Riesgos, Políticas y Herramientas de Seguridad en Redes

Edwin ■ Montoya
Jorge ■ Alonso ■ Cañón

Desde los comienzos de la computación, los sistemas han estado expuestos a una serie de peligros o riesgos que han aumentando conforme se globalizan más las comunicaciones entre estos sistemas.

Inicialmente la seguridad fue enfocada al control de acceso físico ya que para acceder a un computador se requería la presencia física del usuario frente al sistema.

Posteriormente comienzan a proliferar los sistemas *multiusuario* en los cuales un recurso

Edwin Montoya. Profesor y Coordinador del área de Telemática. Universidad Eafit.
emontoya@eafit.edu.co.

Jorge Alonso Cañón. Ingeniero y profesor de Telemática. Universidad Eafit. jcanon@eafit.edu.co.

computacional era compartido por varios usuarios, surgen nuevos riesgos como la utilización del sistema por personas no autorizadas, manipulación de información o aplicaciones por suplantación de usuarios, aparece un primer esquema de protección basado en Códigos de usuarios y Contraseñas (passwords) para restringir el acceso al sistema, además se establecen distintas categorías de control de acceso a los recursos.

Siguen evolucionando los sistemas y se inicia la computación en red, en la cual además de los riesgos asociados a los sistemas multiusuarios, aparece un nuevo tipo de vulnerabilidad, básicamente en el proceso de transmisión de la información; aunque las primeras redes estaban aisladas del mundo exterior a la empresa, estaban expuestas a los posibles atacantes internos. La evolución tecnológica continúa y comienza el proceso de interconexión de las distintas redes aisladas de una empresa para configurar redes corporativas, donde aumentan considerablemente los riesgos ya que es más difícil controlar la totalidad de la red.

Quizás hoy en día estamos en la fase en la cual nuestras redes empresariales están siendo conectadas a redes públicas como Internet, CompuServer, BitNet, etc., en las cuales la seguridad se ha convertido en un problema realmente serio, pero a pesar que nuestro horizonte de oportunidades ha sido ampliado a millones de potenciales clientes, los posibles atacantes también han crecido en forma considerable.

Es responsabilidad de los diseñadores y administradores de los sistemas computacionales, proveer la suficiente garantía y confiabilidad que permita operar en las mejores condiciones y lograr un funcionamiento continuo de los sistemas bajo el mejor clima de confianza de los usuarios, garantizando el respeto por niveles adecuados de confidencialidad e integridad de la información que se procesa.

Aunque inicialmente el interés de entrar ilegalmente a los sistemas fue el reto técnico de lograrlo, el número de incidentes y ganancias por la entrada ilegal ha aumentado considerablemente. Incidentes como el robo de información, espionaje industrial, estafas, extorsión, daño de sistemas, terrorismo, etc. se cuentan como los nuevos objetivos de ataques a nuestros sistemas.

Entre los aspectos más relevantes de preocupación en los sistemas de seguridad se encuentra todo lo relacionado con: 1) los típicos servidores con sistemas operativos como UNIX, DEC, NT, Netware, etc. los cuales, de alguna forma, representan grandes riesgos. 2) Los protocolos de comunicaciones representan uno de los puntos de vulnerabilidad más utilizado en las redes. 3) Las aplicaciones del sistema o de los usuarios. 4) Bases de datos, entre otros tópicos.

Definitivamente si se quieren minimizar los riesgos (nunca hay un sistema 100% protegido), se debe tomar conciencia del problema y adoptar una metodología o guías para enfrentarlo. Esto comienza con el conocimiento profundo de nuestra red, un análisis de amenazas y riesgos, la adopción de políticas de seguridad y finalmente la utilización de las tecnologías adecuadas para implantar

un sistema de seguridad, el cual incorpora herramientas de criptografía, cortafuegos (Firewalls), monitoreo, auditoría y hasta esquemas proactivos que permita adelantarse a los ataques y prevenirlos.

Es responsabilidad de los diseñadores y administradores de los sistemas computacionales, proveer la suficiente garantía y confiabilidad que permita operar en las mejores condiciones y lograr un funcionamiento continuo de los sistemas bajo el mejor clima de confianza de los usuarios, garantizando el respeto por niveles adecuados de confidencialidad e integridad de la información que se procesa.

El objetivo de este artículo es mostrar los peligros o amenazas que poseen los sistemas, cómo diseñar políticas adecuadas de seguridad y las herramientas disponibles para implantar proyectos de seguridad, en los cuales las técnicas de criptografía para el montaje de servicios acompañados con cortafuegos y otros elementos, ayudan a ofrecer servicios seguros aún en ambientes hostiles como el de Internet.

1. AMENAZAS Y ATAQUES

Para analizar el contexto de la seguridad en redes, se define un Sistema Informático como un conjunto de elementos hardware, software, datos/información y personal que hacen posible el almacenamiento, proceso y transmisión de la información con el objetivo de realizar una determinada tarea. Todos estos elementos son susceptibles de ser atacados y sobre ellos tenemos una serie de amenazas.

Aunque son varios los elementos que conforman un sistema informático, es la INFORMACIÓN el recurso más preciado sobre el cual se enfoca todos los esfuerzos para asegurar un nivel aceptable de seguridad. Por esto, se definen los objetivos básicos de la seguridad de la información:

1. *Confidencialidad:* Asegurar que la información no esté expuesta o revelada a personas no autorizadas.
2. *Integridad:* Asegurar consistencia de los datos, en particular prevenir la creación, alteración o borrado de datos de entidades no autorizadas.
3. *Disponibilidad:* Asegurar que los usuarios legítimos no obtengan acceso denegado a su información y recursos
4. *Uso legítimo:* Asegurar que los recursos no sean usados por personas no autorizadas o en formas no autorizadas.

Para soportar estos objetivos se definen las Políticas de Seguridad que regirán en nuestro dominio de seguridad. Estas políticas deben ser definidas en varias categorías: acceso físico, seguridad en la comunicación, computadoras, sistemas operativos, bases de datos, aplicaciones, personal, ambiente natural, respaldos, planes de contingencias, etc.

Una *Amenaza* es una persona, entidad, evento o idea que plantea algún daño a un activo.

Un *Ataque* es una realización de una amenaza.

Una *Protección* son los controles físicos, mecanismos, políticas y procedimientos que protegen los activos o recursos de las amenazas.

Una Vulnerabilidad es el debilitamiento o ausencia de una protección en un recurso o activo.

Un Riesgo es una medida del costo de una realización de una vulnerabilidad que incorpora la probabilidad de éxito de un ataque. El riesgo es alto si el valor del activo vulnerable es alto y la probabilidad de éxito de un ataque es alto.

Las amenazas pueden ser clasificadas en intencionales y accidentales siendo las primeras las más peligrosas. Las amenazas intencionales lo cual se convierte en un ataque, puede ser pasivo o activo.

Un ataque pasivo es aquel que no causa modificación o cambio en la información o recurso, son los más peligrosos ya que los fines que se alcanzan son más letales y beneficiosos para el que los comete. ("Quizás en este momento en su red tenga un intruso invisible"). Los ataques activos, son aquellos que producen cambios en la información o en el comportamiento del sistema.

Clasificación de las amenazas

1. *Amenazas fundamentales:* Afectan directamente los cuatro objetivos básicos de la seguridad: fugas de información, violación a la integridad, negación de servicios y uso ilegítimo.

2. *Amenazas habilitadoras de las primarias:* Son importantes porque la realización de cualquiera de estas amenazas puede conducir directamente a la realización de las amenazas fundamentales. Estas son:
   - *Suplantación:* Una persona o entidad pretende ser otra diferente. Es la forma más común de penetración al perímetro de seguridad.
   - *Sobrepasar los controles:* Un atacante explota las fallas de un sistema o debilidad de seguridad para adquirir acceso no autorizado a los recursos u obtener privilegios.
   - *Violación con autorización:* Una persona autorizada para usar un sistema o recurso, lo utiliza para lograr un propósito no autorizado. Es conocido como amenaza interna.
   - *Caballo de Troya:* Un software que contiene una parte invisible de código, la cual cuando es ejecutada compromete la seguridad del sistema.
   - *Puerta trasera:* Es una característica incorporada en un software que ante un evento o entrada ejecuta acciones que pueden comprometer la seguridad del sistema.
   - *Bombas lógicas:* Son códigos adicionados a los programas que ante ciertas fechas o tiempo de ejecución ejecutan acciones perjudiciales para el sistema.
   - *Virus:* Son programas que se autoreplican y afectan principalmente los archivos ejecutables, a veces llegan a afectar a miles de computadoras.

3. *Amenazas subyacentes:* Si analizamos cualquiera de las amenazas fundamentales o de habilitación de las primarias en un ambiente dado, podemos identificar amenazas subyacentes particulares cualquiera de las cuales puede habilitar las amenazas

fundamentales. Por ejemplo si consideramos la amenaza fundamental de fugas de información podemos encontrar varias amenazas subyacentes, tales como:

- Escuchar sin autorización
- Análisis de tráfico
- Indiscreción por personal
- Reciclaje de medios.

Según estadísticas obtenidas, las siguientes amenazas o tipos de ataque más predominantes son:

- Violación con autorización
- Suplantación
- Sobrepasar los controles
- Caballos de Troya y puertas traseras.

2. SERVICIOS DE SEGURIDAD

Los servicios básicos desarrollados en un ambiente de comunicaciones son categorizados en 5 tópicos:

Servicio de autenticación: Provee aseguramiento de la identidad de alguna entidad. Las contraseñas o passwords son la forma más común de proveer este servicio. Autenticación es el servicio más importante ya que todos los otros servicios dependen en gran medida de éste. Definimos dos contextos de autenticación:

1. *Autenticación de entidad*, en el cual la entidad remota se identifica ante el servicio, también se conoce como autenticación simple.

2. *Autenticación del origen de los datos:* autentica la fuente real de los datos sin importar que pase por muchos sistemas intermedios.

Servicio de control de acceso: Protege contra acceso no autorizado o manipulación de recursos. Contribuye directamente a lograr las metas de seguridad de confidencialidad, integridad, disponibilidad y uso legítimo. El modelo general para un control de acceso asume un conjunto de entidades activas llamadas Sujetos (Iniciadores) los cuales intentan acceder un miembro de un conjunto de recursos pasivos llamadas Objetos (Destinos).

Servicio de confidencialidad: Protege que la información sea divulgada o distribuida a entidades no autorizadas. Se distinguen dos tipos de confidencialidad:

1. *Confidencialidad de datos:* El cual está relacionada con el almacenamiento de la información.
2. *Confidencialidad del flujo de tráfico:* El cual está relacionada con el proceso de transmisión de información. Se dan tres casos diferentes de confidencialidad del flujo: confidencialidad de un servicio orientado a la conexión, confidencialidad de un servicio no orientado a la conexión y servicio de confidencialidad de campo selectivo.

Servicio de integridad de datos: Asegura que los datos no sean cambiados, borrados o sustituidos sin autorización, al igual que el servicio de confidencialidad, diferencia entre integridad de datos e integridad de la comunicación.

Servicio de no repudio: Protege que cualquiera de las dos entidades que participen en una comunicación nieguen que el intercambio ha ocurrido. A diferencia de los anteriores servicios, el objetivo de éste es proteger a los usuarios de la comunicación contra amenazas del otro usuario legítimo más que de atacantes. Cada una de las partes posee pruebas irrefutables ante desacuerdos del origen o destino de los datos. Sin embargo la provisión de este servicio debe considerar el concurso de una tercera parte que ambos extremos de una comunicación confían. Podemos distinguir dos casos:

1. *Repudio de origen:* El destino tiene pruebas demostrables ante terceros de la autenticidad del origen de los datos.

2. *Repudio de destino:* El origen tiene pruebas demostrables ante terceros de la autenticidad del receptor y recepción de los datos.

2.1 SEGURIDAD EN LOS SISTEMAS OPERATIVOS

Una de las principales causas técnicas de violaciones a sistemas informáticos son generados por las fallas intencionales o accidentales de los sistemas operacionales. La mayoría de los sistemas operacionales comerciales y de dominio público presentan altas deficiencias en su base de seguridad, ya que no fueron diseñados con este objetivo como primordial sino que han sido agregados como módulos independientes.

Para agravar más la situación uno de los sistemas operacionales que más prolifera en Internet (UNIX) presenta un ambiente muy propicio para ser atacado, debido a que su código ha sido ampliamente difundido y se conocen muchos detalles de su implementación.

Una de las principales causas técnicas de violaciones a sistemas informáticos son generados por las fallas intencionales o accidentales de los sistemas operacionales. La mayoría de los sistemas operacionales comerciales y de dominio público presentan altas deficiencias en su base de seguridad, ya que no fueron diseñados con este objetivo como primordial sino que han sido agregados como módulos independientes.

Lo ideal es desarrollar un sistema operativo "seguro" el cual pueda ofrecer entre otros las siguientes características: identificación y autenticación de todos los usuarios que ingresan al sistema, controle el acceso a todos los recursos e informaciones, contabilice todas las acciones realizadas por los usuarios, audite los acontecimientos que puedan representar amenazas a la seguridad, garantice la integridad de los datos, mantenga la disponibilidad de los recursos e información.

Las amenazas que se pueden presentar en un sistema operacional son las más variadas ya que aparte de las propias del sistema operacional, se le agrega la de todos los protocolos de comunicaciones.

Dentro de las amenazas que vale la pena resaltar son las ofrecida por los programas hostiles, ocasionados por errores no intencionales, desarrollo y mala instalación o por voluntad de un programador, pueden

provocar mal funcionamiento o pérdida de información. Entre los programas hostiles más comunes están: los caballos de Troya, programas salami (redondean cálculos financieros a favor del programador), canales ocultos, puertas traseras, bombas lógicas o de tiempo, programas voraces (consumo de recursos como CPU o memoria), virus, gusanos, etc.

Clasificación de los sistemas operativos seguros:

Debido a la alta participación de los niveles militares principalmente en los Estados Unidos, a través del Departamento de defensa (DoD) quien a través del organismo National Computer Security Center (NCSC) publicó en 1985 un documento titulado "Trusted Computer Systems Evaluation Criteria [TCSEC]" conocido informalmente como el "Libro Naranja", especifica diferentes niveles de seguridad en hardware, software y firmware, así como metodologías de evaluación de los sistemas informáticos respecto a su seguridad. Los criterios de evaluación están jerarquizadas en cuatro divisiones: D, C, B y A expresando esta división requerimientos progresivos de seguridad. En algunas divisiones hay subdivisiones llamadas clases. A continuación brevemente se describe esta clasificación:

División D: Protección mínima, se otorga a un sistema que no cumple los requisitos mínimos.

División C: Protección discrecional.

- *Clase C1:* Protección mediante seguridad discrecional, separación entre usuarios y datos.

- *Clase C2:* Protección mediante control de accesos, añade a la anterior facilidades de contabilidad y auditoría para los objetos.

División B: Protección obligatoria.

- *Clase B1:* Protección mediante etiquetas. Adiciona el concepto de compartimento.

- *Clase B2:* Protección estructurada. Posee un modelo de seguridad formal, revisado y probado, con un control de acceso tanto obligatorio como discrecional y los mecanismos de autenticación deben ser reforzados.

- *Clase B3:* Dominios de seguridad. Los sujetos y Objetos del sistemas son agrupados en dominios lo que permite una mejor estructuración de la seguridad.

División A: Protección verificada.

- *Clase A1:* Diseño verificado. Funcionalmente es igual a la clase B3 pero añade especificaciones de diseño y técnicas de verificación formal, que garantice que las funciones de seguridad han sido correctamente implementadas.

3. POLÍTICAS DE SEGURIDAD

Para lograr un efectivo control sobre todos los componentes que conforman la red y asegurar que su conectividad a otras redes no es algo frágil, es necesario primero que todo establecer con exactitud qué recursos de la red

y servicios desea proteger, de tal manera que esté preparado para conectar su red con el resto del mundo. Esto implica el estudio y definición de los aspectos necesarios para la planeación de la seguridad de la red, análisis de riesgos, identificación de recursos y amenazas, uso de la red y responsabilidades, planes de acción o contingencia, etc.

3.1 DEFINICIÓN

Una política de seguridad es un conjunto de leyes, reglas y prácticas que regulan cómo una organización maneja, protege y distribuye información sensitiva. Este documento se convierte en el primer paso para construir barreras de protección efectivas.

Para lograr un efectivo control sobre todos los componentes que conforman la red y asegurar que su conectividad a otras redes no es algo frágil, es necesario primero que todo establecer con exactitud qué recursos de la red y servicios desea proteger, de tal manera que esté preparado para conectar su red con el resto del mundo. Esto implica el estudio y definición de los aspectos necesarios para la planeación de la seguridad de la red, análisis de riesgos, identificación de recursos y amenazas, uso de la red y responsabilidades, planes de acción o contingencia, etc.

Es importante tener una política de seguridad de red efectiva y bien pensada que pueda proteger la inversión y recursos de información de su compañía. Sobre todo es importante que la organización defina claramente y valore qué tan importantes son los recursos e información que se tienen en la red corporativa y dependiendo de ésto justificará si es necesario que se preste la atención y esfuerzos suficientes para lograr un nivel adecuado de protección. La mayoría de las organizaciones poseen información sensible y secretos importantes en sus redes, esta información debería ser protegida contra el vandalismo del mismo modo que otros bienes valiosos como propiedades de la corporación y edificios de oficinas.

Una política de seguridad en un sitio es requerida para establecer a lo largo de la organización un programa de cómo usuarios internos y externos interactúan con la red de computadores de la empresa, cómo se implementará la arquitectura de la topología de red y dónde se localizarán los puntos especiales de atención en cuanto a protección se refiere.

La definición de una política de seguridad de red no es algo en lo que se pueda establecer un orden lógico o secuencia aceptada de estados debido a que la seguridad es algo muy subjetivo, cada negocio tiene diferentes expectativas, diferentes metas, diferentes formas de valorar lo que va por su red, cada negocio tiene distintos requerimientos para almacenar, enviar y comunicar información de manera electrónica; por esto nunca existirá una sola política de seguridad aplicable a 2 organizaciones diferentes. Además, así como los negocios evolucionan para adaptarse a los cambios en las condiciones del mercado, la política de seguridad debe evolucionar para satisfacer las condiciones cambiantes de la tecnología. Una política de seguridad de red efectiva es algo que todos los usuarios y administradores pueden aceptar y están dispuestos a reforzar, siempre y cuando la política no disminuya la capacidad de la organización, es decir la política de seguridad debe ser de tal forma que

no evite que los usuarios cumplan con sus tareas en forma efectiva.

3.2 ¿POR QUÉ UTILIZAR POLÍTICAS DE SEGURIDAD EN UN SITIO?

Existen muchos factores que justifican el establecimiento de políticas de seguridad para un sitio específico, pero los más determinantes son:

- Ayudan a la organización a darle valor a la información.
- Es una infraestructura desde la cual otras estrategias de protección pueden ser desarrolladas.
- Proveen unas claras y consistentes reglas para los usuarios de la red corporativa y su interacción con el entorno.
- Contribuyen a la efectividad y direccionan la protección total de la organización.
- Pueden ayudar a responder ante requerimientos legales
- Ayudan a prevenir incidentes de seguridad.
- Proveen una guía cuando un incidente ocurre.
- Es una planeación estratégica del papel que juega la arquitectura de red al interior de la organización.
- Ayuda en la culturización de los usuarios para el uso de servicios de red e inculca el valor real que ellos representan.

3.3 CARACTERÍSTICAS DE LAS POLÍTICAS

Una política de seguridad es un plan elaborado de acuerdo con los objetivos generales de la organización y en el cual se ve reflejado el sentir corporativo a cerca de los servicios de red y recursos que se desean proteger de manera efectiva y que representan activos importantes para el normal cumplimiento de la misión institucional. Por esto la política de seguridad debe cumplir con ciertas características propias de este tipo de planes, como son:

- Debe ser simple y entendible (específica).
- Debe estar siempre disponible.
- Se puede aplicar en cualquier momento a la mayoría de situaciones contempladas.
- Debe ser practicable y desarrollable.
- Se debe poder hacer cumplir.
- Debe ser consistente con otras políticas organizacionales.
- Debe ser estructurada.
- Se establece como una guía, no como una cadena a la cual se tenga que atar para siempre.
- Debe ser cambiante con la variación tecnológica.
- Una política debe considerar las necesidades y requerimientos de seguridad de todas las redes interconectadas como una unidad corporativa.

3.4 DESARROLLO DE UNA POLÍTICA DE SEGURIDAD

El objetivo perseguido para desarrollar una política de seguridad de red oficial corporativa es definir las expectativas de la organización acerca del uso de la red y definir procedimientos para prevenir y responder a incidentes de seguridad provenientes del cada día más avanzado mundo de la comunicación global.

Definir una política de seguridad de red significa desarrollar procedimientos y planes que salvaguarden los recursos de la red contra pérdidas y daños, por lo tanto es muy importante analizar entre otros los siguientes aspectos:

- Determinar los objetivos y directrices de la organización.
- La política de seguridad debe estar acorde con otras políticas, reglas, regulaciones o leyes ya existentes en la organización; por lo tanto es necesario identificarlas y tenerlas en cuenta al momento de desarrollar la política de seguridad de redes.
- Identificación de los recursos disponibles.
- ¿Qué recursos se quieren proteger?
- ¿De quién necesita proteger los recursos?
- Identificación de posibles amenazas
- ¿Qué tan reales son las amenazas?
- ¿Qué tan importante es el recurso?
- ¿Qué medidas se pueden implantar para proteger sus bienes de una manera económica y oportuna?
- Verificación frecuente de la política de seguridad de red para ver si los objetivos y circunstancias han cambiado.

En general, el costo de proteger las redes de una amenaza debe ser menor que el costo de la recuperación, si es que se ve afectado por la amenaza de seguridad. La política de seguridad debe ser comunicada a cada quien que usa un computador en la red con el fin de que sea ampliamente conocida y se pueda obtener una retroalimentación de los usuarios de la misma para efectos de revisiones periódicas y detección de nuevas amenazas o riesgos.

3.5 IDENTIFICACIÓN DE LOS ELEMENTOS A PROTEGER

El primer paso en la creación de la política de seguridad es crear una lista de todas las cosas que necesitan ser protegidas, esta lista debe ser regularmente actualizada. Algunos elementos a considerar son entre otros:

- Hardware: CPUs, Tarjetas, teclados, terminales, estaciones de trabajo, Pcs, impresoras, unidades de almacenamiento, líneas de comunicación, enrutadores, servidores de acceso remoto.
- Software: Programas fuentes, programas objeto, utilidades, programas de diagnóstico, sistemas operacionales, programas de comunicaciones.
- Datos: Durante la ejecución, almacenados en línea, almacenados fuera de línea, respaldos, rastreos de auditoría, bases de datos, en tránsito sobre los medios físicos de comunicación.
- Personas: Usuarios, personal externo con uso de servicios locales.
- Documentación: de programas, hardware, procedimientos de administración local.
- Otros: Medios magnéticos, papel, formas, etc.

3.6 ANÁLISIS DE RIESGOS

El análisis de riesgos involucra la determinación de qué se necesita proteger, contra qué lo necesita proteger, qué se necesita para protegerlo y cómo. Es el proceso de examinar los posibles riesgos y clasificarlos por nivel de severidad, ésto involucra hacer decisiones costo-beneficio. Algunos riesgos incluyen:

- Acceso no autorizado.
- Servicios no disponibles.
- Descubrimiento de información sensitiva.

Como resultado de este proceso se obtiene un esquema para pesar el riesgo contra la importancia del recurso lo cual permitirá determinar cuánto esfuerzo se debe gastar en proteger el recurso.

3.7 DEFINICIÓN DE POLÍTICAS DE USO ACEPTABLE

Los procedimientos antes descritos son una parte de la solución para el desarrollo de una política de seguridad pero no lo son en la totalidad, uno de los aspectos importantes para complementar es cómo los usuarios interactúan con la red y de allí se extraen elementos adicionales. Algunos otros factores a analizar son:

- ¿A quién se le permite el uso de los recursos?
- ¿Cuál es el uso apropiado para los recursos?
- ¿Quién está autorizado para garantizar acceso y aprobar el uso de recursos?
- ¿Quién puede tener privilegios para la administración del sistema?
- ¿Cuáles son los derechos y responsabilidades de los usuarios?
- ¿Cuáles son los derechos y responsabilidades de los administradores del sistema?
- ¿Qué es información altamente sensible?

3.8 AUDITORÍA Y REVISIÓN

Es necesario contar con herramientas que ayuden a determinar si hay una violación a las políticas de seguridad, para ello se debe aprovechar al máximo las herramientas incluídas en los sistemas operacionales y utilidades de la red. La mayoría de sistemas operacionales cuentan con bastantes rastros o archivos de "log" con el fin de informar de la actividad del sistema, la examinación de estos "logs" son el primer paso efectivo para detectar el uso no autorizado del sistema. Para tal efecto se pueden tomar acciones como:

- Comparar listas de usuarios actualmente conectados con listas históricas, para detectar anomalías o comportamientos irregulares.
- Examinar las facilidades de "log" del sistema para chequear mensajes de error inusuales del software del sistema operacional como por ejemplo, un número grande de intentos fallidos de conexión a un usuario específico.
- Comparación de los procesos que están siendo ejecutados en las máquinas a tiempos diferentes pueden mostrar diferencias que lleven a detectar programas no autorizados o extraños en ejecución, quizás lanzados por intrusos.

3.9 COMUNICACIÓN A LOS USUARIOS

La política de seguridad debe ser informada a todos los usuarios de la red para que conozcan acerca del uso apropiado que rige su acceso o estación de trabajo específica. También debe ir acompañada por una campaña educacional que indique como se espera que sean usados todos los recursos involucrados en la red corporativa y cómo se pueden proteger por ellos mismos de accesos

no autorizados. Implantar una política de seguridad de red efectiva es un esfuerzo colectivo y como tal se deben proveer los medios para que los usuarios participen activamente en la definición de la misma y hagan aportes de lo que ellos mismo perciben de su interacción con la red.

Si los usuarios perciben que la política reduce su productividad, se debe permitir que participen. Si es necesario se pueden añadir recursos adicionales a la red para asegurar que los usuarios pueden continuar haciendo su trabajo sin pérdida en la productividad. Para crear una política de seguridad de red efectiva es necesario encontrar un balance entre la protección y la productividad.

3.10 ASEGURAR RESPONSABILIDADES EN TORNO A LA POLÍTICA DE SEGURIDAD

Un aspecto importante en torno a la política de seguridad de red es asegurar que todos saben cuál es su responsabilidad para mantener la seguridad, por lo tanto la política debe poder garantizar que cada tipo de problema tiene a alguién que puede manejarlo de manera responsable. Así mismo pueden existir varios niveles de responsabilidad asociados con una política de seguridad de red. Por ejemplo cada usuario de la red está responsabilizado por su clave de acceso, un usuario que pone en riesgo su cuenta de acceso aumenta la probabilidad de comprometer otras cuentas y recursos. Por otro lado los administradores de red y de sistema son responsables de mantener la seguridad general de la red.

4. SISTEMAS DE CRIPTOGRAFíA

Una de las tecnologías fundamentales para garantizar una seguridad adecuada es mediante las técnicas de encripción. En términos generales la encripción consiste en evitar que el contenido de un mensaje sea conocido por entidades no autorizadas. Estas técnicas se utilizan desde tiempos inmemoriales y ha sufrido grandes evoluciones hasta el punto de lograr un grado de formalización y de bases científicas de las técnicas actuales.

Antiguamente la robustez de los métodos de encripción estaba garantizada en la medida que el algoritmo o la forma de encriptar el mensaje se mantuviese en secreto, esto presenta grandes desventajas ya que con el seguimiento de los mensajes cifrados era posible descubrir el mensaje y el algoritmo de encripción.

A partir de 1970 comienza a generarse una nueva generación de sistema de encripción en los cuales ya la base del sistema de seguridad no es mantener en secreto el algoritmo y por el contrario éste es público y estandarizo, pero la fortaleza de los métodos se centra en mantener las *Claves* de encripción en secreto.

Basado en este esquema se desarrollan dos estrategias que hoy en día se reconoce como los pilares de la criptografía, son éstos los sistemas de clave secreta o simétricos y los sistemas de clave pública o asimétricos.

En los sistemas de clave secreta, los mensajes son cifrados y descifrados con la misma clave

lo que implica que ambas partes deben conocer de antemano dicha clave. Es precisamente el hecho que ambas entidades deben poseer la misma clave lo que ha generado desconcierto en estos sistemas, sin embargo posee gran rapidez y combinado con esquemas de clave pública representa una fortaleza a los sistemas criptográficos modernos. El sistema *DES (Data Encription Standard)* representa el estándar de mayor difusión para los sistemas simétricos.

En los sistema de clave pública, cada entidad que participa en la comunicación posee un par de claves, una que denomina *Clave Pública (Kpu)* la cual es conocida por todos los usuarios de un dominio de seguridad y es utilizada para cifrar los mensajes destinado al dueño de dicha clave pública; y posee otra *Clave Privada (Kpr)* la cual es sólo conocida por el dueño de la clave y no hay necesidad de transmitirla por ningún medio telemático. La robustez de este algoritmo consiste en que un mensaje cifrado con la clave pública sólo puede ser descifrado con el poseedor de la clave privada que debe estar bien custodiada por el dueño. Igualmente estos algoritmos de clave pública son la base para las técnicas de *Firmas Digitales*. Uno de los esquemas más difundidos de clave pública es el *RSA (Rivest, Shamir y Adleman)*.

5. CORTAFUEGOS *(FIREWALLS)*

La conectividad de una red privada corporativa a redes como Internet hace necesario que haya mecanismos de seguridad que permitan un alto grado de confiabilidad y protección de la información, para ello una de las más típicas y eficaces formas existentes son los llamados *FIREWALLS* o barreras de protección, los cuales previenen los accesos indeseables hacia el interior de su red o a alguna porción de la misma.

Una red privada que lleva información sensitiva entre computadores locales requiere de medidas de seguridad propias para proteger la privacidad e integridad del tráfico; cuando tal red privada se conecta a otras redes, o cuando se permite acceso telefónico hacia el interior de la misma, los puntos de conexión remotos, líneas telefónicas y otras conexiones se convierten en extensiones de la red privada que deben ser protegidas apropiadamente. Por lo tanto es necesario un sistema que provea mecanismos para reducir al máximo el riesgo de ataques externos que puedan causar pérdida de información o daños en la integridad de la red o ampliar las posibilidades de acceso no permitido; estos mecanismos deben garantizar fuertes procesos de autenticación de usuarios, control de acceso y protección de la integridad de datos sensibles en la red privada o conjunto de redes.

5.1 ¿QUÉ ES UN *FIREWALL*?

Es un mecanismo para restringir acceso entre la Internet y la red corporativa interna. Típicamente se instala un *firewall* en un punto estratégico donde una red (o redes) se conectan a la Internet. La existencia de un *firewall* en un sitio Internet, reduce considerablemente las probabilidades de ataques externos a los sistemas corporativos y redes internas, además puede servir para evitar que los propios usuarios internos comprometan la

seguridad de la red al enviar información peligrosa (como passwords no encriptados o datos sensitivos para la organización) hacia el mundo externo.

Los ataques a sistemas conectados a Internet que se están viendo hoy por hoy son más serios y técnicamente complejos que en el pasado y la labor de proteger estos sistemas tiene también que serlo, los *firewalls* son mecanismos altamente apropiados para garantizar dicha protección. Aunque es altamente recomendable la inclusión de éstos en un plan de seguridad de redes, los *firewalls* solamente son uno de los componentes, es también de vital importancia que se establezca una política de seguridad en la que se observe claramente las tendencias de la organización referente a la seguridad informática y en la que se considere concretamente el objetivo de un *firewall*.

En la industria de la construcción un *firewall* es diseñado para evitar que el fuego se extienda entre diferentes partes de los edificios, en teoría un *firewall* en Internet tiene un propósito similar: previene que los peligros o amenazas de la Internet se extiendan hacia la red interna.

5.2 OBJETIVOS DE UN *FIREWALL*

Un *firewall* sirve para múltiples propósitos, entre otros podemos anotar los siguientes:

- Restricción de entrada de usuarios a puntos cuidadosamente controlados de la red interna.
- Prevención ante los intrusos que tratan de ganar espacio hacia el interior de la red y los otros esquemas de defensas establecidos.
- Restricción de uso de servicios tanto a usuarios internos como externos.

Todo el tráfico que viene de la Internet o sale de la red corporativa interna pasa por el *firewall* de tal forma que él decide si es aceptable o no.

¿Qué significa ser aceptable? Significa que cualquier cosa que sea la que se esté haciendo (correo electrónico, transferencia de archivos, conexiones remotas o cualquier clase de interacción específica entre sistemas) está conforme a lo estipulado en la política de seguridad del sitio; las políticas de seguridad son diferentes para cada sitio, algunas son altamente restrictivas y otras son relativamente abiertas.

Lógicamente un *firewall* es un separador, un bloqueador y un analizador. La implantación física varía entre cada sitio, la mayoría de las veces un *firewall* es un conjunto de componentes de hardware como un enrutador, un servidor o una combinación de enrutadores, computadores y redes con el software apropiado. Hay una variedad de formas para configurar este equipo, la configuración dependerá de la política de seguridad específica del sitio, presupuesto y funcionalidad dentro de la plataforma de red.

Los *firewalls* ofrecen beneficios significantes para la seguridad, pero ellos no pueden resolver cada problema de seguridad que se presente en el vasto mundo de Internet.

5.3 ¿POR QUÉ UN *FIREWALL*?

Básicamente la razón para la instalación de un *firewall* es casi siempre la misma: proteger una red privada contra intrusos dentro de un esquema de conectividad a Internet. En la mayoría de los casos, el propósito es prevenir el acceso de usuarios no autorizados a los recursos computacionales en una red privada y a menudo prevenir el tráfico no autorizado de información propietaria hacia el exterior.

Con el auge y crecimiento de instituciones comerciales y gubernamentales conectándose a la Internet, la demanda por *firewalls* también aumenta al aumentar los problemas potenciales de seguridad; muchas instituciones solucionan simplemente el problema decidiendo no conectarse a la Internet pero esto tiene que cambiar ya que no es una solución apropiada.

5.3 ¿QUÉ PUEDE HACER UN *FIREWALL*?

Es clara la intención inicial del uso del firewall, pero adicionalmente permite obtener ventajas adicionales en campos que van más allá de la seguridad como tal; entre otras podemos anotar las siguientes:

- Es un punto centralizado para las decisiones de seguridad.
- Puede reforzar la política de seguridad.
- Puede rastrear la actividad Internet eficientemente.
- Limita la revelación de su red al público.

5.4 ¿QUÉ NO PUEDE HACER UN *FIREWALL*?

Los *firewalls* son una buena alternativa contra amenazas en la seguridad de la red, pero no son una solución de seguridad completa, existen ciertas amenazas fuera del control del *firewall*. Algunas de estas "debilidades" son:

- No protege de usuarios internos "maliciosos".
- No puede proteger contra conexiones que no pasan a través de él.
- No tiene un esquema de protección para cada nueva amenaza.
- No puede proteger contra virus.

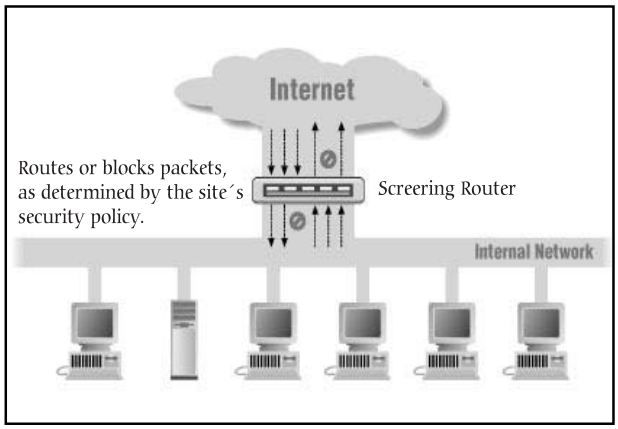
CONSIDERACIONES DE DISEÑO

5.5 *FIREWALLS* Y SUS COMPONENTES

Cuando se habla a cerca del diseño e implementación de arquitecturas de *firewalls* es necesario clarificar una serie de términos para describir los componentes de la arquitectura, algunos de ellos son:

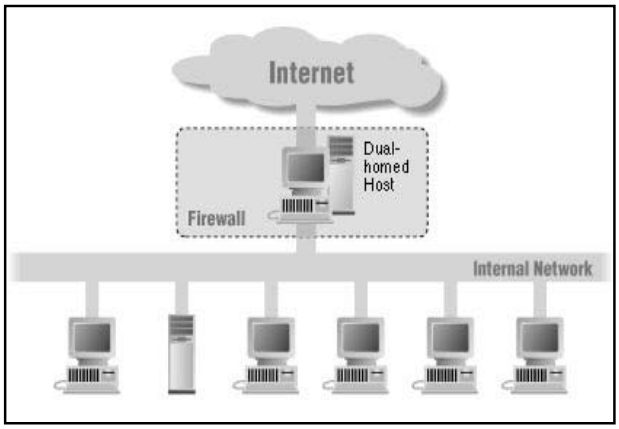
Screening Router: Es un componente básico de la mayoría de *firewalls*, puede ser un enrutador comercial o un enrutador basado en un servidor con alguna clase de software para filtrado de paquetes. Típicamente tienen la habilidad de bloquear tráfico entre redes o máquinas específicas a nivel de puerto IP. Algunos *firewalls* consisten solamente en un *Screening* router entre una red privada y la Internet.

Es muy usado para la implementación de filtrado de paquetes, en la cual se permiten o bloquean ciertos tipos de paquetes para reflejar la política de seguridad corporativa, el esquema de diseño se muestra en la siguiente gráfica:



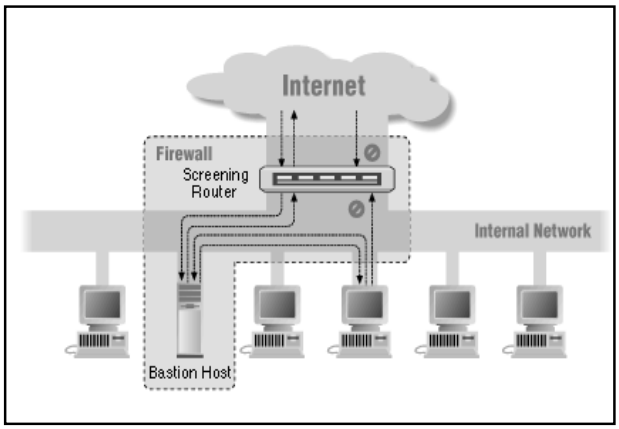
Bastion Host: Es un sistema identificado por el administrador del *firewall* como un punto crítico en el sistema de seguridad de la red, generalmente tienen algún grado de extra protección.

Dual Homed Gateway: Algunos *firewalls* son implementados sin un *Screening* router colocando una máquina de cara a la red interna por un lado y a la Internet por el otro (2 interfaces de red) y deshabilitando el TCP/IP *forwarding*. De esta manera los computadores de la red privada se pueden comunicar con el *gateway* así como los de la Internet también, pero el tráfico directo entre las redes no es posible. La siguiente gráfica muestra como es el esquema más comun para implementaciones a través de *Dual Homed Gateway* o *Dual Homed Host*, como se puede ver, por definición un *Dual Homed Gateway* es un *Bastion Host*.

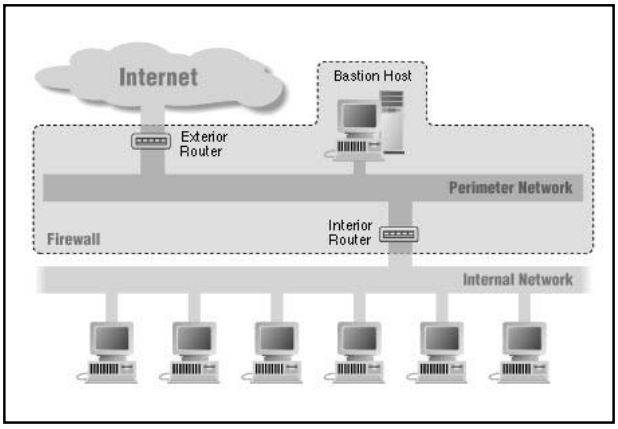


Screened Host Gateway: Es quizás la configuración más común de firewall, es implementada usando un *Bastion Host* y un *Screening router*. Usualmente el *Bastion Host* está ubicado en la red privada y el *Screening router* está configurado de tal forma que el *Bastion Host* es el único sistema en la red privada que se puede alcanzar desde Internet. A menudo el *Screening router* es configurado para evitar tráfico hacia el *Bastion Host* en puertos específicos permitiendo a un número reducido de servicios comunicarse con él.

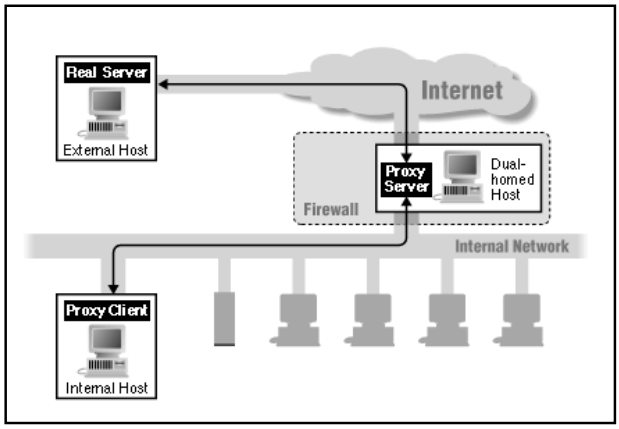
La siguiente gráfica muestra un esquema típico del Screened Host Gateway.



Screened Subnet: En algunas implementaciones para *firewalls* se crea una subred aparte situada entre la Internet y la red privada. Típicamente esta red es aislada usando *Screening router*, lo cual permite implantar niveles de filtramiento de paquetes variable. Generalmente una *Screened Subnet* es configurada de tal forma que tanto las máquinas de la red privada y de la Internet tienen acceso a los que componen esta subred *(Screened Subnet)*, pero el tráfico através de la *Screened Subnet* no es permitido. La figura muestra el esquema típico para este tipo de implementación.



Application Level Gateway: También conocido como *Proxy Gateway*. Son reflectores o "Proveedores" de servicios específicos los cuales operan la mayoría de las veces a nivel de aplicación de usuarios más que a nivel de protocolo. Generalmente estos servicios de "reflexión o pasada" cuando están ejecutándose en un *firewall* son puntos importantes para la totalidad de la seguridad de la red. Los servicios *proxy* son más o menos transparentes entre los usuarios de la red interna y un servicio de la red externa, en vez de "hablar" directamente cada uno "habla" a un *proxy*. Para el usuario, un servidor proxy presenta la ilusión de que el contacto ha sido hecho directamente con el servidor remoto. La configuración típica se muestra a continuación:



En general no podemos hablar de cuál método es el mejor ya que existen muchos factores para determinar cuál es el mejor *firewall* para una situación específica, entre otros, los factores más influyentes son: costos, política corporativa de seguridad, tecnologías de red existentes, políticas al interior de la organización; todos estos pueden prevalecer sobre la consideración técnica justificada para adoptar una plataforma de firewall concreta.

REFERENCIAS

Garfinkel, Simson y Spafford, Gene. 1996. Practical Unix & Internet Security. 2nd Edition. USA: O'Reilly & Associates Inc.

Siyan, Karanjit. 1995. Internet y seguridad en redes. 1ª Edición. México. New Riders Publishing.

Chapman D., Brent y Zwicky, Elizabeth. 1995. Building Internet Firewalls. 1ª Edición. USA. O'Reilly & Associates Inc.

Ranum, Marcus. "Thinking About Firewalls". Disponible vía FTP en: ftp://coast.cs.purdue.edu/pub/doc/firewalls/Marcus_Ranum_Network_Firewall.ps.Z.

Housley, Ford, Polk y Solo. 1996. Internet Public Key Infrastructure. PKIX Working Group, Internet Draft.

Ford, Warwick. 1995. Computer Communications Security. 1ª Edición. New Jersey. Prentice Hall.

"How to Develop a Network Security Policy" disponible vía Internet en: http://www.sun.com/solstice/Networking - products/neT worksec.html.

Giraldo G., Jorge Alberto. 1996. Curso de Seguridad en Sistemas Abiertos. Bogotá. J

Morant R. José Luis y otros. 1994. Seguridad y protección de la información. 1ª Edición. Madrid. Editorial Centro de Estudios Ramón Aceres.