectivo y, si se ejecuta correctamente, asegura una buena protección de la red. Por otra parte, el análisis detallado de los datos de la aplicación requiere una gran capacidad de procesamiento, lo que a menudo implica la ralentización de las comunicaciones, ya que cada paquete debe analizarse minuciosamente.

Además, el proxy debe interpretar una gran variedad de protocolos y conocer las vulnerabilidades relacionadas para ser efectivo.

Finalmente, un sistema como este podría tener vulnerabilidades debido a que interpreta pedidos que pasan a través de sus brechas. Por lo tanto, el firewall (dinámico o no) debería disociarse del proxy para reducir los riesgos de comprometer al sistema.

El concepto de Firewall personal.

El término **firewall personal** se utiliza para los casos en que el área protegida se limita al ordenador en el que el firewall está instalado.

Un firewall personal permite controlar el acceso a la red de aplicaciones instaladas en el ordenador y prevenir notablemente los ataques de programas como los troyanos[6], es decir, programas dañinos que penetran en el sistema para permitir

[6] **Síntomas de infección**
La infección de un Troyano generalmente aparece después de abrir un archivo contaminado que contiene el Troyano (consulte el artículo acerca de cómo protegerse de los gusanos) y la infección es evidente por los siguientes síntomas:
Actividad anormal del módem, adaptador de red o disco duro: los datos se cargan aunque el usuario no registre actividad.
Reacciones extrañas del ratón.

- Programas que se abren en forma inesperada.
- Bloqueos repetidos.
- Principio de un Troyano

Debido a que generalmente un Troyano intenta (y cada vez con más frecuencia) abrir un puerto en la máquina para que un hacker pueda controlarla (por ejemplo, mediante el robo de datos personales almacenados en el disco duro), el primer objetivo del hacker es infectar la máquina obligando a abrir un archivo infectado que contiene el Troyano y, luego, acceder a la máquina a través del puerto abierto.
Sin embargo, para poder infiltrar la máquina, el hacker usualmente conoce su dirección de IP. Entonces:
Usted puede tener una dirección de IP asignada (como ocurre con las empresas, personas que tienen una conexión por cable o similar, etc.), en ese caso esa dirección de IP se puede averiguar fácilmente,

que un hacker controle el ordenador en forma remota. Los firewalls personales permiten subsanar y prevenir intrusiones de aplicaciones no autorizadas a conectarse a su ordenador.

Limitaciones del Firewall.

Por supuesto que los sistemas firewall no brindan seguridad absoluta; todo lo contrario. Los firewalls sólo ofrecen protección en tanto todas las comunicaciones salientes pasen sistemáticamente a través de éstos y estén configuradas correctamente. Los accesos a la red externa que sortean el firewall también son puntos débiles en la seguridad. Claramente, éste es el caso de las conexiones que se realizan desde la red interna mediante un módem o cualquier otro medio de conexión que evite el firewall.

Asimismo, la adición de medios externos de almacenamiento a los ordenadores de sobremesa o portátiles de red interna puede dañar enormemente la política de seguridad general.

Para garantizar un nivel máximo de protección, debe ejecutarse un firewall en el ordenador y su registro de actividad debe controlarse para poder detectar intentos de intrusión o anomalías. Además, se recomienda controlar la seguridad (por ejemplo, inscribiéndose para recibir alertas de seguridad de CERT) a fin de modificar los parámetros del dispositivo de firewall en función de las alertas publicadas.

---

puede tener una dirección de IP dinámica (reasignada cada vez que se conecta), como en el caso de las conexiones por módem. En este caso, el hacker debe analizar la dirección IP aleatoriamente para detectar aquellas que corresponden a máquinas infectadas.

Protección contra Troyanos

La instalación de un firewall (programa que filtra los datos que entran y salen de su máquina) es suficiente para protegerlo de este tipo de intrusión. Un firewall controla tanto los datos que salen de su máquina (generalmente iniciados por los programas que está utilizando) como los que se introducen en ella. Sin embargo, el firewall puede detectar conexiones externas de las víctimas previstas de un hacker. Éstas pueden ser pruebas realizadas por su proveedor de servicios de Internet o un hacker que está analizando de forma aleatoria una cantidad de direcciones de IP.

Existen dos firewalls gratuitos y muy útiles para los sistemas Windows:

- ZoneAlarm
- Tiny Personal Firewall

En caso de infección

El firewall pide la confirmación de la acción antes de iniciar una conexión si un programa, cuyos orígenes desconoce, intenta abrir una conexión. Es muy importante que no autorice conexiones para un programa que desconoce porque podría tratarse de un Troyano.

Si esto vuelve a ocurrir, es conveniente verificar que su ordenador no esté infectado con un Troyano usando un programa que los detecta y elimina. (denominadobouffe-troyen).

La instalación de un firewall debe llevarse a cabo de la mano de una política de seguridad real.

2.8 DMZ (Zona desmilitarizada).

El concepto de Aislamiento

Los sistemas Firewall permiten definir las reglas de acceso entre dos redes. Sin embargo, en la práctica, las compañías cuentan generalmente con varias subredes con diferentes políticas de seguridad. Por esta razón, es necesario configurar arquitecturas de firewall que aíslen las diferentes redes de una compañía. Esto se denomina "aislamiento de la red".

Arquitectura DMZ.

Cuando algunas máquinas de la red interna deben ser accesibles desde una red externa (servidores web, servidores de correo electrónico, servidores FTP[7]), a veces es necesario crear una nueva interfaz hacia una red separada a la que se pueda acceder tanto desde la red interna como por vía externa sin correr el riesgo de comprometer la seguridad de la compañía. El término "zona desmilitarizada" o DMZ hace referencia a esta zona aislada que posee aplicaciones disponibles para el público. La DMZ actúa como una "zona de búfer" entre la red que necesita protección y la red hostil.

Los servidores en la DMZ se denominan "**anfitriones bastión**" ya que actúan como un puesto de avanzada en la red de la compañía.

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

- El tráfico de la red externa a la DMZ está **autorizado**
- El tráfico de la red externa a la red interna está **prohibido**

---

7 El protocolo FTP (Protocolo de transferencia de archivos) es, como su nombre lo indica, un protocolo para transferir archivos.
La implementación del FTP se remonta a 1971 cuando se desarrolló un sistema de transferencia de archivos (descrito en RFC141) entre equipos del Instituto Tecnológico de Massachusetts (MIT, Massachusetts Institute of Technology). Desde entonces, diversos documentos de RFC (petición de comentarios) han mejorado el protocolo básico, pero las innovaciones más importantes se llevaron a cabo en julio de 1973.
El protocolo FTP define la manera en que los datos deben ser transferidos a través de una red TCP/IP.
El objetivo del protocolo FTP es:

- permitir que equipos remotos puedan compartir archivos
- permitir la independencia entre los sistemas de archivo del equipo del cliente y del equipo del servidor
- permitir una transferencia de datos eficaz

- El tráfico de la red interna a la DMZ está **autorizado**
- El tráfico de la red interna a la red externa está **autorizado**
- El tráfico de la DMZ a la red interna está **prohibido**
- El tráfico de la DMZ a la red externa está **denegado**

De esta manera, la DMZ posee un nivel de seguridad intermedio, el cual no es lo suficientemente alto para almacenar datos imprescindibles de la compañía.
Debe observarse que es posible instalar las DMZ en forma interna para aislar la red interna con niveles de protección variados y así evitar intrusiones[8] internas.

2.9 El concepto de NAT

El proceso de la traducción de direcciones de red (NAT, por sus siglas en inglés) se desarrolló en respuesta a la falta de direcciones de IP[9] con el protocolo IPv4 (el protocolo IPv6[10] propondrá una solución a este problema).

---

[8] **El término IDS** (Sistema de detección de intrusiones) hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.
Existen dos claras familias importantes de IDS:

- El grupo N-IDS (Sistema de detección de intrusiones de red), que garantiza la seguridad dentro de la red.
- El grupo H-IDS (Sistema de detección de intrusiones en el host), que garantiza la seguridad en el host.

Un N-IDS necesita un hardware exclusivo. Éste forma un sistema que puede verificar paquetes de información que viajan por una o más líneas de la red para descubrir si se ha producido alguna actividad maliciosa o anormal. El N-IDS pone uno o más de los adaptadores de red exclusivos del sistema en modo promiscuo. Éste es una especie de modo "invisible" en el que no tienen dirección IP. Tampoco tienen una serie de protocolos asignados. Es común encontrar diversos IDS en diferentes partes de la red. Por lo general, se colocan sondas fuera de la red para estudiar los posibles ataques, así como también se colocan sondas internas para analizar solicitudes que hayan pasado a través del firewall o que se han realizado desde dentro.

9 Una dirección IP es una dirección de 32 bits, escrita generalmente con el formato de 4 números enteros separados por puntos. Una dirección IP tiene dos partes diferenciadas:

- los números de la izquierda indican la red y se les denomina netID (identificador de red).
- los números de la derecha indican los equipos dentro de esta red y se les denomina host-ID (identificador de host).

[10] **El protocolo IPv6** responde razonablemente a los objetivos fijados. Conserva las mejores funciones de IPv4, mientras que elimina o minimiza las peores y agrega nuevas cuando es necesario.
En general, IPv6 no es compatible con IPv4, pero es compatible con todos los demás protocolos de Internet, incluyendo TCP, UDP, ICMP, IGMP, OSPF, BGP y DNS. A veces se requieren modificaciones mínimas (particularmente, cuando se trabaja con direcciones extensas).
La principal innovación de IPv6 es el uso de direcciones más extensas que con IPv4. Están codificadas con 16 bytes y esto permite que se resuelva el problema que hizo que IPv6 esté a la orden del día: brindar un conjunto prácticamente ilimitado de direcciones de Internet.
IPv4 puede admitir 2^32=4,29.10^9 direcciones mientras que IPv6 puede admitir 2^128=3,4.10^38 direcciones.
La mejora más importante de IPv6 es la simplificación de los encabezados de los datagramas. El encabezado del datagrama IPv6 básico contiene sólo 7 campos (a diferencia de los 14 de IPv4). Este cambio permite que los routers procesen datagramas de manera más rápida y mejore la velocidad en general.
La tercera mejora consiste en ofrecer mayor flexibilidad respecto de las opciones. Este cambio es esencial en el nuevo encabezado, ya que los campos obligatorios de la versión anterior ahora son opcionales.

En efecto: en la asignación de direcciones IPv4, no hay suficientes direcciones IP enrutables (es decir, únicas en el mundo) para permitir que todas las máquinas que necesiten conectarse a internet puedan hacerlo.

El concepto de NAT como se muestra en la fig. 2.2 consiste en utilizar una dirección IP enrutable (o un número limitado de direcciones IP) para conectar todas las máquinas a través de la traducción, en la pasarela de internet, entre la dirección interna (no enrutable) de la máquina que se desea conectar y la dirección IP de la pasarela.

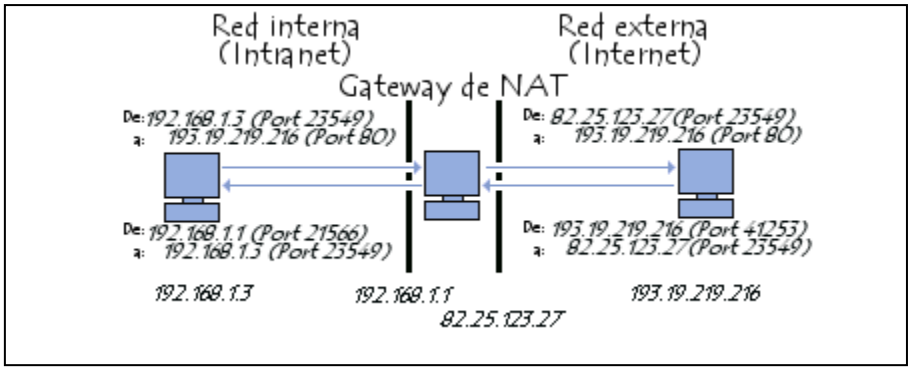


Fig. 2.2 Concepto NAT.

Además, el proceso de traducción de direcciones permite a las compañías **asegurar** la red interna siempre y cuando oculte la asignación de direcciones internas. Para un observador que se ubica fuera de la red, todos los pedidos parecen provenir de la misma dirección IP.

Espacio para la dirección.

El organismo que administra el espacio público de direcciones (direcciones IP enrutables) es el *Organismo de Asignación de Números en Internet* (IANA, por sus siglas en inglés). El RFC 1918 define un espacio para direcciones privadas que permite a organizaciones asignar direcciones IP a sus máquinas con redes internas sin correr el riesgo de entrar en conflicto con una dirección IP pública

Además, la manera en la que las opciones están representadas es distinta, dado que permite que los routers simplemente ignoren las opciones que no están destinadas a ellos. Esta función agiliza los tiempos de procesamiento de datagramas. Además, IPv6 brinda más seguridad.

asignada por IANA. Estas direcciones, conocidas como no enrutables, corresponden a los siguientes rangos de direcciones:

- Clase A: va desde 10.0.0.0 hasta 10.255.255.255
- Clase B: va desde 172.16.0.0 hasta 172.31.255.255 va desde 10.16.0.0 hasta 172.31.255.255
- Clase C: va desde 192.168.0.0 hasta 192.168.255.55 va desde 192.168.0.0 hasta 172.31.255.255

Todas las máquinas de una red interna que están conectadas a internet a través de un router y que no poseen una dirección IP pública deben utilizar una dirección que se encuentre dentro de uno de estos rangos. Para redes francesas pequeñas, generalmente se utiliza el rango de direcciones que va desde 192.168.0.1 hasta 192.168.0.255.

Traducción estática.

El concepto de NAT estática consiste en hacer coincidir una dirección IP pública con una dirección IP de red privada interna. Un router[11] (o, más precisamente, la pasarela[12]) hace coincidir una dirección IP privada (por ejemplo, *192.168.0.1*) con una dirección IP pública enrutable en internet y, en cierto sentido, realiza la traducción mediante la modificación de la dirección en el paquete IP.

La traducción de las direcciones estáticas permite conectar máquinas de red interna a internet de manera transparente, aunque no resuelve el problema de escasez de direcciones debido a que se necesitan n direcciones IP enrutables para conectar n máquinas de la red interna.

11 **Un router** es un dispositivo de interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.
Cuando un usuario accede a una URL, el cliente web (navegador) consulta al servidor de nombre de dominio, el cual le indica la dirección IP del equipo deseado.

12 **Una pasarela** de aplicación (gateway) es un sistema de hardware/software para conectar dos redes entre sí y para que funcionen como una interfaz entre diferentes protocolos de red.
Cuando un usuario remoto contacta la pasarela, ésta examina su solicitud. Si dicha solicitud coincide con las reglas que el administrador de red ha configurado, la pasarela crea una conexión entre las dos redes. Por lo tanto, la información no se transmite directamente, sino que se traduce para garantizar una continuidad entre los dos protocolos.
El sistema ofrece (además de una interfaz entre dos tipos de redes diferentes), seguridad adicional, dado que toda la información se inspecciona minuciosamente (lo cual puede generar demora) y en ocasiones se guarda en un registro de eventos.
La principal desventaja de este sistema es que debe haber una aplicación de este tipo disponible para cada servicio (FTP, HTTP, Telnet, etc.).

Traducción dinámica.

La NAT dinámica permite compartir una dirección IP enrutable (o una cantidad reducida de direcciones IP enrutables) entre varias máquinas con direcciones privadas. Así, todas las máquinas de la red interna poseen la misma dirección IP virtual en forma externa. Por esta razón, el término "**enmascaramiento de IP**" se usa en ciertos casos para procesar la NAT dinámica.

Para poder "multiplexar" (compartir) diferentes direcciones IP con una o más direcciones IP enrutables, la NAT dinámica utiliza la **traducción de direcciones de puerto**, es decir, la asignación de un puerto de origen diferente para cada solicitud, de modo que se pueda mantener una correspondencia entre los pedidos que provienen de la red interna y las respuestas de las máquinas en internet, las cuales están dirigidas a la dirección IP del router.

Presentación de la tecnología RAID.

La tecnología RAID (sigla que significa *Redundant Array of Inexpensive Disks, conjunto redundante de discos de bajo costo*, o en algunos casos *Redundant Array of Independent Disks, conjunto redundante de discos independientes*) permite al usuario formar una unidad de almacenamiento a partir de varios discos rígidos. Por tanto, la unidad creada (denominada clúster) es altamente tolerante a los errores (disponibilidad alta) o posee una mayor capacidad/velocidad de escritura. La distribución de datos en varios discos rígidos proporciona una mayor seguridad de los datos y servicios asociados más fiables.

Esta tecnología fue desarrollada en 1987 por tres investigadores (*Patterson*, *Gibson* y *Katz*) en la Universidad de California (Berkeley). Desde 1992, la junta consultiva para el uso de sistemas RAID (RAID Advisory Board) ha administrado estas especificaciones. Estas consisten en la formación de una unidad con gran capacidad (y por lo tanto costosa) a partir de unidades más pequeñas y económicas (es decir, unidades en las que el MTBF, *Mean Time Between Failure [tiempo medio entre fallos]*, sea corto).

Con la tecnología RAID, los discos unidos pueden utilizarse de maneras diferentes, denominadas niveles RAID. La Universidad de California ha definido 5

niveles, a los que se han agregado los niveles 0 y 6. Cada uno de estos niveles describe la forma en la que se distribuyen los datos en las unidades:

- **Nivel 0**: denominado configuración en bandas (striping)
- **Nivel 1**: Nivel 1: denominado réplica (mirroring), emulación (shadowing) o duplicación (duplexing)
- **Nivel 2**: Nivel 2: denominado configuración en bandas con paridad (obsoleto)
- **Nivel 3**: Nivel 3: denominado conjunto de discos con datos entrelazados en bits
- **Nivel 4**: Nivel 4: denominado conjunto de discos con datos entrelazados en bloques
- **Nivel 5**: Nivel 5: denominado conjunto de discos con paridad distribuida de entrelazado de bloques
- **Nivel 6**: Nivel 5: denominado conjunto de discos con paridad distribuida de entrelazado de bloques

Cada uno de estos niveles constituye una forma de utilizar el clúster, según:

- El rendimiento
- El costo
- El acceso a los discos.

Nivel 0.

El nivel RAID-0, denominado de configuración en bandas (striping, concepto al que a veces se denomina erróneamente *stripping*) consiste en almacenar datos distribuyéndolos en todas las unidades de clúster. Este nivel no tiene redundancia alguna y por tanto no tolera errores. De hecho, si falla una de las unidades, los datos divididos y distribuidos por todas las unidades se perderán.

Sin embargo, dado que cada unidad del clúster posee su propio controlador, esta solución ofrece una velocidad de transferencia elevada.

El RAID-0 (ver tabla 2) supone la yuxtaposición lógica (agregación) de varios discos rígidos físicos. En el modo RAID-0, los datos se anotan en *bandas* (traducción del término inglés "stripes"):

Tabla 2

Unidad 1	Unidad 2	Unidad 3
Banda 1	Banda 2	Banda 3
Banda 4	Banda 5	Banda 6
Banda 7	Banda 8	Banda 9

El término "striping" se utiliza para caracterizar el tamaño relativo de los fragmentos (*bandas*) almacenadas en cada unidad física. La salida promedio depende de este factor (cuanto más cortas sean las bandas, mejor serán las salidas)

Si alguno de los elementos del clúster es más grande que el resto, el sistema que se usa para almacenar datos en las unidades se bloqueará cuando el disco más pequeño se llene. Por tanto, el tamaño final equivale al doble de la capacidad del más pequeño de los dos discos:

- Dos unidades de 20 GB equivalen a una unidad lógica de 40 GB
- Si una unidad de 10 GB se utiliza junto con una unidad de 27 Gb, se creará una unidad lógica de 20 Gb (17 GB de la segunda unidad quedarán entonces inutilizados)

Se recomienda utilizar dos discos del mismo tamaño para el RAID-0; de lo contrario, no se podrá explotar al máximo la unidad con mayor capacidad.

Nivel 1.

El objetivo del nivel 1 es duplicar la información y almacenarla en varias unidades. Los términos *réplica (mirroring)* o *emulación (shadowing)* se utilizan para describir este procedimiento, (tabla 3.).

Tabla 3

Unidad 1	Unidad 2	Unidad 3
Banda 1	Banda 1	Banda 1
Banda 2	Banda 2	Banda 2
Banda 3	Banda 3	Banda 3

El nivel 1 brinda una mayor seguridad de datos, ya que si una de las unidades falla los datos se guardan en la otra. Asimismo, la lectura de los datos puede ser mucho más rápida cuando ambos discos están en funcionamiento. Por último, dado que cada unidad tiene su propio controlador, el servidor puede continuar funcionando aún cuando una de las unidades falle, de la misma manera en que un camión puede seguir en movimiento si uno de sus neumáticos revienta, ya que posee varios neumáticos en cada eje.

Por el contrario, la tecnología RAID-1 es muy costosa si se tiene en cuenta que sólo se aprovecha la mitad de la capacidad de almacenamiento.

Nivel 2.

Actualmente el nivel RAID-2 es obsoleto, ya que utiliza un código Hamming para la corrección de errores (códigos ECC - *Error Correction Code (código de corrección de errores*). En la actualidad, el código Hamming se encuentra directamente integrado dentro de los controladores de los discos rígidos.

Esta tecnología consiste en el almacenamiento de datos bajo el mismo principio que se aplica al RAID-0, aunque la escritura de bits de verificación *ECC* se realiza en una unidad aparte (normalmente se utilizan 3 unidades ECC para 4 unidades de datos).

La tecnología RAID 2 ofrece rendimientos mediocres pero un alto nivel de seguridad.

Nivel 3.

La tecnología del nivel 3 RAID (Tabla 4) almacena datos en bytes en cada unidad y utiliza una de las unidades para almacenar un bit de paridad[13].

13 **La verificación de paridad** (a veces denominada VRC o verificación de redundancia vertical) es uno de los mecanismos de verificación más simples. Consiste en agregar un bit adicional (denominado bit de paridad) a un cierto número de bits de datos denominado palabra código (generalmente 7 bits, de manera que se forme un byte cuando se combina con el bit de paridad) cuyo valor (0 o 1) es tal que el número total de bits 1 es par. Para ser más claro, 1 si el número de bits en la palabra código es impar, 0 en caso contrario.

Tabla 4

Unidad 1	Unidad 2	Unidad 3	Unidad 4
Byte 1	Byte 2	Byte 3	Paridad 1+2+3
Byte 4	Byte 5	Byte 6	Paridad 4+5+6
Byte 7	Byte 8	Byte 9	Paridad 7+8+9

De esta manera, si uno de los discos fallara, sería posible reconstituir la información a partir de las demás unidades. Luego de reconstituir la información, el contenido de la unidad con fallos volvería a estar completo. Por otro lado, si dos de las unidades fallaran en forma simultánea, sería entonces imposible recuperar cualquier dato perdido.

Nivel 4.

La tecnología RAID 4 es muy similar a la del nivel 3. La diferencia reside en el nivel de paridad: El nivel 4 utiliza striping a nivel de bloque con un disco de paridad dedicado, mientras que el nivel 3 utiliza striping a nivel de byte. Más precisamente, esto significa que el striping es diferente al del RAID 3 (Tabla 5).

Tabla 5

Unidad 1	Unidad 2	Unidad 3	Unidad 4
Bloque 1	Bloque 2	Bloque 3	Paridad 1+2+3
Bloque 4	Bloque 5	Bloque 6	Paridad 4+5+6
Bloque 7	Bloque 8	Bloque 9	Paridad 7+8+9

Para leer una cantidad reducida de bloques, no es necesario que el sistema acceda a unidades físicas múltiples, sino solamente a aquéllas en las que los datos están realmente almacenados. Por el contrario, la unidad que posee los datos de control debe tener un tiempo de acceso equivalente a la suma del tiempo de acceso de los demás discos para no limitar el rendimiento del conjunto.

Nivel 5.

El nivel 5 es similar al nivel 4, es decir que la paridad se calcula a nivel del bloque pero se distribuye en todas las unidades del clúster (Tabla 6).

Tabla 6

Unidad 1	Unidad 2	Unidad 3	Unidad 4
Bloque 1	Bloque 2	Bloque 3	Paridad 1+2+3
Bloque 4	Paridad 4+5+6	Bloque 5	Bloque 6
Paridad 7+8+9	Bloque 7	Bloque 8	Bloque 9

De esta manera, el RAID 5 mejora en gran medida el acceso a los datos (tanto en escritura como en lectura) ya que el acceso a los bits de paridad se distribuye en las diferentes unidades del clúster.

RAID-5 brinda rendimientos muy similares a los obtenidos en RAID-0 al tiempo que asegura una alta tolerancia de errores. Por este motivo, es uno de los mejores modos RAID en términos de rendimiento y confiabilidad.

Ya que el espacio utilizable de unidad en un clúster de *n* unidades equivale a *n-1* unidades, se recomienda contar con un gran número de unidades para lograr que el RAID 5 sea más "rentable".

Nivel 6.

Se agregó el nivel 6 a los niveles definidos por los investigadores de Berkeley. Se define el uso de dos funciones de paridad y su almacenamiento en dos unidades dedicadas. Este nivel asegura redundancia en caso de que ambas unidades se dañen simultáneamente. Esto significa que se necesitan al menos 4 unidades para implementar el sistema RAID-6.

Comparación

Las soluciones RAID que generalmente se utilizan son los niveles 1 y 5.

La elección de una solución RAID depende de tres criterios:

- **Seguridad**: Tanto el RAID 1 como el 5 ofrecen un alto nivel de seguridad. Sin embargo, el método de reconstrucción de unidades es diferente en cada solución. Si el sistema falla, el RAID 5 reconstruye la unidad que falta con la información almacenada en las otras unidades, mientras que RAID 1 proporciona una copia en cada unidad.
- **Rendimiento**: El RAID 1 ofrece un mayor rendimiento que el RAID 5 en términos de lectura, pero su rendimiento es menor en términos de escritura.

- **Costo**: el costo está directamente vinculado a la capacidad de almacenamiento que debe implementarse para tener una capacidad efectiva específica. La solución RAID 5 ofrece un volumen utilizable que representa entre el 80 y el 90% del volumen asignado. (el resto se utiliza para la corrección de errores). Por otro lado, el volumen disponible de la solución RAID 1 constituye sólo el 50% del volumen total (si se tiene en cuenta que la información se duplica).

2.10 Cómo implementar la solución RAID

Hay diferentes maneras de implementar una solución RAID en un servidor.

- **RAID basado en software**: Generalmente, aquí se necesita un driver en el nivel del sistema operativo del ordenador que sea capaz de crear un volumen lógico con varias unidades (SCSI o IDE).
- **RAID basado en hardware:**
- **Con los DASD** (*Direct Access Storage Device, dispositivo de almacenamiento de acceso directo*): unidades de almacenamiento externo con fuente de alimentación propia. Además, estos dispositivos cuentan con conectores que permiten el cambio de unidades mientras se encuentran encendidos (dichas unidades son "*intercambiables en caliente*"). Estos dispositivos administran sus unidades en forma automática, por lo que se los reconoce como unidades SCSI estándares.
- **Con controladores RAID**: tarjetas que se colocan en ranuras de expansión PCI o ISA y que permiten el control de varios discos rígidos.

2.11 Fuente de alimentación ininterrumpible.

Una fuente de alimentación ininterrumpible (*UPS,* por sus siglas en inglés) es un dispositivo que protege equipos electrónicos contra posibles fallas eléctricas. Un UPS es un dispositivo conectado entre la red eléctrica (conectado a la alimentación de la empresa eléctrica) y los materiales que necesitan protección.

El UPS permite que los materiales reciban alimentación de una batería de emergencia durante varios minutos en caso de que se produzcan problemas eléctricos, en especial durante:

- Interferencias en la red eléctrica; es decir, un corte de electricidad de un segundo que puede provocar que el ordenador se reinicie
- Cortes de electricidad, correspondientes a una interrupción en la fuente de alimentación por un tiempo determinado
- Sobrevoltaje; es decir, un valor nominal mayor que el valor máximo previsto para el funcionamiento normal de los aparatos eléctricos
- Baja tensión, es decir, un valor nominal menor al valor mínimo previsto para el funcionamiento normal de los aparatos eléctricos
- Picos de voltaje; es decir, sobrevoltajes transitorios (de corta duración) de amplitud alta. Estos picos ocurren cuando se apagan y se encienden dispositivos que demandan mucha alimentación. Con el tiempo, esto puede ocasionar daños a los componentes eléctricos
- Descargas de rayos, las cuales constituyen una fuente extrema de sobrevoltaje que se produce repentinamente durante el mal tiempo (tormentas)

Los sistemas de informática toleran la mayoría de las interrupciones eléctricas. Sin embargo, a veces pueden causar la pérdida de datos, la interrupción de los servicios, e incluso daños materiales.

El UPS contribuye a la "disminución" del voltaje, es decir, elimina los picos que sobrepasan ciertos niveles. Cuando se produce un corte de electricidad, la energía almacenada en la batería de emergencia mantiene la fuente de alimentación, suministrando electricidad a los equipos durante un período de tiempo reducido (generalmente de 5 a 10 minutos). Más allá de los minutos de autonomía que brinda el UPS, este tiempo ganado permite también que el equipo se conecte a otras fuentes de energía. Algunos UPS también pueden conectarse directamente al ordenador (por ejemplo, con un cable USB) para que este pueda apagarse por sí solo ante un corte de electricidad, evitándose así la pérdida de datos.

Tipos de UPS

Generalmente existen tres tipos de UPS:

- "Los UPS "**fuera de línea**" se conectan a través de un relé eléctrico. Cuando todo funciona de manera adecuada, se utiliza el voltaje de la red eléctrica para recargar las baterías. Cuando la batería supera o se encuentra debajo de cierto nivel (máximo o mínimo), el relé se abre y el voltaje se regenera mediante el uso de la energía almacenada en la batería. Debido al tiempo que se necesita para que el relé se abra y se cierre, este tipo de UPS no ofrece protección contra interferencias en la red eléctrica.
- "Los UPS "**en línea**" se conectan en serie y regulan el voltaje constantemente.
- "Los UPS "**interactivos en línea** cuentan con tecnología híbrida. Los UPS *interactivos en línea* se conectan en forma paralela a través de un relé, pero cuentan con un microprocesador que controla el voltaje constantemente. En caso de una caída de voltaje leve o una interferencia en la red eléctrica, el UPS puede inyectar voltaje para compensar. Sin embargo, en los casos en que se produzca un corte total de electricidad, el UPS funcionará como un UPS fuera de línea.

Características de una fuente de alimentación ininterrumpible.

El tiempo de protección eléctrica que brinda un UPS se expresa en VA (*voltios-amperios*). Generalmente, para contar con protección eléctrica durante un corte de electricidad de 10 minutos, es necesario un UPS con una capacidad equivalente a la alimentación de todos los materiales conectados al UPS multiplicada por 1,6.

Al escoger un UPS, también es importante verificar la cantidad de sockets (tomas de alimentación) que posee.

En algunos casos, los UPS tienen conectores (USB, de red, paralelos, etc.) que permiten conectarlos al CPU para que éste se apague automáticamente si se produce un corte de electricidad durante un tiempo prolongado y para realizar copias de seguridad de todo el trabajo no terminado.

Debe tenerse en cuenta que los UPS no protegen conexiones telefónicas. Por consiguiente, un ordenador conectado a un UPS al mismo tiempo que a un módem puede aún dañarse si la descarga de rayo tiene impacto sobre la línea telefónica.

Cuartos de autosuficiencia.

En el caso de aquellas compañías en las que es fundamental contar con una alimentación eléctrica constante, es posible instalar una serie de UPS en un cuarto denominado "cuarto de autosuficiencia".

Estas cámaras están generalmente equipadas con decenas o incluso cientos de UPS capaces de proporcionar alimentación eléctrica durante un corte de electricidad de varias horas. Las cámaras de "autosuficiencia" también pueden incluir un generador que continúe proporcionando electricidad una vez agotada la energía de los UPS.

2.12 Tipos de Ataques.

Scanning.

El scaneo, como método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo. La idea es recorrer (scanear) tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular. Muchas utilidades de auditoría también se basan en este paradigma

El Scaneo de puertos pertenece a la Seguridad Informática desde que era utilizado en los sistemas de telefonía. Dado que actualmente existen millones de números de teléfono a los que se pueden acceder con una simple llamada, la solución lógica (para encontrar números que puedan interesar) es intentar conectarlos a todos.

La idea básica es simple: llamar a un número y si el módem devuelve un mensaje de conectado, grabar el número. En otro caso, la computadora cuelga el teléfono y llama al siguiente número. Scanear puertos implica las mismas técnicas de fuerza bruta. Se envía una serie de paquetes para varios protocolos y se deduce que

servicios están "escuchando" por las respuestas recibidas o no recibidas. Existen diversos tipos de Scanning según las técnicas, puertos y protocolos explotados:

TCP Connect, Scanning.

Esta es la forma básica del scaneo de puertos TCP. Si el puerto está escuchando, devolverá una respuesta de éxito; cualquier otro caso significará que el puerto no está abierto o que no se puede establecer conexión con a él.

Las ventajas que caracterizan esta técnica es que no necesita de privilegios especiales y su gran velocidad.

Su principal desventaja es que este método es fácilmente detectable por el Administrador del sistema. Se verá un gran número de conexiones y mensajes de error para los servicios en los que se ha conseguido conectar la máquina que lanza el scanner e inmediatamente se ha desconectado.

TCP SYN Scanning.

Cuando dos procesos establecen una comunicación usan el modelo Cliente/Servidor para establecer la conexión. La aplicación del Servidor "escucha" todo lo que ingresa por los puertos. La identificación del Servidor se efectúa a través de la dirección IP del sistema en el que se ejecuta y del número de puerto del que depende para la conexión. El Cliente establece la conexión con el Servidor a través del puerto disponible para luego intercambiar datos.

La información de control llamada HandShake (saludo) se intercambia entre el Cliente y el Servidor para establecer un dialogo antes de transmitir datos.

Los "paquetes" o segmentos TCP tienen banderas que indican el estado del mismo.

El protocolo TCP de Internet, sobre el que se basa la mayoría de los servicios (incluyendo el correo electrónico, el web y el IRC) implica esta conexión entre dos máquinas. El establecimiento de dicha conexión se realiza mediante lo que se llama Three-Way Handshake ("conexión en tres pasos") ya intercambian tres segmentos. En forma esquemática se tiene:

1. El programa Cliente (C) pide conexión al Servidor (S) enviándole un segmento SYN (Synchronize Sequence Number). Este segmento le dice a S que C desea establecer una conexión.
2. S (si está abierto y escuchando) al recibir este segmento SYN (activa su indicador SYN) y envía una autentificación ACK de manera de acuse de recibo a C. Si S está cerrado envía un indicador RST.
3. C entonces ACKea (autentifica) a S. Ahora ya puede tener lugar la transferencia de datos.

Cuando las aplicaciones conectadas terminan la transferencia, realizaran otra negociación a tres bandas con segmentos FIN en vez SYN.
La técnica TCP SYN Scanning, se implementa un scaneo de "media-apertura", dado que nunca se abre una sesión TCP completa. Se envía un paquete SYN (como si se fuera a usar una conexión real) y se espera por la respuesta. Al recibir un SYN/ACK se envía, inmediatamente, un RST para terminar la conexión y se registra este puerto como abierto.
La principal ventaja de esta técnica de escaneo es que pocos sitios están preparados para registrarlos. La desventaja es que en algunos sistemas Unix, se necesitan privilegios de Administrador para construir estos paquetes SYN.

TCP FIN Scanning- Stealth Port Scanning.
Hay veces en que incluso el scaneo SYN no es lo suficientemente "clandestino" o limpio. Algunos sistemas (Firewalls y filtros de paquetes) monitorizan la red en busca de paquetes SYN a puertos restringidos. Para subsanar este inconveniente los paquetes FIN, en cambio, podrían ser capaces de pasar sin ser advertidos. Este tipo de Scaneo está basado en la idea de que los puertos cerrados tienden a responder a los paquetes FIN con el RST correspondiente. Los puertos abiertos, en cambio, suelen ignorar el paquete en cuestión.
Este es un comportamiento correcto del protocolo TCP, aunque algunos sistemas (entre los que se hallan los de Microsoft(r)) no cumplen con este requerimiento, enviando paquetes RST siempre, independientemente de si el puerto está abierto

o cerrado. Como resultado, no son vulnerables a este tipo de scaneo. Sin embargo, es posible realizarlo en otros sistemas Unix.

Este último es un ejemplo en el que se puede apreciar que algunas vulnerabilidades se presentan en las aplicación de tecnologías (en este caso el protocolo TCP nacido en los años ´70) y no sobre sus implementaciones. Es más, se observa que una implementación incorrecta (la de Microsoft(r)) soluciona el problema. "Muchos de los problemas globales de vulnerabilidades son inherentes al diseño original de algunos protocolos".

Fragmentation Scanning.

Esta no es una nueva técnica de scaneo como tal, sino una modificación de las anteriores. En lugar de enviar paquetes completos de sondeo, los mismos se particionan en un par de pequeños fragmentos IP. Así, se logra partir una cabecera IP en distintos paquetes para hacerlo más difícil de monitorizar por los filtros que pudieran estar ejecutándose en la máquina objetivo.

Sin embargo, algunas implementaciones de estas técnicas tienen problemas con la gestión de este tipo de paquetes tan pequeños, causando una caída de rendimiento en el sistema del intruso o en el de la víctima. Problemas de esta índole convierte en detectables a este tipo de ataque.

Eavesdropping-Packet Sniffing.

Muchas redes son vulnerables al Eavesdropping, o a la pasiva intercepción (sin modificación) del tráfico de red. Esto se realiza con Packet Sniffers, los cuales son programas que monitorean los paquetes que circulan por la red. Los Sniffers pueden ser colocados tanto en una estación de trabajo conectada a la red, como a un equipo Router o a un Gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

En la cabecera de los paquetes enviados a través de una red, entre otros datos, se tiene, la dirección del emisor y la del destinatario. De esta forma, independientemente de protocolo usado, las tramas llegan a su destino. Cada máquina conectada a la red (mediante una placa con una dirección única) verifica

la dirección destino del paquete. Si estas direcciones son iguales asume que el paquete enviado es para ella, caso contrario libera el paquete para que otras placas lo analicen.

Un Sniffers consiste en colocar a la placa de red en un modo llamado promiscuo, el cual desactiva el filtro de verificación de direcciones y por lo tanto todos los paquetes enviados a la red llegan a esta placa (computadora donde está instalado el Sniffer).Inicialmente este tipo de software, era únicamente utilizado por los Administradores de redes locales, aunque con el tiempo llegó a convertirse en una herramienta muy usada por los intrusos.

Actualmente existen Sniffers para capturar cualquier tipo de información específica. Por ejemplo passwords de un recurso compartido o de acceso a una cuenta, que generalmente viajan sin encriptar al ingresar a sistemas de acceso remoto. También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mails entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos. Para realizar estas funciones se analizan las tramas de un segmento de red, y presentan al usuario sólo las que interesan.

Normalmente, los buenos Sniffers, no se pueden detectar, aunque la inmensa mayoría, y debido a que están demasiado relacionados con el protocolo TCP/IP, si pueden ser detectados con algunos trucos.

Snooping – Downloading.

Los ataques de esta categoría tienen el mismo objetivo que el Sniffing: obtener la información sin modificarla.

Sin embargo los métodos son diferentes. Aquí, además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de correo electrónico y otra información guardada, realizando en la mayoría de los casos un downloading (copia de documentos) de esa información a su propia computadora, para luego hacer un análisis exhaustivo de la misma.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos más

resonantes de este tipo de ataques fueron: el robo de un archivo con mas de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

2.13 Ataques de autentificación.

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

Spoofing – Looping.

Spoofing puede traducirse como "hacerse pasar por otro" y el objetivo de esta técnica, justamente, es actuar en nombre de otros usuarios, usualmente para realizar tareas de Snooping o Tampering (ver a continuación Ataques de Modificación y Daño). Una forma común de Spoofing es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y así sucesivamente. Este proceso, llamado Looping, y tiene la finalidad de "evaporar" la identificación y la ubicación del atacante.

El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país. Otra consecuencia del Looping es que una compañía o gobierno pueden suponer que están siendo atacados por un competidor o una agencia de gobierno extranjera, cuando en realidad están seguramente siendo atacado por un Insider, o por un estudiante a miles de Km de distancia, pero que ha tomado la identidad de otros.

La investigación de procedencia de un Looping es casi imposible, ya que el investigador debe contar con la colaboración de cada Administrador de cada red utilizada en la ruta. El envío de falsos e-mails es otra forma de Spoofing que las

redes permiten. Aquí el atacante envía E-Mails a nombre de otra persona con cualquier motivo y objetivo. Tal fue el caso de una universidad en EE.UU. que en 1998, que debió reprogramar una fecha completa de exámenes ya que alguien en nombre de la secretaría había cancelado la fecha verdadera y enviado el mensaje a toda la nómina de estudiantes.

Muchos ataques de este tipo comienzan con Ingeniería Social y los usuarios, por falta de cultura, facilitan a extraños sus identificaciones dentro del sistema usualmente través de una simple llamada telefónica.

Spoofing.

Este tipo de ataques (sobre protocolos) suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Los ataques tipo Spoofing bastante conocidos son el IP Spoofing, el DNS Spoofing y el Web Spoofing IP Spoofing

Con el IP Spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete. Su utilización más común es enviar los paquetes con la dirección de un tercero, de forma que la víctima "ve" un ataque proveniente de esa tercera red, y no la dirección real del intruso. El esquema con dos puentes es el siguiente:

Nótese que si la Victima descubre el ataque verá a la PC 3 como su atacante y no el verdadero origen.

DNS Spoofing.

Este ataque se consigue mediante la manipulación de paquetes UDP pudiéndose comprometer el servidor de nombres de dominios (Domain Name Server-DNS) de Windows NT(c). Si se permite el método de recursión en la resolución de "Nombre “Dirección IP" en el DNS, es posible controlar algunos aspectos del DNS remoto. La recursión consiste en la capacidad de un servidor de nombres para resolver una petición de dirección IP a partir de un nombre que no figura en su base de datos. Este es el método típico (y por defecto) de funcionamiento.

Web Spoofing.

En el caso Web Spoofing el atacante crea un sitio web completo (falso) similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante, permitiéndole monitorizar todas las acciones de la víctima, desde sus datos hasta las passwords, números de tarjeta de créditos, etc. El atacante también es libre de modificar cualquier dato que se esté transmitiendo entre el servidor original y la víctima o viceversa.

IP Splicing – Hijacking.

Se produce cuando un atacante consigue interceptar una sesión ya establecida. El atacante espera a que la víctima se identifique ante el sistema y tras ello le suplanta como usuario autorizado.

Utilización de BackDoors.

"Las puertas traseras son trozos de código en un programa que permiten a quien las conoce saltarse los métodos usuales de autentificación para realizar ciertas tareas. Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo".

Esta situación se convierte en una falla de seguridad si se mantiene, involuntaria o intencionalmente, una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control normales.

Utilización de Exploits.

Es muy frecuente ingresar a un sistema explotando agujeros en los algoritmos de encriptación utilizados, en la administración de las claves por parte la empresa, o simplemente encontrado un error en los programas utilizados.

Los programas para explotar estos "agujeros" reciben el nombre de Exploits y lo que realizan es aprovechar la debilidad, fallo o error hallado en el sistema (hardware o software) para ingresar al mismo. Nuevos Exploits (explotando nuevos errores en los sistemas) se publican cada día por lo que mantenerse

informado de los mismos y de las herramientas para combatirlos es de vital importancia.

Obtención de Passwords.

Este método comprende la obtención por "Fuerza Bruta" de aquellas claves que permiten ingresar a los sistemas, aplicaciones, cuentas, etc. atacados. Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario y, además, esta nunca (o rara vez) se cambia. En esta caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la password correcta.

Uso de Diccionarios.

Los Diccionarios son archivos con millones de palabras, las cuales pueden ser passwords utilizadas por los usuarios. Este archivo es utilizado para descubrir dicha password en pruebas de fuerza bruta. El programa encargado de probar cada una de las palabras encripta cada una de ellas (mediante el algoritmo utilizado por el sistema atacado) y compara la palabra encriptada contra el archivo de passwords del sistema atacado (previamente obtenido). Si coinciden se ha encontrado la clave de acceso al sistema mediante el usuario correspondiente a la clave hallada. Actualmente es posible encontrar diccionarios de gran tamaño orientados, incluso, a un área específica de acuerdo al tipo de organización que se esté atacando.

2.14 Denial of Service (DOS).

Los protocolos existentes actualmente fueron diseñados para ser empleados en una comunidad abierta y con una relación de confianza mutua. La realidad indica que es más fácil desorganizar el funcionamiento de un sistema que acceder al mismo; así los ataques de Negación de Servicio tienen como objetivo saturar los

recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.

Jamming o Flooding.

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más pueda utilizarla.

Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP (usando Spoofing y Looping). El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas. Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Muchos Hosts de Internet han sido dados de baja por el "ping de la muerte" (una versión-trampa del comando ping). Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el bloqueo instantáneo del equipo. Esta vulnerabilidad ha sido ampliamente utilizada en el pasado pero, aún hoy pueden encontrarse sistemas vulnerables. Otra acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los sistemas destinos.

Syn Flood.

Como ya se explicó en el TCP SYN Scanning el protocolo TCP se basa en una conexión en tres pasos. Si el paso final no llega a establecerse, la conexión permanece en un estado denominado "semiabierto". El Syn Flood es el más famoso de los ataques del tipo Denial of Service, publicado por primera vez en la revista Phrack. Se basa en un "saludo" incompleto entre los dos hosts. El Cliente envía un paquete SYN pero no responde al paquete ACK ocasionando que la pila TCP/IP espere cierta cantidad de tiempo a que el host hostil responda antes de cerrar la conexión. Si se crean muchas peticiones incompletas de conexión (no se

responde a ninguna), el Servidor estará inactivo mucho tiempo esperando respuesta. Esto ocasiona la lentitud en los demás servicios.

El problema es que muchos sistemas operativos tienen un límite muy bajo en el número de conexiones "semiabiertas" que pueden manejar en un momento determinado. Si se supera ese límite, el servidor sencillamente dejará de responder a las nuevas peticiones de conexión que le vayan llegando. Las conexiones "semiabiertas" van caducando tras un tiempo, liberando "huecos" para nuevas conexiones, pero mientras el atacante mantenga el Syn Flood, la probabilidad de que una conexión recién liberada sea capturada por un nuevo SYN malicioso es muy alta.

La potencia de este ataque reside en que muchos sistemas operativos fijan un límite del orden de 5 a 30 conexiones "semiabiertas", y que éstas caducan alcabo de un par de minutos. Para mantener el servidor fuera de servicio, un atacante sólo necesita enviar un paquete SYN cada 4 segundos (algo al alcance de, incluso, un módem de 300 baudios). Este ataque suele combinarse también con el IP Spoofing, de forma de ocultar el origen del ataque.

Connection Flood.

La mayoría de las empresas que brindan servicios de Internet (ISP) tienen un límite máximo en el número de conexiones simultáneas. Una vez que se alcanza ese límite, no se admitirán conexiones nuevas. Así, por ejemplo, un servidor Web puede tener, por ejemplo, capacidad para atender a mil usuarios simultáneos. Si un atacante establece mil conexiones y no realiza ninguna petición sobre ellas, monopolizará la capacidad del servidor. Las conexiones van caducando por inactividad poco a poco, pero el atacante sólo necesita intentar nuevas conexiones, (como ocurre con el caso del Syn Flood) para mantener fuera de servicio el servidor.

Net Flood.

En estos casos, la red víctima no puede hacer nada. Aunque filtre el tráfico en sus sistemas, sus líneas estarán saturadas con tráfico malicioso, incapacitándolas

para cursar tráfico útil. Un ejemplo habitual es el de un teléfono: si alguien quiere molestar, sólo tiene que llamar, de forma continua. Si se descuelga el teléfono (para que deje de molestar), tampoco se puede recibir llamadas de otras personas. Este problema es habitual, por ejemplo, cuando alguien intenta mandar un fax empleando el número de voz: el fax insiste durante horas y sin que el usuario llamado pueda hacer nada al respecto.

En el caso de Net Flooding ocurre algo similar. El atacante envía tantos paquetes de solicitud de conexión que las conexiones auténticas simplemente no pueden competir. En casos así el primer paso a realizar es el ponerse en contacto con el Proveedor del servicio para que intente determinar la fuente del ataque y, como medida provisional, filtre el ataque en su extremo de la línea. El siguiente paso consiste en localizar las fuentes del ataque e informar a sus Administradores, ya que seguramente se estarán usando sus recursos sin su conocimiento y consentimiento. Si el atacante emplea Ip Spoofing, esto puede ser casi imposible, ya que en muchos casos la fuente del ataque es, a su vez, víctima y el origen último puede ser prácticamente imposible de determinar.

Land Attack.

Este ataque consiste en un Bug (error) en la implementación de la pila TCP/IP de las plataformas Windows(c). El ataque consiste en mandar a algún puerto abierto de un servidor (generalmente al 113 o al 139) un paquete, maliciosamente construido, con la dirección y puerto origen igual que la dirección y puerto destino. Por ejemplo se envían un mensaje desde la dirección 10.0.0.1:139 hacia ella misma. El resultado obtenido es que luego de cierta cantidad de mensajes enviados-recibidos la máquina termina colgándose.

Existen ciertas variantes a este método consistente, por ejemplo, en enviar el mensaje a una dirección específica sin especificar el puerto Smurf o Broadcast Storm. Este ataque es bastante simple y a su vez devastador. Consiste en recolectar una serie de direcciones para a continuación mandar una petición ICMP (simulando un Ping) a cada una de ellas en serie, varias veces, falsificando la dirección IP de origen. Este paquete maliciosamente manipulado, será repetido en

Broadcast, y cientos ó miles de hosts (según la lista de direcciones de Broadcast disponible) mandarán una respuesta a la víctima cuya dirección IP figura en el paquete ICMP.

Supernuke o Winnuke.

Un ataque característico (y quizás el más común) de los equipos con Windows(c) es el Nuke, que hace que los equipos que escuchan por el puerto UDP 137 a 139 (utilizados por los protocolos Netbios de Wins), queden fuera de servicio (o disminuyan su rendimientos) al enviarle paquetes UDP manipulados. Generalmente se envían fragmentos de paquetes, que la máquina víctima detecta como inválidos pasando a un estado inestable.

Teardrop I y II-Newtear-Bonk-Boink.

Al igual que el Supernuke, los ataques Teardrop I y Teardrop II afectan a fragmentos de paquetes. Algunas implementaciones de colas IP no vuelven a armar correctamente los fragmentos que se superponen, haciendo que el sistema se cuelgue. Windows NT(c) 4.0 de Microsoft(r) es especialmente vulnerable a este ataque. Aunque existen Patchs (parches) que pueden aplicarse para solucionar el problema, muchas organizaciones no lo hacen, y las consecuencias pueden devastadoras.

Los ataque tipo Teardrop son especialmente peligrosos ya que existen multitud de implementaciones (algunas de ellas forman paquetes), que explotan esta debilidad. Las más conocidas son aquellas con el nombre Newtear, Bonk y Boink.

E-Mail Bombing-Spamming.

El E-Mail Bombing consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando así mailbox del destinatario. Él Spamming, en cambio se refiere a enviar el e-mail miles de usuarios, haya estos solicitados el mensaje o no. Es muy utilizado por las empresas para publicitar sus productos. El Spamming está siendo actualmente tratado por las leyes europeas como una violación de los derechos de privacidad del usuario.

2.15 Ataques de modificación-daño.

Tampering o Data Diddling.

Esta categoría se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima (incluyendo borrado de archivos). Son particularmente serios cuando el que lo realiza ha obtenido derechos de Administrador o Supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema. Aún así, si no hubo intenciones de "bajar" el sistema por parte del atacante; el Administrador posiblemente necesite darlo de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada. Como siempre, esto puede ser realizado por Insiders o Outsiders, generalmente con el propósito de fraude o de dejar fuera de servicio a un competidor.

Son innumerables los casos de este tipo: empleados (o externos) bancarios que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule una deuda impositiva. Múltiples Web Sites han sido víctimas del cambio en sus páginas por imágenes (o manifiestos) terroristas o humorísticos, como el ataque de The Mentor, ya visto, a la NASA. Otras veces se reemplazan versiones de software por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos, etc.). La utilización de programas troyanos y difusión de virus esta dentro de esta categoría, y se profundizará sobre el tema en otra sección el presente capítulo.

Borrado de Huellas.

El borrado de huellas es una de las tareas más importantes que debe realizar el intruso después de ingresar en un sistema, ya que si se detecta su ingreso el Administrador buscará como conseguir "tapar el hueco" de seguridad, evitar ataques futuros e incluso rastrear al atacante. Las Huellas son todas las tareas que realizó el intruso en el sistema y por lo general son almacenadas en Logs (archivo que guarda la información de lo que se realiza en el sistema) por el

sistema operativo. Los archivos Logs son una de las principales herramientas (y el principal enemigo del atacante) con las que cuenta un Administrador para conocer los detalles de las tareas realizadas en el sistema y la detección de intrusos

Ataques Mediante Java Applets.

Java es un lenguaje de programación interpretado desarrollado inicialmente por SUN. Su mayor popularidad la merece en su alto grado de seguridad. Los más usados navegadores actuales, implementan Máquinas Virtuales Java (MVJ) para ser capaces de ejecutar programas (Applets) de Java. Estos Applets, al fin y al cabo no son más que código ejecutable y como tal, susceptible de ser manipulado por intrusos. Sin embargo, partiendo del diseño, Java siempre ha pensado en la seguridad del sistema. Las restricciones a las que somete a los Applets son de tal envergadura (imposibilidad de trabajar con ficheros a no ser que el usuario especifique lo contrario, imposibilidad de acceso a zonas de memoria y disco directamente, firma digital, etc.) que es muy difícil lanzar ataques. Sin embargo, existe un grupo de expertos especializados en descubrir fallas de seguridad en las implementaciones de las MVJ.

Ataques Mediante JavaScript y VBScript.

JavaScript (de empresa Netscape(r)) y VBScript (de Microsoft(r)) son dos lenguajes usados por los diseñadores de sitios Web evitando el uso de Java. Los programas realizados son interpretados por el navegador. Aunque los fallos son mucho más numerosos en versiones antiguas de JavaScript, se pueden encontrar algunos de los siguientes:

- Cuando apareció JavaScript, éste permitía el envío de mensajes de correo electrónico sin el reconocimiento del usuario, la lectura del historial de páginas visitadas, la lectura de directorios y de archivos. Estas fueron razón más que suficiente para que cientos de intrusos informáticos se aprovecharan de estas debilidades.
- El problema más importante apareció en Netscape 2.0 y fue bautizado como "Stuck On Load". Lo que sucedía es que se podía crear una ventana

de 1*1 pixeles, por la cual los intrusos podían seguir extrayendo información sin que el usuario se enterase y aún cuando éste hubiese salido de la página, ya que esta ventana (un simple punto en la pantalla) era imperceptible para el usuario.

Ataques Mediante ActiveX.

ActiveX es una de las tecnologías más potentes que ha desarrollado Microsoft(r). Mediante ActiveX es posible reutilizar código, descargar código totalmente funcional de un sitio remoto, etc. Esta tecnología es considerada la respuesta de Microsoft(r) a Java. ActiveX soluciona los problemas de seguridad mediante certificados y firmas digitales. Una Autoridad Certificadora (AC) expende un certificado que acompaña a los controles activos y a una firma digital del programador. Cuando un usuario descarga una página con un control, se le preguntará si confía en la AC que expendió el certificado y/o en el control ActiveX. Si el usuario acepta el control, éste puede pasar a ejecutarse sin ningún tipo de restricciones (sólo las propias que tenga el usuario en el sistema operativo). Es decir, la responsabilidad de la seguridad del sistema se deja en manos del usuario, ya sea este un experto cibernauta consciente de los riesgos que puede acarrear la acción o un perfecto novato en la materia.

Esta última características es el mayor punto débil de los controles ActiveX ya que la mayoría de los usuarios aceptan el certificado sin siquiera leerlo, pudiendo ser esta la fuente de un ataque con un control dañino.

La filosofía ActiveX es que las Autoridades de Certificación se fían de la palabra del programador del control. Es decir, el programador se compromete a firmar un documento que asegura que el control no es nocivo. Evidentemente siempre hay programadores con pocos escrúpulos o con ganas de experimentar. Así, un conocido grupo de hackers alemanes, desarrolló un control ActiveX maligno que modificaba el programa de Gestión Bancaria Personal Quicken95(c) de tal manera que si un usuario aceptaba el control, éste realizaba la tarea que supuestamente tenía que hacer y además modificaba el Quicken, para que la próxima vez que la

víctima se conectara a su banco, se iniciara automáticamente una transferencia a una cuenta del grupo alemán.

Otro control ActiveX muy especialmente "malévolo" es aquel que manipula el código de ciertos exploradores, para que éste no solicite confirmación al usuario a la hora de descargar otro control activo de la Web. Es decir, deja totalmente descubierto a ataques con tecnología ActiveX el sistema de la víctima. La autentificación de usuarios mediante Certificados y las Autoridades Certificadoras será abordada con profundidad en capítulos posteriores.

Ataques por Vulnerabilidades en los Navegadores.

Generalmente los navegadores no fallan por fallos intrínsecos, sino que fallan las tecnologías que implementan, aunque en este punto analizaremos realmente fallos intrínsecos de los navegadores, como pueden ser los "Buffer Overflow". Los "Buffer Overflows" consisten en explotar una debilidad relacionada con los buffers que la aplicación usa para almacenar las entradas de usuario. Por ejemplo, cuando el usuario escribe una dirección en formato URL ésta se guarda en un buffer para luego procesarla. Si no se realizan las oportunas operaciones de comprobación, un usuario podría manipular estas direcciones.

Los protocolo usado pueden ser HTTP, pero también otros menos conocidos, internos de cada explorador, como el "res:" o el "mk:". Precisamente existen fallos de seguridad del tipo "Buffer Overflow" en la implementación de estos dos protocolos. Para poder lanzar este tipo de ataques hay que tener un buen conocimiento de lenguaje Assembler y de la estructura interna de la memoria del Sistema Operativo utilizado. También se puede citar el fallo de seguridad descubierto por Cybersnot Industries(r) relativo a los ficheros ".lnk" y ".url"de Windows 95(c) y NT(c) respectivamente. Algunas versiones de Microsoft Internet Explorer(c) podían ser utilizadas para ejecutar la aplicación que se deseara siempre que existiera en el ordenador de la víctima (por ejemplo el tan conocido y temido format.com).

Para más información relacionada con los ataques intrínsecos a los navegadores, se aconsejan las páginas no oficiales de seguridad tanto en Internet Explorer(c) como en Netscape Communicator(c).

2.16 Explotación de errores de diseño, implementación y operación.

Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de "puertas invisibles" son descubiertas (cada día) en sistemas operativos, aplicaciones de software, protocolos de red, browsers de Internet, correo electrónico y todas clase de servicios informático disponible.

Los Sistemas operativos abiertos (como Unix y Linux) tienen agujeros mas conocidos y controlados que aquellos que existen en sistemas operativos cerrados (como Windows(c)). La importancia (y ventaja) del código abierto radica en miles de usuarios analizan dicho código en busca de posibles bugs y ayudan a obtener soluciones en forma inmediata.

Constantemente encontramos en Internet avisos de nuevos descubrimientos de problemas de seguridad (y herramientas de Hacking que los explotan), por lo que hoy también se hace indispensable contar con productos que conocen esas debilidades, puedan diagnosticarlas y actualizar el programa afectado con el parche adecuado.

CAPÍTULO 3.
IMPLEMENTACIÓN Y SOLUCIÓN DE UN CASO PRÁCTICO.

Al principio de su existencia, las redes de ordenadores fueron usadas generalmente para el envío de correo electrónico y para compartir recursos, generalmente impresoras, en empresas de mediano/gran tamaño. En estas condiciones la seguridad carecía prácticamente de importancia y no fue objeto de atención. Sin embargo, en la actualidad millones de ciudadanos usan redes para transacciones bancarias, compras, etc., la seguridad aparece como un problema potencial de grandes proporciones. Los problemas de seguridad de las redes pueden dividirse de forma general en cuatro áreas interrelacionadas:

El secreto, encargado de mantener la información fuera de las manos de usuarios no autorizados.

La validación de identificación, encargada de determinar la identidad de la persona/computadora con la que se está hablando.

El no repudio, encargado de asegurar la “firma” de los mensajes, de igual forma que se firma en papel una petición de compra/venta entre empresas.

El control de integridad, encargado de asegurar que el mensaje recibido fue el enviado por la otra parte y no un mensaje manipulado por un tercero.

Aunque muchos de estos problemas tratan de resolverse en capas de la red que se encuentran por debajo de la capa de aplicación, por ejemplo en la capa de red pueden instalarse muros de seguridad para mantener adentro (o afuera) los paquetes, en la capa de transporte pueden cifrarse conexiones enteras terminal a terminal, ninguna de ellas resuelve completamente los problemas de seguridad antes enumerados.

La resolución de estos problemas de seguridad se realiza como una parte previa o de apoyo de la capa de aplicación. A continuación se expondrán distintos trabajos que tratan de resolver cada uno de los cuatro problemas de seguridad planteados con anterioridad, esto es, el secreto, la validación de identificación, el no repudio y el control de integridad.

Antes de comenzar este capítulo, pasemos a realizar una serie de definiciones:

1. La Organización Internacional de Estándares (ISO), como parte de su norma 7498 en la que se establece el modelo de referencia para la interconexión de sistemas abiertos, define la ***seguridad informática como una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos***, donde un bien se define como algo de valor y la vulnerabilidad se define como la debilidad que se puede explotar para violar un sistema o la información que contiene. Para ello, se han desarrollado protocolos y mecanismos adecuados, para preservar la seguridad.
2. El **criptoanálisis**, es la ciencia que se encarga de descifrar los mensajes (los intrusos utilizan estas técnicas), mientras que la **criptografía** busca métodos más seguros de cifrado, y se puede clasificar en:

Criptografía clásica: cifrados rudimentarios basados en sustitución y trasposición

Criptografía moderna: cifrados basados en algoritmos parametrizados en base a claves.

“seguridad de una red” implica la seguridad de cada uno de las computadoras de la red

“hacker”: cualquier barrera es susceptible de ser superada y tiene como finalidad la de salir de un sistema informático (tras un ataque) sin ser detectado. Es un programador

“cracker”: no es un programado y utiliza sus ataques para sacar beneficio económico

“Amenaza o ataque”: intento de sabotear una operación o la propia preparación para sabotearla (poner en compromiso), que a su vez, estas amenazas se pueden realizar por:

Compromiso: la entidad atacante obtiene el control de algún elemento interno de la red, por *ejemplo utilizando cuentas con contraseña trivial o errores del sistem.*

Modificación: la entidad atacante modifica el contenido de algún mensaje o texto

Suplantación: la entidad atacante se hace pasar por otra persona **Reenvío**: la entidad atacante obtiene un mensaje o texto en tránsito y más tarde lo reenvía para duplicar su efecto **Denegación de servicio**: la entidad atacante impide que un elemento cumpla su función

También es importante resaltar, que los temas que vinculan a seguridad son muy peliagudos y están íntimamente relacionados con **temas legales**, los cuales no debemos de dejar de lado. Muestra de ello, es que en muchos gobiernos el uso de información cifrada está prohibido. Los Gobiernos tratan de implantar reglas (o estándares de cifrado) que ellos mismos puedan descifrar fácilmente. Por ejemplo en Francia y EEUU no están permitidas transacciones cifradas, que el gobierno no sea capaz de descifrar, pues pueden utilizarse para comercio de armas, delincuencia.

3.1 Seguridad perimetral.

La forma de resolver actualmente problemas de Seguridad Informática es diferente de cómo se realizaba años atrás. Se volvió más complejo debido a que ahora cuando se habla de “Seguridad” se involucrar a toda la organización. Pero no sólo eso sino la existencia de nuevas vulnerabilidades y amenazas y también la necesidad de mantener comunicación de forma global. Aquí es donde algunas soluciones empiezan a ser alcanzadas al proveer Disponibilidad, Integridad y Confiabilidad que requieren los Sistemas de Información.
Debido a que históricamente y conceptualmente se tiene el paradigma de que implantar un Firewall resolverá el grueso de los problemas perimetrales de seguridad, este trabajo presenta de forma general, la idea errónea y los problemas que también deben considerarse para establecer soluciones que sean adecuadas al entorno.
La Seguridad Perimetral, alternativas o soluciones propuestas y nuevas amenazas no son suficientes para tener el control de los Sistemas de Información.
En la historia de la Seguridad Informática una de sus principales preocupación es proteger el perímetro. Y cuando se logra proteger (el perímetro) se tiene cierta confianza en que los sistemas en el interior estarán seguros y la solución a todo el peligro se resolverá con un Firewall. Antes, el perímetro era claramente definido; por ejemplo, servidores y estaciones de trabajo en el mismo segmento lógico y físico de la red, (se) contaban únicamente con un enlace dedicado a Internet y solo era necesario permitir los puertos de los servicios de Internet necesarios.

Actualmente la situación de las redes corporativa es diferente, es decir, se tiene más de 1 enlace hacia Internet, redes inalámbricas, WAN, Redes Privadas Virtuales (VPN por sus siglas en Inglés), además de Servidores y Servicios que corren sobre la red y que son críticos para la organización. La Seguridad de la Información que fluye en arquitecturas como la planteada en el párrafo anterior es ahora más compleja que antes, las amenazas y vulnerabilidades cambian al igual que la tecnología y mantener una Seguridad Perimetral es mayor. Existe una gran cantidad de soluciones tecnológicas, Firewall 's corporativos con opción de VPN, cifrado de información, Firewall para estaciones de trabajo, soluciones de Antivirus para servidores y estaciones de trabajo, revisión de correo, protección de filtro de contenido, detectores de intrusos reactivos a nivel de host y red, etc. Entonces, cual es el problema, si la tecnología existe para minimizar las posibles amenazas. El problema entonces es como aplicar esas soluciones para poder tener un control sobre lo que existe en la red o redes de un corporativo. Además de mantener siempre la visibilidad de lo que está ocurriendo y corroborar que lo que se hace está dentro del marco de políticas aceptadas por la organización.
El problema que existe en la mayoría de los corporativos es la falta de políticas de seguridad que sean aplicables al proceso del negocio, además de permitir a la información que fluya y conserve las tres primicias de seguridad, las cuales son Confidencialidad, Integridad y Disponibilidad y el No-repudio. Hablar de una política adecuada universal es complicado, sobre todo por que se considera a los Sistemas de Información, los cuales deben ayudar a aumentar la productividad y funcionalidad de las operaciones en la organización. Siempre hay que tener presente los procesos del negocio, de lo contrario, cualquier solución no podrá ser aplicada eficazmente ni eficientemente. Logrando así ningún beneficio al negocio, y el apoyo de los directivos a gastos innecesarios.

Soluciones y Estrategias.

En la historia de la Seguridad Informática una de sus principales preocupación es proteger el perímetro. Y cuando se logra proteger (el perímetro) se tiene cierta confianza en que los sistemas en el interior estarán seguros y la solución a todo el

peligro se resolverá con un Firewall. Antes, el perímetro era claramente definido; por ejemplo, servidores y estaciones de trabajo en el mismo segmento lógico y físico de la red, (se) contaban únicamente con un enlace dedicado a Internet y solo era necesario permitir los puertos de los servicios de Internet necesarios. Actualmente la situación de las redes corporativa es diferente, es decir, se tiene más de 1 enlace hacia Internet, redes inalámbricas, WAN, Redes Privadas Virtuales (VPN por sus siglas en Inglés), además de Servidores y Servicios que corren sobre la red y que son críticos para la organización. La Seguridad de la Información que fluye en arquitecturas como la planteada en el párrafo anterior es ahora más compleja que antes, las amenazas y vulnerabilidades cambian al igual que la tecnología y mantener una Seguridad Perimetral es mayor. Existe una gran cantidad de soluciones tecnológicas, Firewall 's corporativos con opción de VPN, cifrado de información, Firewall para estaciones de trabajo, soluciones de Antivirus para servidores y estaciones de trabajo, revisión de correo, protección de filtro de contenido, detectores de intrusos reactivos a nivel de host y red, etc. Entonces, cual es el problema, si la tecnología existe para minimizar las posibles amenazas. El problema entonces es como aplicar esas soluciones para poder tener un control sobre lo que existe en la red o redes de un corporativo. Además de mantener siempre la visibilidad de lo que está ocurriendo y corroborar que lo que se hace está dentro del marco de políticas aceptadas por la organización.

El problema que existe en la mayoría de los corporativos es la falta de políticas de seguridad que sean aplicables al proceso del negocio, además de permitir a la información que fluya y conserve las tres primicias de seguridad, las cuales son Confidencialidad, Integridad y Disponibilidad y el No-repudio. Hablar de una política adecuada universal es complicado, sobre todo por que se considera a los Sistemas de Información, los cuales deben ayudar a aumentar la productividad y funcionalidad de las operaciones en la organización. Siempre hay que tener presente los procesos del negocio, de lo contrario, cualquier solución no podrá ser aplicada eficazmente ni eficientemente. Logrando así ningún beneficio al negocio, y el apoyo de los directivos a gastos innecesarios.

3.2 Problemas Tecnológicos y Posibles Soluciones.

Lo más común es implementar un Firewall para proteger posibles ataques desde Internet. Este dispositivo frecuentemente está conectado debajo del equipo de ruteo a la salida de Internet. Debe poder controlar el tráfico de entrada y salida de la organización, además de filtrar la información que pudiera ser perjudicial a los sistemas, como, virus, troyanos, código malicioso en general. La información saliente de la empresa debe preocupar a cualquiera, por eso, es importante tener un conocimiento completo de las aplicaciones permitidas y aplicar políticas para restringir el uso de otras que puedan afectar al sistema o negocio. Por lo antes mencionado, debe ser un requerimiento de seguridad, conocer los puertos que utilizan las aplicaciones permitidas y verificar la forma de tener control sobre la información que viaja sobre estas. Además de definir qué puertos son permitidos para dicha aplicación.

Podemos mencionar que es necesario tener filtros de contenido para correo y navegación. Así como la necesidad de tener ubicados los servicios de Internet, como es Correo electrónico -puerto 25- y para el Hipertexto -puerto 80-. En estos servicios es recomendable utilizar un segmento separado de la red, conocido regularmente como Red de Servicio o DMZ, la cual estará protegida por una tarjeta especial del Firewall principal. Otro punto importante a revisar son las Redes Privadas Virtuales, mejor conocidas como VPN´s. Estas deben de cumplir con aspectos mínimos de seguridad, con el fin de garantizar que su uso cubra los requisitos mínimos solicitados por el corporativo. Algunos de los aspectos son: contar con un Firewall personal en todo momento, para garantizar que un equipo remoto tenga acceso y utilice servicios de la red y no se convierta en un puente u otro punto de vulnerabilidad. También es necesario asegurar que este equipo cuente con una protección antivirus aceptable y lo más importante es, únicamente permitir el acceso a los servicios necesarios para ese usuario. Este es uno de los detalles más importantes debido que al confiar en el usuario de la VPN, regularmente es un empleado, este no hará nada por afectar los servicios que utiliza.

Algo que debe siempre considerarse en un entorno seguro es la protección hacia

los sistemas y las personas que los utilizan. Es complicado concientizar al personal de una organización sobre la importancia de la seguridad y lo que esto implica cuando se presenta una situación que pueda afectar al negocio. Por ejemplo, el requisito de utilizar una contraseña con ciertas características, es un elemento de seguridad, el cual proporciona control de acceso a la información que se maneja, evitando que ésta pueda ser vista por usuarios no autorizados. La necesidad de conocer y controlar el tráfico entrante y saliente de la red es un factor clave a considerar y posiblemente anticiparse ante un evento que pueda ocasionar daños a la Información. Es necesario contar con soluciones que permitan aplicar filtrado de contenido en la navegación de los usuarios. Un caso interesante es el virus Opaserv.H, infecta un equipo agregando un archivo de procesamiento por lotes para bajar una actualización de software de un sitio especifico en la red. El punto es que si la dirección de este sitio a nivel de Internet se cambia por 127.0.0.1, dirección loopback de TCP/IP, puede provocar la caída de servidores Proxy o equipos que realizan filtrado de contenido. Esta petición se hace de forma continua e interna, mas de 50 veces por segundo, crea un ataque de negación de servicio. Es interesante observar entonces, que actualmente el ataque puede ocasionarse desde el interior de la empresa si no se cuenta con las políticas necesarias para aplicar soluciones y evitar eventos que provoquen problemas con el flujo de la información. Los detectores de intrusos por su parte permiten un conocimiento mayor sobre los problemas que acontecen a la red crítica. Por eso es importante tenerlos en cuenta para detectar anomalías en los protocolos y considerar los basados en firmas para ataques conocidos. Esto permitirá reacciones tempranas ante cualquier evento que pueda ocasionar algún tipo de problema.

La mejora en la seguridad -un tema completo- es necesario que varias de las decisiones que guíen a la empresa y/o corporación estén también dirigidas a la protección de la información. En realidad, la Información que genera una empresa puede ser el activo más crítico y sensible y es cuando más deben realizarse esfuerzos para proteger la información.

Los análisis de vulnerabilidades ayudan a identificar las debilidades actuales del sistema y a obtener prioridades respecto a lo que se debe implantar para disminuir el mayor número de vulnerabilidades y evitar que estas puedan convertirse en riesgos. Este tipo de análisis se recomienda aplicarlos con cierta frecuencia y desde diversas perspectivas para obtener una visión general sobre los puntos críticos a resolver y así aplicar una metodología de seguridad continua, la cual permitirá que la infraestructura con la que cuenta la empresa sea mejor y el numero de riesgos sea mínimo y controlado.

3.3 ¿Qué sucede con una red inalámbrica?

Una red claramente sin cables es muy recurrida cuando se necesita movilidad y flexibilidad. Respecto a la seguridad hay elementos que pueden coadyuvar a que estas redes sean seguras; por ejemplo, la autenticación utilizando la dirección MAC, utilización de una contraseña y posiblemente hasta certificados digitales creen una sensación de seguridad. Cabe mencionar que el medio que utilizan estas redes es público, una solución es utilizar un Firewall entre la red inalámbrica que debe definirse solo para usuarios y la red de cableado, además de aplicar autenticación para poder utilizar servicios de una red a otra, esto garantizará hasta cierto punto que el uso de recursos se permite únicamente a personas que están autorizadas para el uso de los mismos. La forma de manejar la autenticación también es importante, se puede manejar el uso de un password de un solo uso o de múltiple uso, siendo necesario considerar la importancia de la información que se está protegiendo, y considerando la relación costo-beneficio. Mucho se comenta sobre la incidencia de ataques y que estos regularmente vienen desde el interior de la empresa, entonces ¿cómo protegerse si el enemigo está dentro?

La solución a esta cuestión es la vigilancia permanente y el monitoreo de las políticas de la organización, así como la autorización al uso de programas validos y necesarios para las operaciones. Es un tema que comienza a tener importancia y se aplica con buenos resultados. ¿Que se protege con un esquema como el anterior?, evitar la instalación de aplicaciones no necesarias que pueden ser nocivos para la red y directamente disminuir la instalación de puertas traseras o

programas con códigos maliciosos. Como se menciono anteriormente pueden no solo ocasionar problemas locales, si no también provocan problemas a nivel general. Otro problema que está empezando a ser grave es el Spam. Este tipo de correo comercial no solicitado en ocasiones provoca la negación del servicio de correo en servidores que permiten relay. Nuevamente, regresamos al punto de que es necesario tener al menos un sistema de autenticación para la utilización de los servicios, pero que sucede cuando técnicamente el correo está diseñado para permitir la libre comunicación entre servidores. Hay soluciones simples y efectivas que recurren al uso de verificación por dominio, estas logran ser buenas para evitar ser presa del relay. Esto no se resuelve el problema de correo no solicitado. Hay que considerar que un error o un descuido de configuración puede ocasionar una serie de eventos que desencadenan en un incidente que puede dañar las operaciones de la empresa. La facilidad de las comunicaciones actualmente se ve reducida al mandar mensajes por correo electrónico, los cuales no disponen de un mecanismo de control que impida al usuario leer el mensaje antes de revisarlo. Regularmente esta actividad es la que actualmente aprovechan los virus para distribuirse.

Entonces como observamos, el correo no solicitado provoca realmente dos problemas, hasta el momento. El primero se puede resolver verificando que el dominio este bien configurado, el DNS cumpla con los registros necesarios y verificar también que la dirección IP no esté en listas negras que permita relay. Una solución de este tipo requiere la cooperación completa de las demás organizaciones para mantener un DNS correctamente configurado y seguro. El segundo problema puede resolverse utilizando algún tipo de filtrado de mensajes, de esta forma rápidamente se realiza una protección mínima para los problemas presentados anteriormente. Algo que se debe considerar en el párrafo anterior es la cooperación de todas las entidades, tener un DNS correctamente configurado y seguro. Estamos entonces tocando un tema interesante. El perímetro seguro del cual hemos comentado, se vuelve aun más complejo, empieza a tomar la forma de algo general en donde, como debemos suponer al ser Internet un red mundial, una red global, y cualquier persona, entidad, organización que este en ella, ofrece o

utiliza servicios de esta, por lo tanto pertenece a dicha red, es también participe de los eventos que ocurren y tiene su parte en ella, y por lo tanto deben estar comprometidos al buen funcionamiento de la misma. Podemos imaginar una situación en la cual, existen células buenas y células malas, si las células buenas realizan los procedimientos necesarios para procesar los nutrimentos adecuadamente, y estas células buenas se agrupan para formar una defensa ante lo que puede ser malo para ellas, las células malas, entonces tendrán un campo de acción reducido a únicamente las células que fallaron en la aplicación de ciertos procedimientos. Así funciona Internet. Y los procedimientos existen, y estos son generales. Recordemos uno de los últimos eventos que ocasionaron pérdidas a una gran cantidad de empresas. El gusano SQLSlammer, aprovecha una vulnerabilidad en la aplicación de base de datos de Microsoft SQL Server, este gusano rastrea computadoras que tengan el puerto 1434 UDP, para inyectar código con el que lograba ejecutar su rutina de código, al infectar el equipo, este realiza el mismo procedimiento para distribuirse y de esta forma logró contaminar varias computadoras en aproximadamente 2 días, la distribución del virus inicio un sábado y para el lunes gran cantidad de equipos ya reportaban este comportamiento y el problema como tal. Esta distribución de virus pudo haberse evitado. En primer lugar Microsoft había ya liberado un parche para esa vulnerabilidad, este es un tema interesante de comentar, que abordaremos más adelante. En segundo lugar, porque habría una empresa en permitir un servicio tan crítico como es un manejador de base de datos, y la conexión de esos servicios estar permitida desde Internet.

Hay reglas generales de seguridad, las aplicaciones que son internas, solo deben ser internas, y las que son externas, deben de estar colocadas de tal forma que un incidente en estas no genere problemas más allá de esa aplicación. También se debe tener conciencia histórica, si un incidente tuvo lugar, se debe hacer lo necesario para evitar que al menos ese incidente no vuelva a repetirse, y si se repite disminuir en la medida de lo posible el daño que pueda causar. Otra regla general que debiera ser aplicada es tener soluciones antivirus en cualquier parte de la empresa, en cualquier lugar y el cualquier rincón. Y posiblemente la mas

complicada pero más importante, es conocer el entorno que se tiene, el funcionamiento y la relación que hay entre las aplicaciones y los servicios que se prestan. Mucho se habla también de las vulnerabilidades, y por consiguiente de sus soluciones, los parches. Aquí existe una dependencia entre el usuario y el proveedor. Es evidente que si una vulnerabilidad existe, y no se tiene un parche, debe al menos de existir una solución temporal, conocida como workaround. Si este no existe, se está en un punto donde la amenaza es real, no hay solución, y lo que debe hacerse es minimizar los daños que se pueden presentar si la vulnerabilidad es aprovechada ya sea por un virus, un Cracker o un script-kiddie.

La actualización de software debe ser un tema importante en cualquier implantación de servicios, se recomienda que se cuenten con equipos de prueba idénticos a los de producción donde primero se pruebe el parche, y se revise la situación y después se aplique al equipo en producción. ¿Costoso?, Que sucede si se pierde tiempo en recuperar el servicio en producción por un problema en el parche. Hay que mencionar claro que es necesario contar con respaldo actualizado y probado, y tiempos y procedimientos de recuperación en caso de desastre. Entonces, después de este breve análisis, cual es la solución para evitar ser víctimas y hasta cómplices de un ataque. Si el perímetro es cada día mas complicado de definir, y como ya observamos la interdependencia con los demás sistemas está presente, una solución es crear perímetros a nivel de computadora, a nivel de servicio, a nivel de aplicación. Crear un verdadero sistema a prueba de fallas. Si un elemento del sistema falla, el sistema debe ser capaz de continuar funcionando y restaurar el fallo, lo más rápido posible para evitar complicaciones y afectar al sistema entero.

3.4 Diagramas funcionales en la implementación de redes perimetrales.

Cisco ASA Firewall - Stateful Packet Inspection.

Un firewall “stateful” (Fig. 3.1) guarda en memoria atributos significativos de cada conexión, de inicio a fin. Estos atributos, mejor conocidos como el estado de la conexión, incluyen direcciones IP, puertos involucrados en la conexión y los números de secuencia de los paquetes, entre otros.

El firewall “stateful” se basa en el “Three-Way HandShake” para las conexiones TCP. Los paquetes con el bit SYN encendido son considerados por el firewall como conexiones nuevas. Si el servicio que pide el cliente está disponible en el servidor (destino), el servicio responde al paquete SYN con un paquete en el que los bits SYN y ACK están encendidos. El cliente entonces responde con un paquete ACK y la conexión entrará en estado “Established”, es decir, la conexión se establece. Por ende, un firewall “stateful” solo pasa paquetes que sean parte de conexiones establecidas.

Para evitar que la tabla de estados de conexiones se llene, las sesiones expirarán si no pasan tráfico por un periodo de tiempo determinado y la conexión se removerá de la tabla. Algunas aplicaciones mandan mensajes de “keepalive” periódicamente para evitar que la conexión se borre de la tabla en periodos de no actividad.

Para UDP y otros protocolos no basados en conexión, la conexión se establece con el primer paquete SYN enviado y solo pueden expirar por time-out.

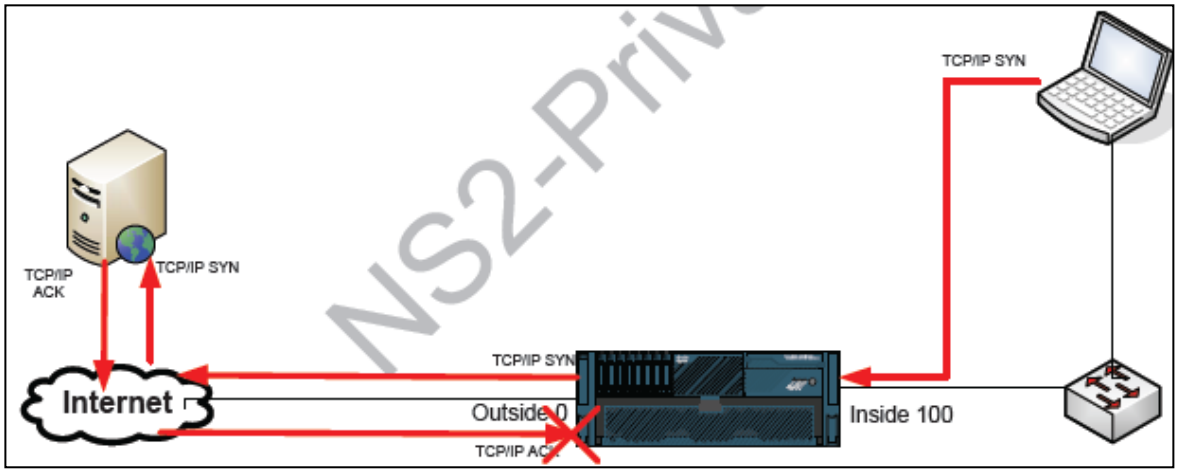


Fig. 3.1

De esta manera, si el firewall recibe un paquete de una conexión que no es el que se espera en la tabla de conexiones, el "stateful inspection" del firewall tirará ese paquete (Fig. 3.2, 3.3 y 3.4).

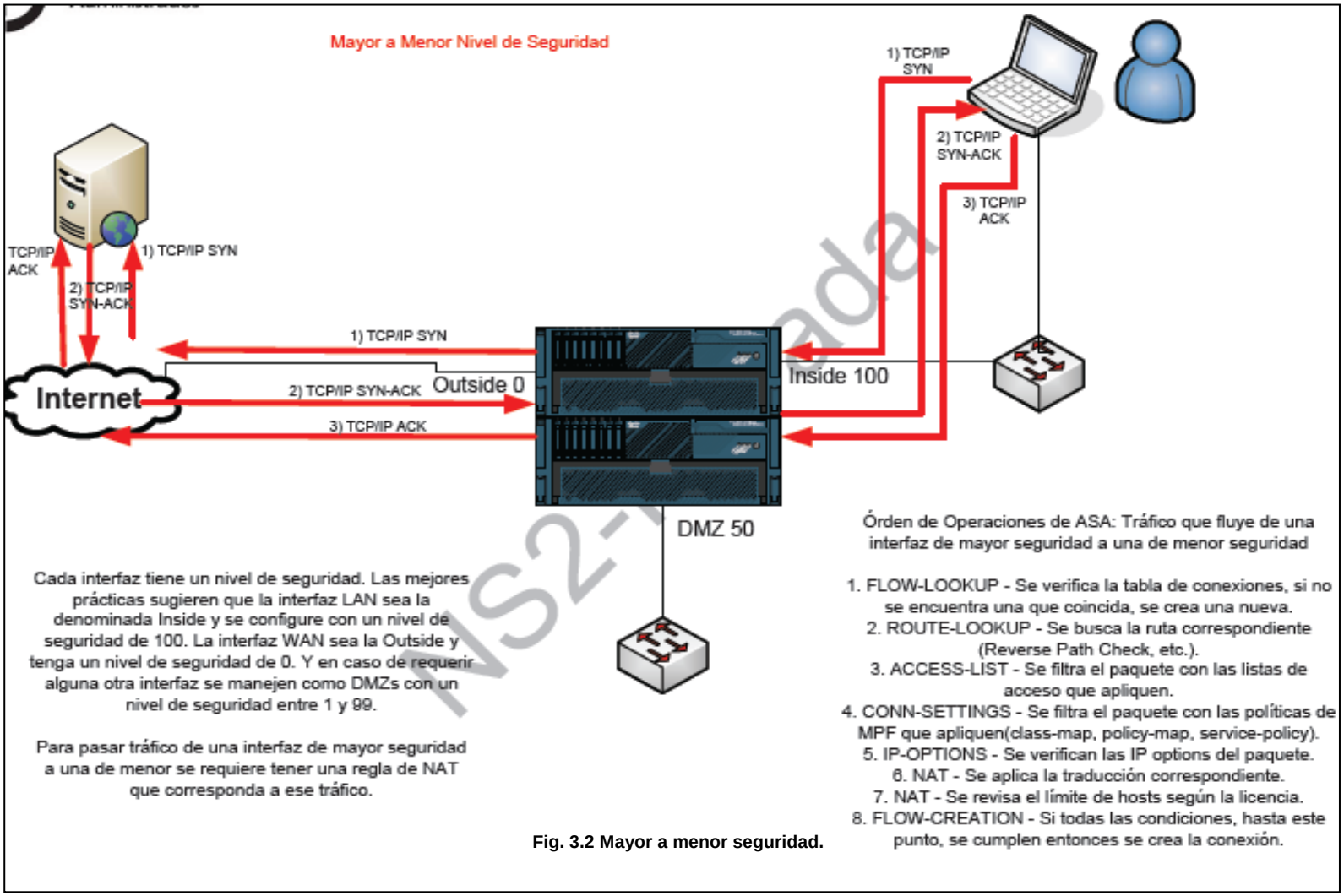


Fig. 3.2 Mayor a menor seguridad.

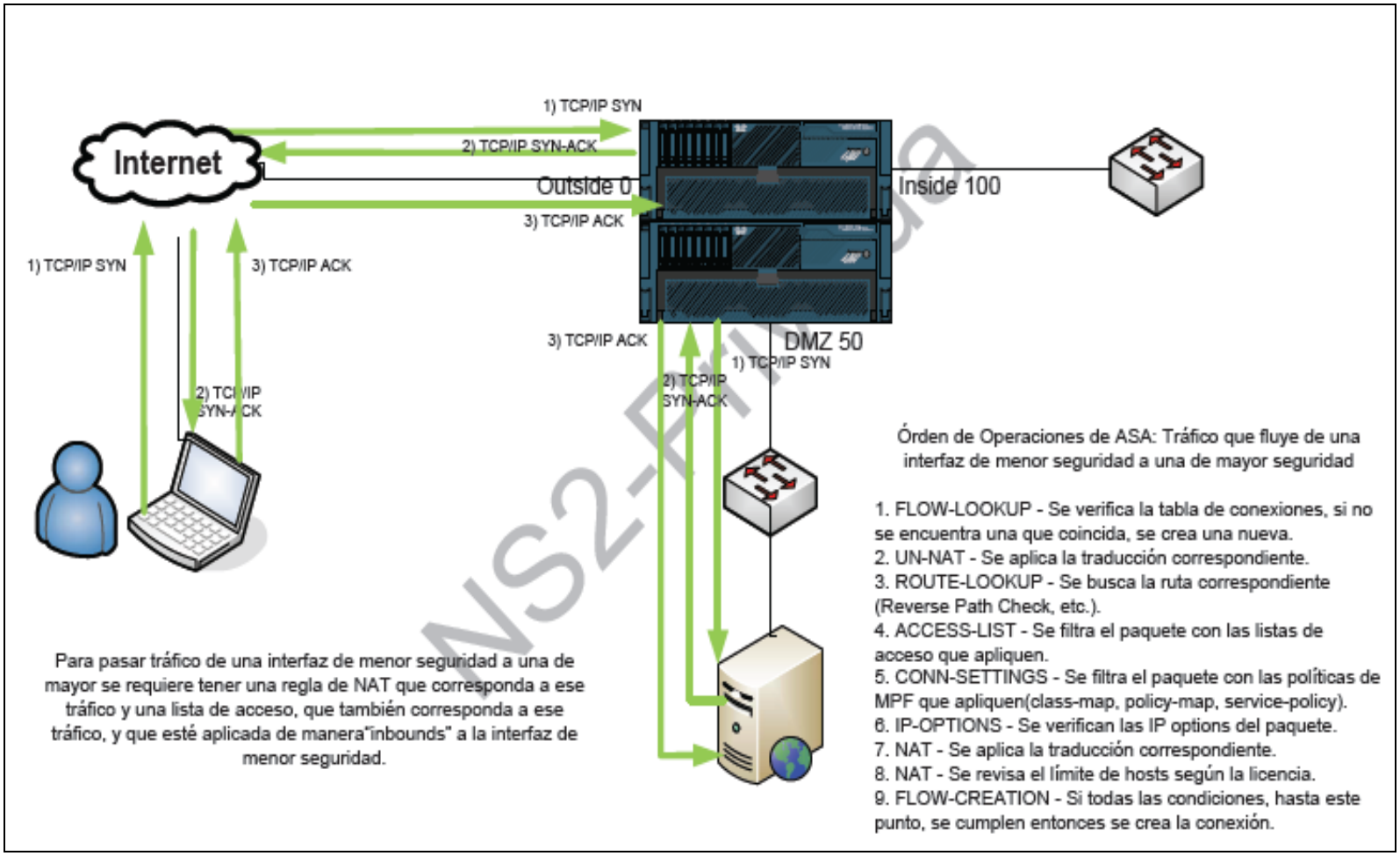


Fig. 3.3. Escenario1

Se puede particionar un ASA en multiples dispositivos virtuales, conocidos como "security contexts" ó contextos. Cada contexto es un dispositivo independiente, con su propia política de seguridad, interfaces y administradores. Equivale a tener varias cajas de ASA.

No soporta:

- Ruteo dinámico
- VPN
- Ruteo de Multicast
- Threat detection

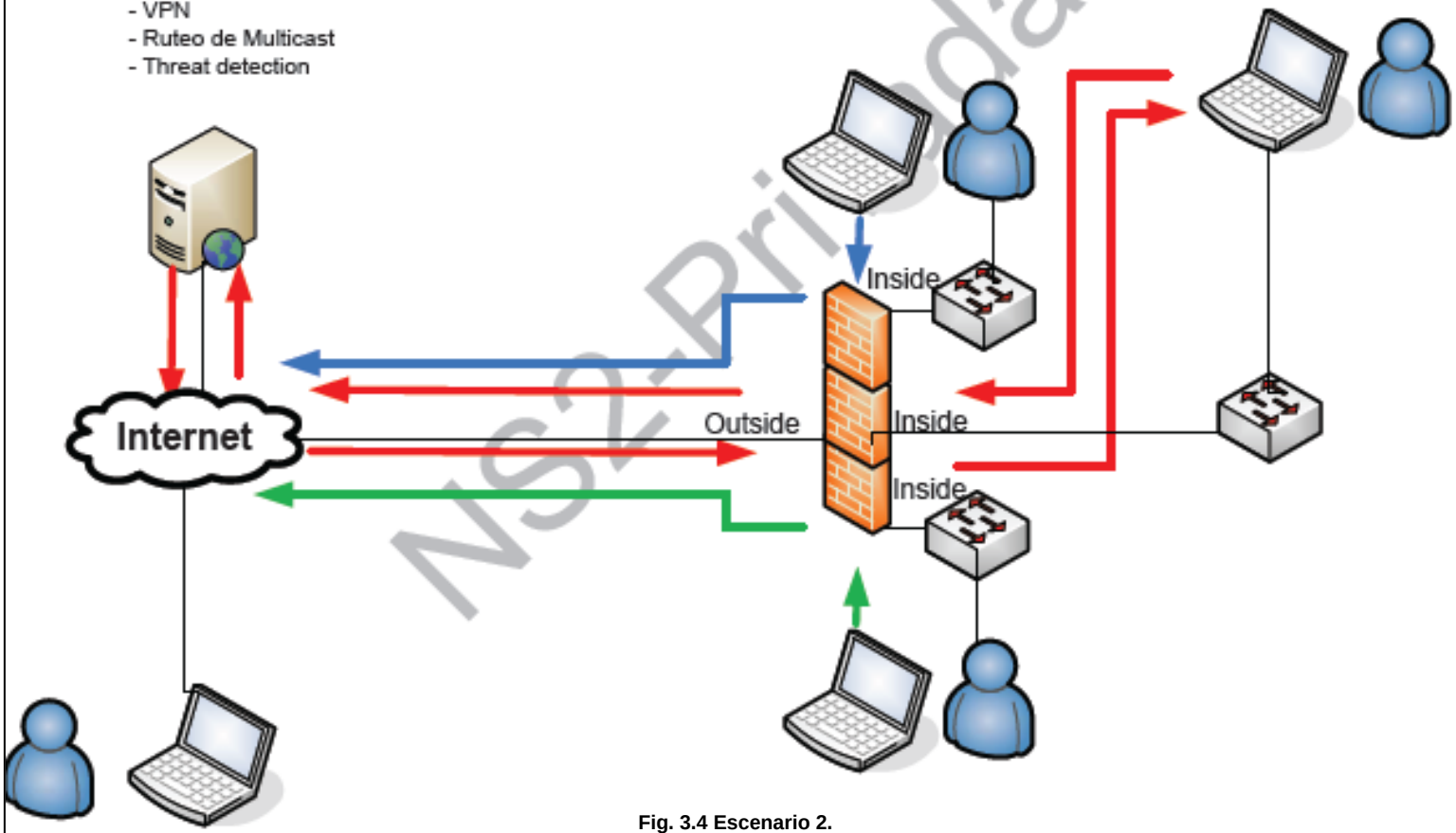


Fig. 3.4 Escenario 2.

Blue Coat SG – Transparent Proxy Deployment.

El objetivo de esta solución es que se redireccione el tráfico al Proxy SG (Fig.3.5, 3.6, 3.7 y 3.8) sin que exista la necesidad de que el cliente tenga conocimiento de la existencia del éste en la red.

El dispositivo de redirección puede ser un switch capa 4 ó un ruteador que soporte el protocolo WCCP de Cisco.

En este caso, la petición lleva la dirección IP destino del servidor web y no la del proxy, ya que el cliente desconoce la existencia de este último, ya que el "user agent" del cliente cree que está comunicándose con el servidor web directamente, sin intermediarios.

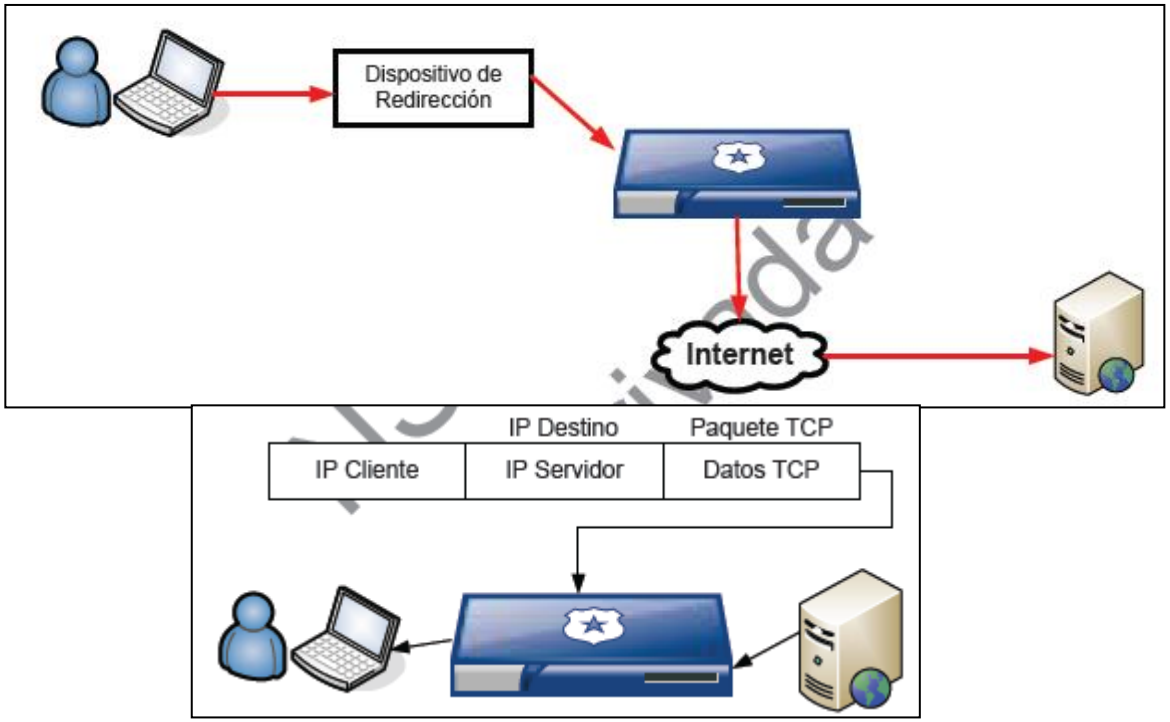


Fig. 3.5 El cliente cree que está comunicándose con el servidor web directamente, sin intermediarios.

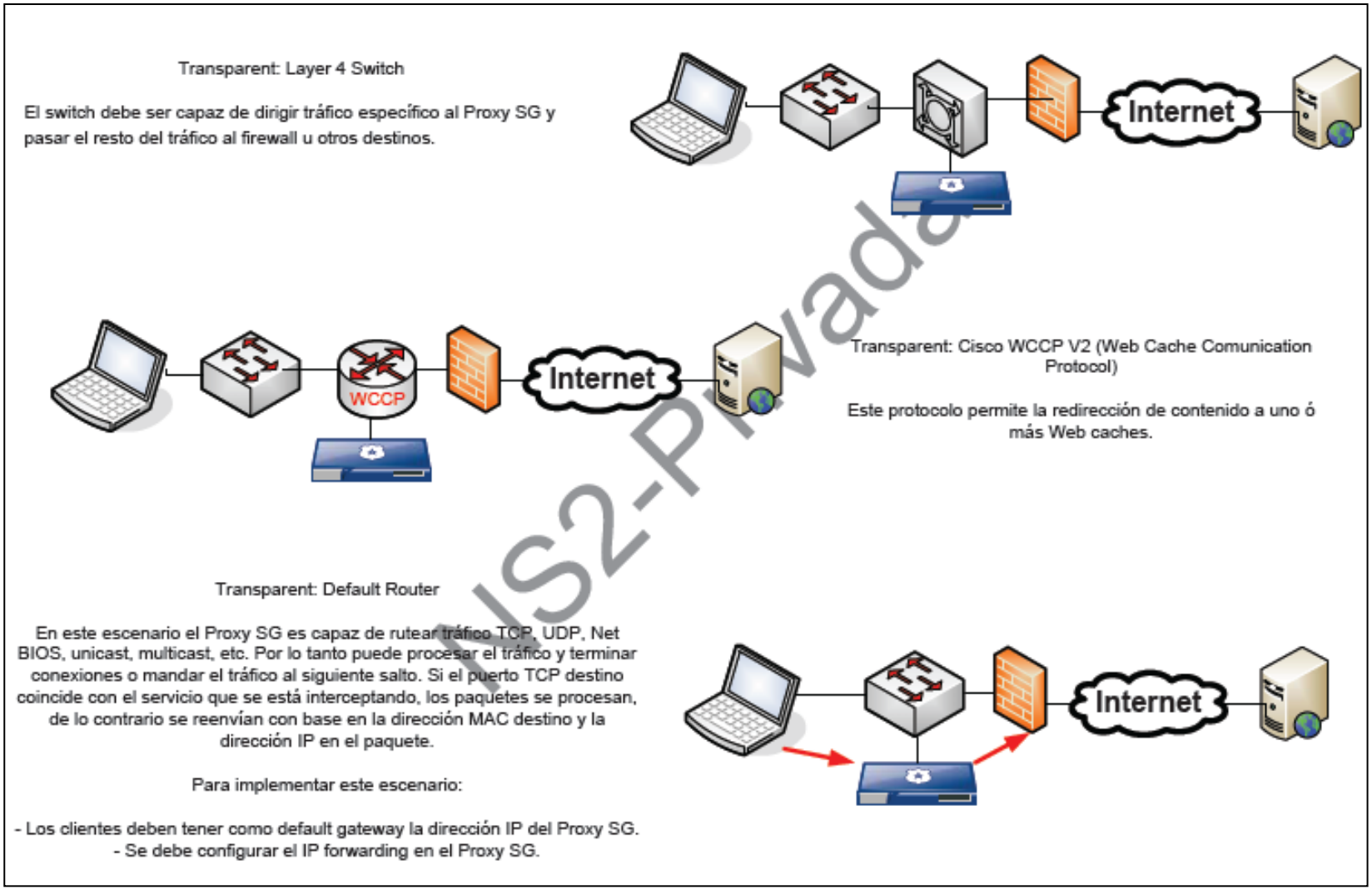


Fig. 3.6. Escenario posible 1.

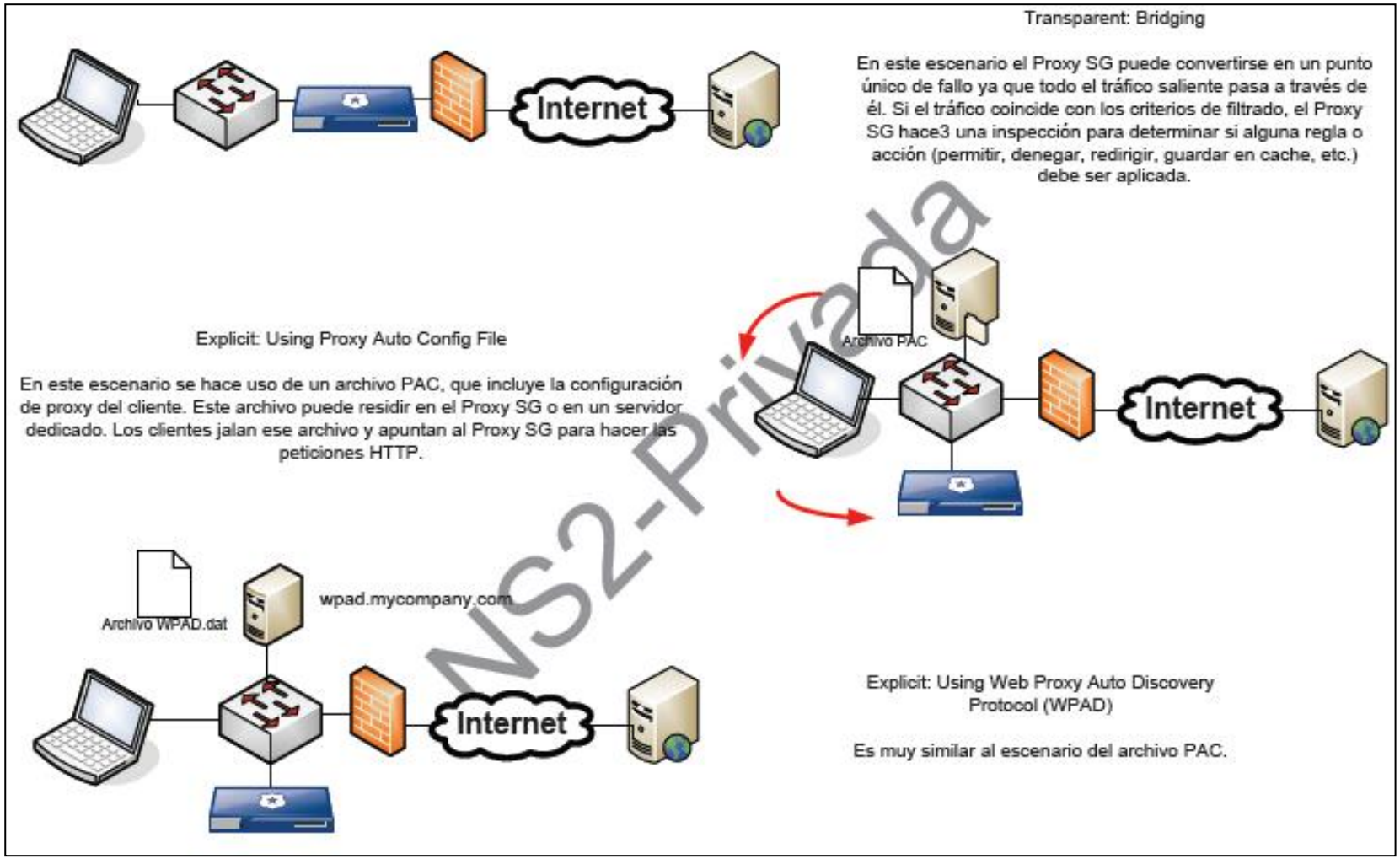


Fig. 3.7 Escenario posible 2.

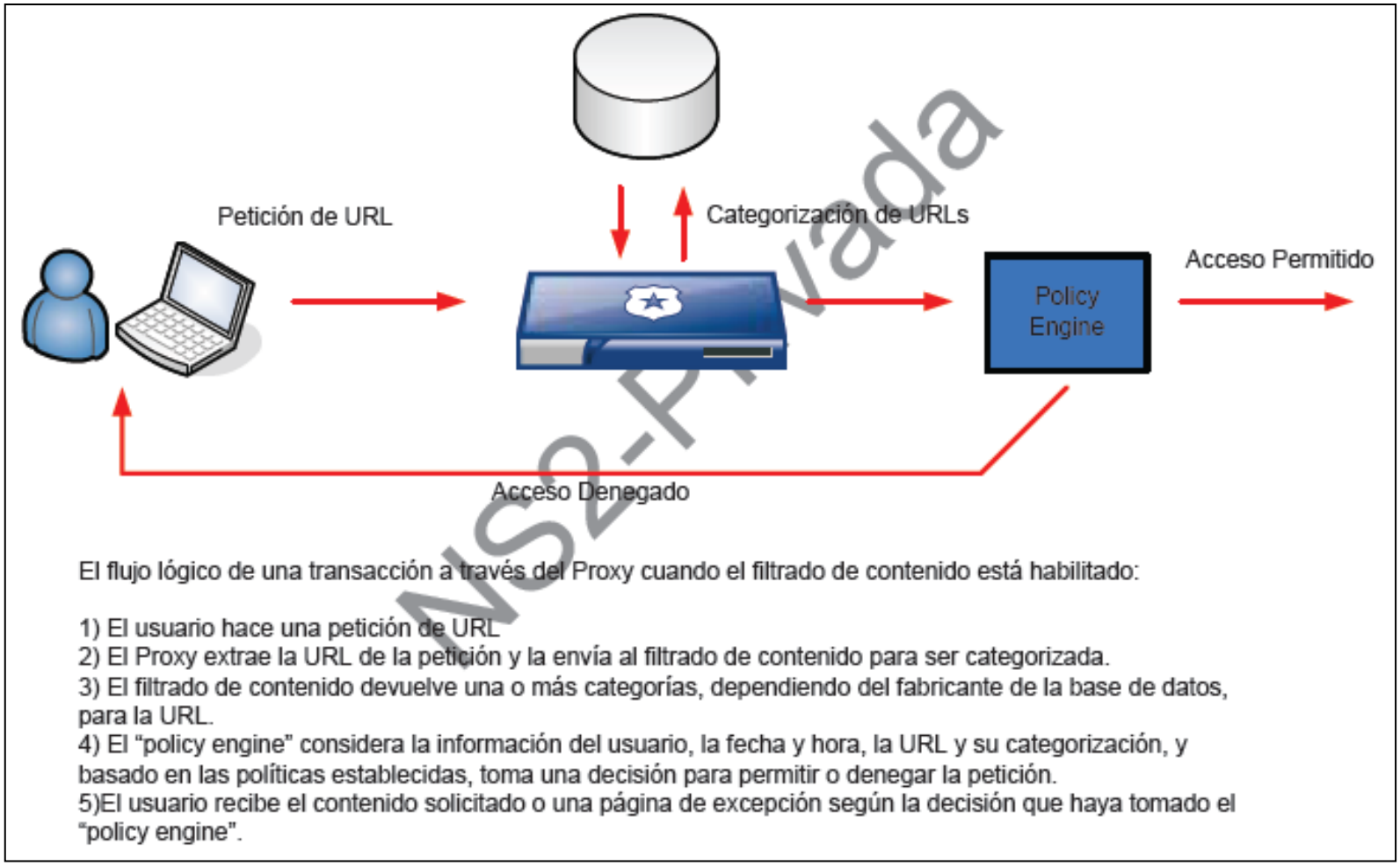


Fig. 3.8 Filtrado de contenido.

IronPort Email Security Appliance.

La solución de filtrado de correo de IronPort cuenta con las funciones de filtrado por reputación, antispam, antivirus, filtrado de contenido, Virus Outbreak Filters y aplicación de políticas organizacionales.

Mejores Prácticas de Filtrado:

- Regla para evitar correo con identidad falsa (“spoofing”). Debe de descartar todo el correo con remitentes que contengan como dominio del remitente los dominios locales y que no provenga de los servidores oficiales de la organización, o al menos que no provenga de las redes internas.
- Regla para evitar mensajes de rebote (“backscatter”) y ataques de rebotes redirigidos. Utilizar la función o característica de verificación de rebotes si el equipo cuenta con ella, en lugar de ésta regla.
- Regla (s) de límites de los mensajes (tamaño de mensaje, cantidad de anexos, tamaño de anexos, niveles de compresión anidada, etc.), para limitar el ancho de banda utilizado en el correo.
- Regla de tipos de archivo anexos para disminuir los riesgos y amenazas que pudieran contener éstos tipos de archivos.

Filtrado por reputación.

Permite clasificar remitentes de correo electrónico y restringir acceso a la infraestructura de correo basándose en la confiabilidad del remitente según el servicio de reputación de IronPort Sender Base (ver Fig. 3.9).

Este servicio permite rechazar posible spam basándose en la dirección IP del remitente. Este servicio, al ser consultado, regresa un puntaje de reputación basado en la probabilidad de que un mensaje proveniente de cierto origen sea spam. Además, a través de la función Mail Flow Monitor, nos permite obtener más información de quién está enviando dicho mensaje.

El filtrado por reputación nos permite:

- Reducir la cantidad de spam entrante
- Protege contra los “spam floods”
- Mejora el rendimiento de la infraestructura de correo electrónico.

Virus Outbreak Filters.

Esta funcionalidad provee protección contra brotes de virus de hora zero contenidos en mensajes de correo electrónico. Detecta los brotes en tiempo real y responde dinámicamente para prevenir que el tráfico sospechoso entre en la red. Ofrece protección contra virus mientras los fabricantes de antivirus liberan las firmas para detectar y combatir los nuevos virus.

El motor de esta funcionalidad compara los mensajes entrantes con las reglas publicadas para los Virus Outbreak Filters. A los mensajes que coinciden con dichas reglas se les asigna un nivel de amenaza. El nivel de amenaza se compara con el umbral de nivel de amenaza que se configure en el Iron Port. Los mensajes que igualen o rebasen dicho umbral serán puestos en cuarentena.

El proceso de detección de brote de virus comienza con la Sende Base de IronPort, ésta le da seguimiento a más de 20 millones de direcciones IP y observa alrededor del 25% del tráfico de correo electrónico del mundo.

Con esta información se crea una estadística de patrones de tráfico de correo electrónico.

Para remitentes confiables, se omite el filtrado. Para remitentes dudosos, se filtra y analiza ó se restringe el flujo. Y para remitentes hostiles, se elimina o etiqueta.

Antispam: Reduce la carga de correo SPAM en sus sistemas y buzones.

Antivirus: Previenen, detecta y remueve “malware”, incluyendo virus, gusanos de computadoras y caballos de troya. Igualmente pueden prevenir y remover “adware”, “spyware” y otras formas de “malware”.

Filtrado de contenido: El correo es bloqueado o permitido basado en el análisis de su contenido en vez de su fuente o algún otro criterio.

Virus Outbreak Filters (Filtros contra Brotes de Virus): Protección contra virus de hora cero.

Fig. 3.9 Filtrado por reputación.

Para utilizar esta función, se debe crear un perfil de cifrado que especifique las características del mensaje que se quiere cifrar y la información de conectividad del servidor de llaves. Éste puede ser el “Cisco Registered Envelope Service” o un servidor administrado localmente. También se deben configurar filtros de contenido y/o filtros de mensaje para determinar qué mensajes deben ser cifrados.

Un mensaje saliente que cumple con las condiciones del filtro de cifrado se pone en una cola para ser procesado. Una vez que se ha cifrado el mensaje, la llave utilizada para cifrarlo se guarda en el servidor especificado en el perfil de cifrado y dicho mensaje se encola para ser entregado.

Cuando se utiliza el cifrado de correo (Fig. 3.10), la aplicación de IronPort cifra el mensaje y guarda la llave de cifrado del mensaje en un servidor local de llaves o en un servicio hospedado de llaves. Cuando el recipiente o recibidor del mensaje lo abre, es autenticado por el servicio de llaves y el mensaje descifrado es mostrado.

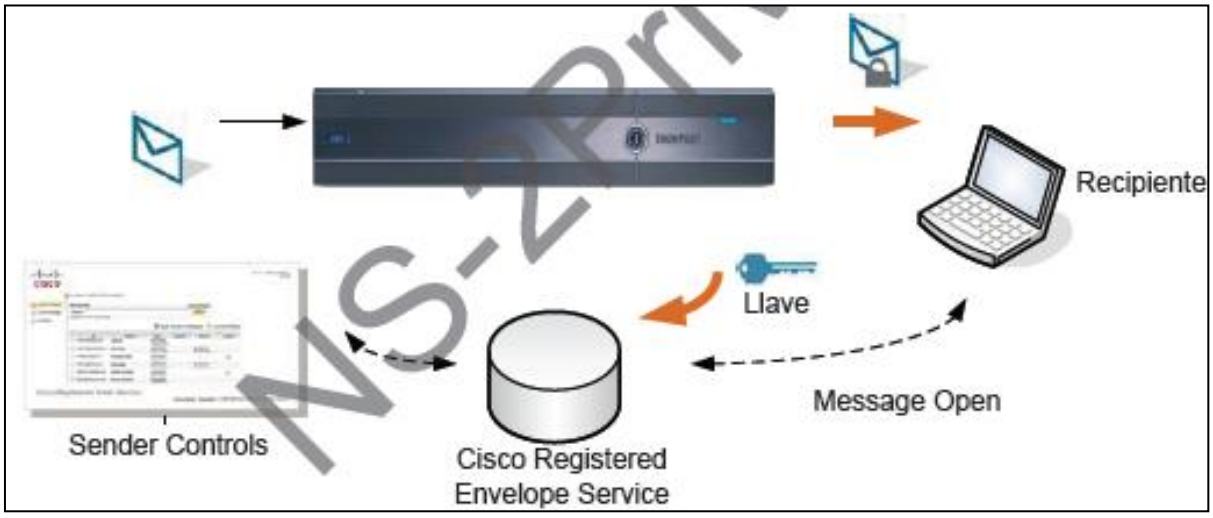


Fig.3.10 Cifrado de correo.

Tipiing Point Intrusion Prevention System.

Sistema de Prevención e intrusión (Fig. 3.11)

- Funciona en modo “In-line”, es decir, el tráfico pasa a través del dispositivo
- Revisa el tráfico y toma acciones como bloqueo, “rate-limit” o envío de alertas, basado en la política configurada
- Actúa como un dispositivo “bump-in-the-wire”:
  - No usa direcciones IP ni MAC e inspecciona de Capa 3 a 7
  - Se ve como un dispositivo Capa 2 en la red
- No genera Falsos Positivos (no bloquea lo que no debería bloquear)
- Posee un motor de inspección flexible que se adapta a las nuevas amenazas
- Actualizaciones en tiempo real sin causar afectación al servicio
- Alto desempeño y baja latencia.

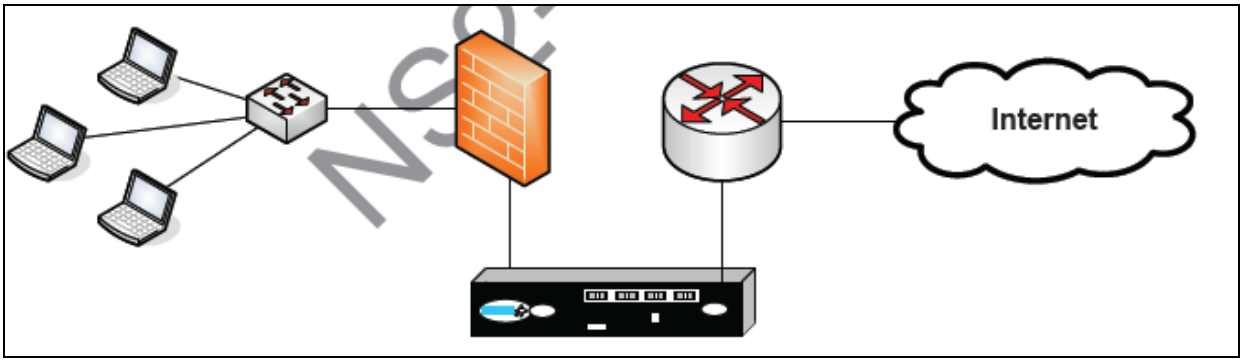


Fig. 3.11 Sistema de Prevención e intrusión.

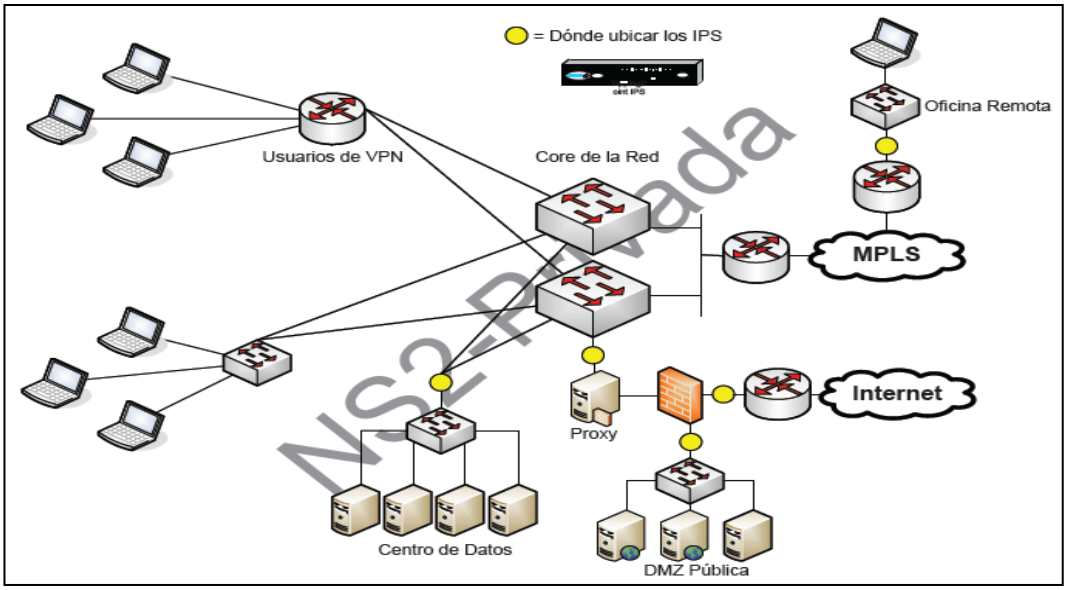


Fig. 3.12 Ubicación en la red.

Un IPS Profile especifica qué hacer cuando el tráfico iguala las condiciones del filtro.

Los filtros vienen contenidos en las Digital Vaccines.

Un Action Set está asociado a un IPS Profile. El Action Set define qué hacer cuando se dispare el filtro:

- Qué hacer con el tráfico (bloquear, permitir, hacer rate-limit)
- Cómo notificar un evento (enviar un correo, un syslog o un SNMP-Trap)
- Otras: TCP Reset, poner en Cuarentena, etc.

Los IPS Profiles se aplican a los segmentos o Segment Groups.

Los Segment Groups son conjuntos lógicos de segmentos que pueden tener aplicada la misma política, por ejemplo:

- Perímetro (Entre el Internet y los usuarios)
- Core (Entre los usuarios y los Core Servers)

Un segmento es una agrupación de dos puertos físicos.

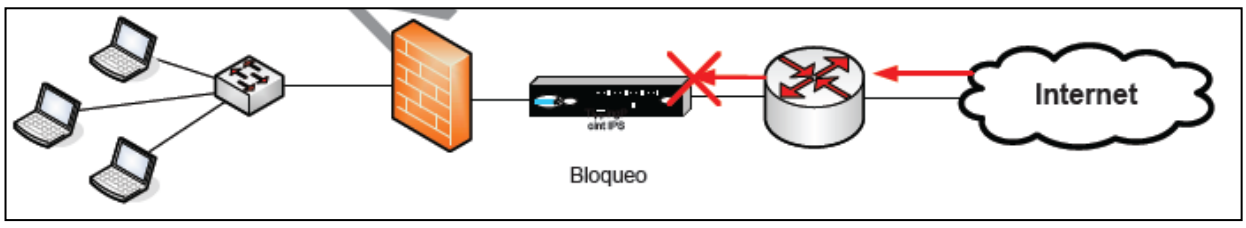


Fig. 3.13 Acciones de filtrado.

Las Digital Vaccines son las actualizaciones de nuevos filtros y se obtienen a través del portal Threat Management Center de Tipping Point (https:// tmc.tippingpoint.com) de forma automática o manual.

La Digital Vaccine contiene los filtros usados por el IPS:

Filtro.

- Metadatos
- Hardware triggers
- Reglas de coincidencia de patrones (Pattern matching rules)

Políticas por defecto

- “Action Sets” por defecto
- Contactos de notificación por defecto

Mapeos de servicios por puerto y protocolo por defecto (ej. HTTP es puerto 80 y 8080)

- otros archivos de configuración y control

Solamente un DV puede residir en el Tipping Point a la vez.

- Las DVs se liberan dos veces a la semana o más de ser necesario.
- La DV por defecto brinda protección inmediata con los parámetros recomendados.
- Las actualizaciones son en tiempo real y no causan afectación al servicio.

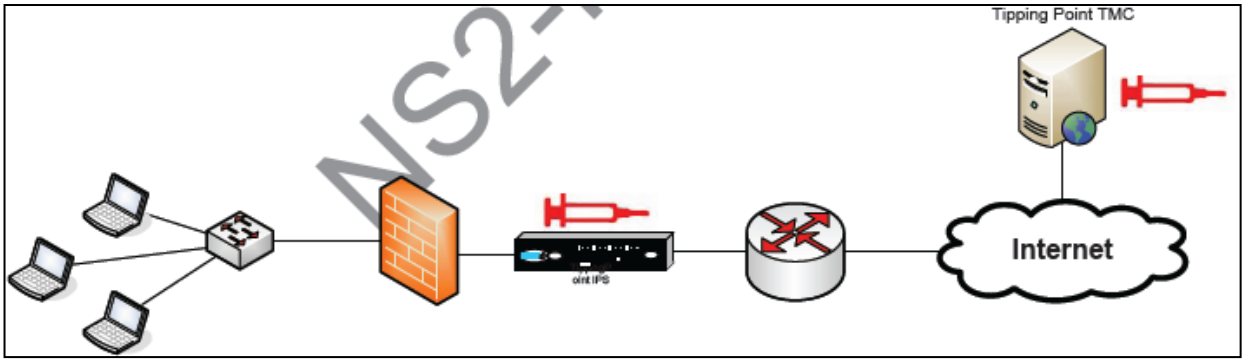


Fig. 3.14 Actualizaciones de nuevos filtros.

3.5 Implementación de un caso práctico.

Objetivo del documento.

Presentar un plan de trabajo detallado para la implementación, puesta a punto y arranque de servicio administrado para la siguiente infraestructura de la:

- Firewall en Alta disponibilidad
- Sistema de prevención de intrusos
- Control de accesos a páginas web
- Seguridad de correo electrónico con antispam y antivirus
- Servicio de Proxy
- Antivirus para computadoras personales
- Equipo para la conectividad para la segmentación de las zonas.

Alcance.

Implementar, afinar, administrar y monitorear la infraestructura ofrecida a la SEP Secretaria de Educación Pública) de acuerdo a la propuesta establecida por Scitum[1].

Visión General.

Instalación del equipamiento central

Firewall en alta disponibilidad

Sistema de prevención de intrusos (IPS)

Control de Accesos a páginas Web

Seguridad de Correo Electrónico con antispam

Equipo para la conectividad para la segmentación de las zonas

Desarrollo.

Firewall en Alta disponibilidad / Equipo para la conectividad para la segmentación de las zonas

Se ofrece una solución de firewall en alta disponibilidad con 2 equipos Cisco Catalyst 6506E Firewall Security System (cada equipo incluye: un Cisco Catalyst 6506-E, una tarjeta Supervisor Engine 720-3B, FWSM, y un Catalyst 6506 Fan) y 2 equipos Cisco

[1] Empresa líder en Latinoamérica en soluciones de seguridad de la información, www.scitum.com

ASA 5520, estos últimos con licenciamiento para 750 clientes de VPN IPSEC y 250 clientes de VPN SSL como parte de la solución de Firewall en alta disponibilidad.

Los equipos destinados a las tareas de Firewall en Alta disponibilidad fueron propuestos para cumplir al mismo tiempo con el requerimiento de Equipo para la conectividad para la segmentación de las zonas.

Se ofrece una solución de equipo para la conectividad para la segmentación de las zonas con 2 equipos Cisco Catalyst 6506E Firewall Security System, estos dispositivos son los que se suministran para realizar la funcionalidad de firewall en alta disponibilidad, ya que estos tienen la capacidad de soportar ambas funcionalidades, facilitando la administración de estas soluciones y mejorando el desempeño de las mismas.

Implicaciones de la Actividad.

Para esta tarea el impacto es considerado como **ALTO**, debido a que, durante el cambio, instalación y segmentación inicial de los switches, se perderá comunicación con cada uno de los servicios que pasan a través de ellos y además será imposible la realización de adiciones, modificaciones o bajas en la configuración de reglas, objetos y servicios con los módulos de Firewall hasta que las comunicaciones de los switches trabajen correctamente.

Requerimientos Adicionales.

Debido al impacto del cambio en las diferentes zonas de la red, es necesario que se considere, después de la implementación, revisar adecuadamente, cada uno de los servicios por los responsables involucrados.

Se tienen los siguientes requerimientos de espacio y energía:

- Switch 6506E 12 UR por cada equipo (son 2, 24 UR)
- ASA 5520 1 UR por cada equipo (son 2, 2UR)
- Energía:
- Contactos Físicos correctamente aterrizados

Implementación de Seguridad de correo electrónico con antispam y antivirus.

Se ofrece una solución de seguridad de correo electrónico con antispam con 2 appliances **Ironport C350** y con licencias de **Ironport Antispam**.

Dicha solución será implementada de acuerdo al siguiente plan de trabajo (Tabla 1).

Actividad	Responsable	Tiempo
Montado de Ironports en Rack	RP / RH	30 min
Cableado y pruebas de comunicación entre dispositivos.	RP / RH	30 min
Configuración en Cluster de ambos filtrados	RP / RH	90 min
Activación de filtros	RP / RH	10 min
Pruebas de filtrado	RP / RH	60 min
	TOTAL	220 min

Tabla 1

Implicaciones de la Actividad.

Para esta tarea el impacto es considerado como **ALTO**, debido a que, durante la implementación de la solución de seguridad de correo electrónico con antispam, se perderá el servicio de correo electrónico.

Implementación Sistema de Prevención de Intrusos (Tabla 2).

Se ofrece una solución de sistema de prevención de intrusos (IPS) con 8 appliances TippingPoint 600E con bypass externo, y throughput de 600 Mbps, con una consola de administración del mismo fabricante Security Management System (SMS).

Actividad	Responsable	Tiempo
Revisión de arquitectura de red	OM/FG	30 mins
Montaje rack de 8 IPS y 1 consola de administración SMS	OM/FG	90 mins
Configuración de consola SMS	OM/FG	40 mins
Conexión de segmentos de red y energía eléctrica	OM/FG	1 hora
Pruebas de conectividad	OM/FG	1 hora
Asignación a consola de los 8 IPS Tippingpoint	OM/FG	1 hora
Configuración/Aplicación de política de monitoreo a segmentos protegidos	OM/FG	1 hora
Verificación de monitoreo de segmentos	OM/FG	2 horas
Pruebas y liberación	OM	1 hora
Tiempo Total Estimado		10 horas

Tabla 2.

Implicaciones de la actividad.

Para esta tarea el impacto es considerado como **ALTO**, debido a que durante al movimiento de la implementación los servicios de red serán interrumpidos temporalmente.

Requerimientos Adicionales

Para realizar el plan de trabajo de manera efectiva se requiere:

- Presencia de personal de Redes desde el inicio hasta el final de la aplicación del plan de trabajo.
- Conexión a la red LAN productiva.
- Acceso al servicio de Internet.
- Cableado de los segmentos de red, hacia y desde los dispositivos IPS, ya que este ultimo deberá ubicársele en medio de la red que se desea proteger.
- Configuración de velocidades amarradas al máximo.
- Cables cruzados y rectos para cada par de segmentos a proteger, con sus debidas dimensiones de largo.
- Espacio en rack para los diferentes equipos a aprovisionar.

Implementación Servicio de Proxy / Control de accesos a páginas web (Tabla 3).

Se ofrece una solución de servicio de proxy con 2 appliances **Blue Coat SG8100-10,** estos dispositivos son los que se suministran para realizar la funcionalidad de control de acceso a página Web, ya que estos tienen la capacidad de soportar ambas funcionalidades, facilitando la administración de estas soluciones y mejorando el desempeño de las mismas.

Actividad	Responsable	Tiempo
Montado de Proxys Blue Coat SG	RH	90 min.
Cableado y pruebas de comunicación entre dispositivos.	RH	30 min.
Desconexión física de Proxys de producción	SEP	5 min.
	RH	10 min.
Pruebas de navegación	RH	15 min.
Tiempo Total Estimado		2:30 hrs.

Tabla 3.

Implicaciones de la actividad.

Para esta tarea el impacto es considerado como **ALTO,** debido a que, durante la implementación de la solución de Proxy, se perderá toda comunicación con el Internet por parte de los usuarios así como de los servicios que pasan a través de ellos.

Requerimientos Adicionales

Se tiene previsto la implantación de 2 dispositivos los cuales ya deben de existir los lugares donde se van a montar así como los servicios de red necesarios, para las Bluecoat SG son necesarios 4 servicios de red. Una vez concluida la migración es importante que personal valide los servicios de filtrado de contenido, así como de navegación.

Factores críticos de éxito para la implementación.

Para realizar con éxito toda la fase de implementación y arranque se deberá considerar lo siguiente:

- Presencia de la personal encargada de aplicaciones y comunicaciones involucradas directa o indirectamente con la implementación desde el inicio hasta el final del plan de trabajo.
- Suministro de información necesaria para la implantación de los servicios; topologías de red, direccionamiento IP, flujos de aplicaciones, etc.
- Conexión a la red LAN productiva.
- Acceso al servicio de Internet.
- En caso de contar con alguna aplicación que se desee probar (VPN, FTP, HTTPS o SMTP), proporcionar un usuario y password para dichas aplicaciones.

CONCLUSIONES.

Como conclusión. Nos gustaría que quedase claro que la Seguridad Informática es un aspecto muchas veces descuidado en nuestros sistemas, pero de vital importancia para el correcto funcionamiento de todos ellos.

Sería importante hacer hincapié en los siguientes conceptos:

- Todo sistema es susceptible de ser atacado, por lo que conviene prevenir esos ataques.
- Conocer las técnicas de ataque ayuda a defenderse más eficientemente.
- Elegir SOs con poco énfasis en la seguridad, puede suponer un auténtico infierno.
- La seguridad basada en la ocultación no existe.

Como se menciono, el perímetro es cada vez más complicado de proteger, la integración de los sistemas actuales con Internet y la necesidad de movilidad y de obtención de resultados en el menor tiempo, provoca una complicada conjunción entre la seguridad y la facilidad de uso. La conciencia y las políticas deben ser la llave para proteger la información y de la misma forma realizar las tareas más sencillas con el grado necesario de seguridad. Como observamos, hay diferentes planteamientos al problema, se puede tener protección a nivel de host, tener todo un arsenal de defensas y conocimiento de eventos en cada equipo, implica otro tipo de problemas, cual es el resultado, sistemas seguros, sistemas que puedan determinar rápidamente cual es la fuente del problema, del ataque, erradicar esa fuente de riesgo, auto protegerse, posiblemente hasta aprender de los ataques y generar automáticamente defensas, podríamos general defensas automáticas que aprendan de la solución y el tiempo de respuesta sea cada vez menor, pero podría acaso un virus burlar una protección “inteligente”, esto podría provocar un sistema de seguridad que propiamente sea también un virus, solo que evitando la reproducción de ciertos eventos que puedan causar problemas. Un sistema seguro entonces, debiera protegerse así mismo, para garantizar que las operaciones realizadas en el estarán libre de riesgos o al menos estos serán mínimos y controlables.

Algo que si debe considerarse mucho es que actualmente no existe la cultura de la protección, y mientras esta cultura continúe sin modificación será complicado avanzar hacia la creación de sistemas seguros, que sean confiables, e íntegros. El reto realmente es avanzar hacia la creación de esta cultura, y la formación de profesionales dedicados a apoyar en todos los ámbitos a que los lineamientos necesarios sean aplicados e Internet funcione como un todo seguro, a prueba de fallas, que así lo ha demostrado, pero también que sea una entidad confiable. Esto es necesario para aprovechar de mayor forma las bondades que brinda la interconexión existente y empezar a confiar en procesos cada día más importantes. La salud de Internet, si es que el termino se puede aplicar y ser utilizado, depende de cada usuario, es derecho y obligación de cada persona que la utiliza, aportar su granito de arena en convertir la red en un lugar seguro para su información, esto redundara en crear una red segura, que será mejor para todos.

BIBLIOGRAFÍA.

Amato, Vito: *Academia de Networking de Cisco Systems: Guía del primer año*. Cisco Press, 2000. ISBN 1-57870-218-6, PVP 7.900. Mas información en http://www.ciscopress.com/book.cfm?series=3&book=112

Amato, Vito: *Programa de la Academia de Networking de Cisco: Guía del segundo año*. Cisco Press, 2001. ISBN 1-578713-002-5. Mas información en http://www.ciscopress.com/book.cfm?series=3&book=181

Black, Uyless: *Tecnologías emergentes para Redes de Computadoras, 2ª Ed*. Prentice Hall, 1999. ISBN 970-17-0268-9, PVP 5.500 Pts. http://vig.prenhall.com/catalog/academic/product/1,4096,0137428340,00.html

**Schneier, Bruce. (1999),
Applied Cryptography: Protocols, Algorithms and Source Code in C. Cisco
Networking academy, Mind Wide Open, Exploration 4.0**

**Practical Cisco Routers.
Joe Habraken.**

**Seguridad Informática
José Ignacio Sánchez Marín**

**Guías base de configuración.
Scitum.**

**Seguridad Perimetral, Monitoreo de recursos de red.
Ing. Carlos Alberto Vicente.
UNAM.**

**Diseño e implantación de arquitecturas informáticas seguras: Una aproximación practica.
Albert Luis Corrales.
Universidad Rey Juan Carlos.**

www.securityfocus.com

www.symantec.com

www.virusattack.com.ar

www.kriptopolis.com

www.scitum.com

http://cisco.frcu.utn.edu.ar

http://www.petri.co.il/configure_tcp_ip_from_cmd.htm

http://www.winnetmag.com/Windows/Article/ArticleID/5082/5082.html

http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ntcmds.mspx

GLOSARIO.

ActiveX – Es una tecnología de Microsoft que permite añadir nuevo software cuando accedes a una página Web.

ADSL – Es una tecnología de transmisión de datos que te permite enviar y recibir información a gran velocidad por los hilos telefónicos de cobre convencionales.

Antivirus – Es una software que se instala en tu ordenador y que permite prevenir que programas diseñados para producir daños, también llamados virus, dañen tu equipo. También tiene la misión de limpiar ordenadores ya infectados.

ASCII – Es un conjunto de normas de codificación de caracteres mediante caracteres numéricos, de amplia utilización en informática y telecomunicaciones.

Apache – Es uno de los servidores Web más populares y utilizados. Se da la circunstancia de que es de dominio público. Está basado en el sistema operativo Linux

Aplicación – Es simplemente otra forma de llamar a un programa informático. Se instala en ordenador y nos permite realizar tareas de todo tipo. Desde mandar un correo a gestionar la contabilidad de una empresa.

AI - Asociación de internautas. Agrupa a los usuarios de Internet en España y promueve sus derechos.

Avatar - Es una imagen que los usuarios de Internet se atribuyen a la hora de escribir en foros o chatear. Suele identificar de laguna manera a dicho usuario.

Backup – También llamado *copia de seguridad,* es la tarea de duplicar y guardar cualquier tipo de datos o información en otro lugar (disco, servidor...) para que pueda ser recuperado en caso de la perdida de la información original.

Bandwidth – Ancho de banda. Es la cantidad de datos que pueden ser enviados en un espacio de tiempo determinado a través de un circuito o conexión.

Banner – Es una imagen o gráfico que permite a una empresa anunciarse. Suele ir a un lado, arriba o debajo de una página Web. Pinchando sobre el banner, se irá a la página del anunciante.

Bit – Es la unidad mínima de información digital que puede ser tratada por un ordenador.

Bluetooth – Es un sistema de conexión inalámbrica para voz y datos. Es utilizado en distancias cortas. Su límite de acción es de unos 10 metros.

Browser – Es un programa o aplicación que nos permite navegar por Internet y encontrar exactamente la información o temática que nos interesa. Las mas populares son Internet Explorer, Netscape y Firefox.

Bug – Se refiere a los fallos existentes en cualquier tipo de software o hardware.

Byte – Es una unidad de medida de información digital que se compone de 8 bits.

Cache – Es una memoria existente en el disco duro que permite guardar copias temporales de archivos para poder acceder a ellos en ciertos momentos. Cuando se accede a Internet, esto resulta muy útil ya que puede guardar algunos elementos de páginas Web para no tener que cargarlos en la próxima visita a la misma página.

CSS – Es un formato de archivo con varias instrucciones HTML que permite dar una presencia homogénea a varias páginas Web solo preocupándose de modificar dicho archivo CSS.

Certificación – Es un método por el cual una entidad o persona garantizan que un programa es de quien realmente dice ser.

Chat – Es una forma de comunicación en tiempo real (simultaneo), entre varias personas a través de Internet.

Chip – Es un circuito integrado formado por transistores y otros elementos electrónicos.

Computadora – Es un dispositivo electrónico que permite procesar información y datos con programas diseñados para ello. Actualmente este término no se usa demasiado en el mundo de la informática.

Cookie – Son pequeños ficheros que se instalan en la memoria virtual del ordenador cuando se accede a páginas Web. Sirven para que la página visitada conozca el perfil de sus visitantes, guardar contraseñas...

Copyright – Son los derechos de autor de un determinado producto.

CPU – Es un viejo término para procesador y es la unidad central de un ordenador la cual permite especificar cómo funcionará tu ordenador. Es el cerebro del tu computadora.

Criptografía – Es una forma de proteger información de vistas ajenas cuando se están transfiriendo archivos por la red.

Directorio – Es un espacio lógico de el ordenador donde se guarda y almacena información.

DOS – Fue el primer sistema operativo que se creo para los ordenadores y fue creado por Bill Gates.

Dominio – Estrictamente hablando, es un nombre que representa una entidad lógica y que puede estar formado por otros dominios formando un árbol o estructura jerárquica.

Download – *Descarga*. Se refiere al proceso de transferir datos desde un punto remoto (servidor u otro ordenador) a tu propio ordenador.

Driver - *Controlador*. Programa que generalmente forma parte del sistema operativo y que controla una pieza específica de hardware.

E-book – Es un libro pero en formato digital y con la peculiaridad de que no se compra en una librería convencional sino por Internet.

Firewall – Es un dispositivo que asegura las comunicaciones entre usuarios de una red e Internet.

Firmware - Conjunto de instrucciones integrado en el hardware que controla y dirige actividades de la memoria del microprocesador.

Formatear – Es el proceso de preparar tu disco duro para que se pueda instalar el sistema operativo.

Fragmentación - El sistema operativo almacena los datos de un fichero o archivo concreto en muchas partes del disco, dejando grandes espacios entre los registros. Al fragmentar se “colocan” todos esos espacios al principio del disco y de forma ordenada.

Gráficos – son dibujos e imágenes instalados en el ordenador.

Hardware – Hace referencia a la parte física o sólida de un ordenador u otro elemento informático.

HTML – Es el lenguaje con que se escriben las páginas Web.

Interface – Es el punto de comunicación entre dos elementos electrónicos o informáticos. Muchas veces se refiere a el como *puerto*. También se podría definir como El punto de contacto entre el usuario, el ordenador y el programa, por ejemplo, el teclado o un menú.

Internet - Red de telecomunicaciones a la cual están conectadas centenares de millones de personas, organismos y empresas en todo el mundo. Su creación fue uno de los acontecimientos mas importantes en la historia de la informática.

ISP – Organización o empresa que tiene como misión dar acceso a Internet y proporcionar ciertos servicios añadidos a usuarios o empresas.

IP - Numero de 32 bits que identifica a ordenadores o equipos de red en Internet.

Mail – *Correo*. Carta escrita virtual que se puede mandar de un ordenador a otro.

Memoria ampliada - Memoria superior a los 640 kilobytes de memoria convencional utilizada normalmente por el sistema operativo y las aplicaciones.

Menú – Es una lista de opciones para que una persona elija una acción. Es interactivo con el usuario.

Microprocesador - Componente de hardware que contiene un solo circuito integrado que lleva a cabo instrucciones.

Modem – dispositivo que servirá para conectar con Internet. Lo que hace es modular los datos digitales para su transmisión por líneas telefónicas convencionales para después remodular la señal a su llegada.

Pantalla - Monitor CRT, de plasma, LCD u otro dispositivo de reproducción de imágenes que el ordenador utiliza como dispositivo de salida de visualización.

PCMCIA – Hace referencia a las tarjetas de memoria utilizadas en los ordenadores personales.

Píxel – Es la unidad mas pequeña con la que se forman las imágenes.

Placa base – Es la tarjeta de circuito impreso principal donde van conectados los demás elementos que componen el ordenador como son tarjetas gráficas, de sonido, memorias, discos duros...

Plug and Play – Es un método por el cual el ordenador reconoce

automáticamente un nuevo dispositivo insertado.

Protocolo - Conjunto de reglas que establecen la temporización y el formato del intercambio de datos.

Puerto serie – También llamado puerto COM. Es un conector en la parte trasera de la caja donde se pueden conectar algunos dispositivos como el ratón, un modem o una impresora.

ROM – Es una memoria del ordenador que se encarga de ciertas funciones básicas del ordenador.

Sistema informático – Es el conjunto de elementos hardware, software y periféricos que conectados entre si, forman un ordenador.

Sistema operativo – Es un conjunto de programas que sirven para manejar un ordenador.

Software - El conjunto de programas, procedimientos y documentación asociado a un sistema informático.

Tarjeta – Es una placa electrónica que va normalmente conectada a la placa base y sirve para realizar ciertas funciones.

VGA - Se trata de un adaptador de vídeo estándar que permite ejecutar cualquier programa software de los más conocidos