UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA ELÉCTRICA

IMPLANTACIÓN DE UNA PLATAFORMA DE SEGURIDAD PARA EL ACCESO A INTERNET DE UNA EMPRESA DEDICADA AL RAMO LEGAL

Trabajo de Grado presentado a la ilustre Universidad Central de Venezuela para optar al título de Especialista en Comunicaciones y Redes de Comunicación de Datos

Presentado por:

Ing. Tammy Hernández Conde

Tutor Académico:

Prof. Vincenzo Mendillo

Caracas, Octubre de 2004

AGRADECIMIENTO

A Dios, quien depositó en mi corazón la fortaleza, la luz y el amor para poder seguir adelante; y por permitir aquellas adversidades que cruzaron mi camino porque me enseñaron tolerancia, perseverancia, autocontrol y algunas otras virtudes que nunca habría conocido.

A mi madre, por su empeño en que yo siguiera estudiando.

A todos mis amigos y profesores con los que compartí momentos y experiencias muy agradables en tan prestigiosa universidad.

A todas aquellas personas que me apoyaron y me asesoraron en la implantación de este proyecto.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

Capítulo II: Marco Teórico

Capítulo III: Sistema Actual

Capítulo IV: Sistema Propuesto

ÍNDICE DE CUADROS

Capítulo IV: Sistema Propuesto

ÍNDICE DE ANEXOS

UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA ELÉCTRICA

POSTGRADO EN ESPECIALIZACIÓN EN COMUNICACIONES Y REDES DE COMUNICACIÓN DE DATOS

IMPLANTACIÓN DE UNA PLATAFORMA DE SEGURIDAD PARA EL ACCESO A INTERNET DE UNA EMPRESA DEDICADA AL RAMO LEGAL

Autor: Ing. Tammy Hernández Conde **Tutor**: Prof. Vicenzo Mendillo

Octubre de 2004

RESUMEN

El presente Trabajo Especial de Grado tiene como objetivo implantar una plataforma de seguridad para el acceso a Internet de una empresa dedicada al ramo legal, con la finalidad de garantizar la integridad y confiabilidad de la información confidencial, así como la disponibilidad de los recursos y servicios de la red, permitiendo aumentar la calidad de los procedimientos relacionados con el área de negocios. Dicha empresa actualmente cuenta con servicios y aplicaciones que requieren de un sistema más sofisticado para el acceso a Internet, que pueda brindar confiabilidad, escalabilidad, rendimiento y una mayor seguridad para cubrir las demandas de protección de toda la plataforma tecnológica existente. Para alcanzar el objetivo se realizó un estudio y análisis del sistema de seguridad, lo cual permitió evaluar opciones que conllevaron a reforzar la seguridad del acceso a Internet, mejorando y brindando una mayor protección a toda la infraestructura informática. El diseño del sistema propuesto se implantó satisfactoriamente, solventando así las vulnerabilidades existentes mediante mecanismos de seguridad tanto técnicos como administrativos disponibles a través de la tecnología basada en firewall, obteniendo los resultados esperados y cubriendo así los requerimientos de la organización.

INTRODUCCIÓN

La seguridad en Internet ha llegado a ser una prioridad en las organizaciones debido al aumento de los incidentes relacionados con la misma en los últimos años. Según va creciendo la penetración de Internet, se está creando un mundo más interdependiente y los problemas relacionados con la seguridad aumentan.

La aparición de las redes globales de comunicación se ha convertido en uno de los eventos más importantes de la historia reciente. Las organizaciones y los individuos han establecido complejos procesos, de muy diversa índole, que utilizan a Internet como elemento primordial en su operación; las empresas realizan transacciones comerciales con clientes y proveedores a través de la red, los individuos compran y efectúan transacciones bancarias en sitios Web, entre muchas otras acividades. Cuanto más trascendentes son estos procesos en la vida de las organizaciones, más importante es la necesidad de que "la red de redes" cuente con altos niveles de seguridad, disponibilidad y confiabilidad.

Desafortunadamente, a lo largo de los años se han conocido casos en que importantes empresas y organizaciones han visto comprometidas sus operaciones debido a que han sufrido ataques perpetrados a través de redes globales como Internet. En 1990, el sistema de conmutación de llamadas de larga distancia de AT&T fue puesto fuera de servicio durante nueve horas, dando como resultado que más de 70 millones de llamadas no fueran completadas. En 1994, dos crackers ingleses penetraron y robaron información en varios sitios militares estadounidenses, entre ellos los Rome Labs de la Fuerza Aérea. En 1997, un solo cracker obtuvo y trató de vender información sobre más de 100,000 tarjetas de crédito obtenida ilegalmente de varias compañías que realizan negocios en la Web. En el año 2000, el sitio Web de la compañía Yahoo, el más visitado en el mundo, estuvo fuera de servicio durante varias horas debido a un ataque distribuido de negación de servicio perpetrado por un clan de crackers. En

mayo de 2001, el sitio Web promocionado como “más seguro” de la Unión Europea (http://www.saferinternet.org) fue penetrado y la página principal fue sustituida por otra que alardeaba sobre el éxito del ataque. En muchos de estos casos el costo de la reparación de los daños causados se elevó a varios miles de dólares.

Muchas empresas venezolanas no han sido la excepción al sufrir constantes ataques por parte de estos crakers, generándoles pérdidas cuantiosas que se ven reflejadas en los daños ocasionados a programas y archivos y en la violación de información confidencial, impactando negativamente en la productividad y generando graves consecuencias con la caída de los sistemas, transmitiendo desconfianza por parte de los clientes que llevarían a involucrar a las empresas en problemas de orden legal. Esto ha llevado a la necesidad de tomar decisiones más firmes con respecto a la seguridad y realizar las inversiones necesarias para proteger los activos de información.

El presente Trabajo Especial de Grado representa una solución para la empresa bajo estudio y consiste en la implantación de una plataforma de seguridad para el acceso a Internet. Dicha empresa cuenta actualmente con servicios y aplicaciones que requieren de un sofisticado sistema que permita un acceso seguro a Internet y que a su vez pueda brindar confiabilidad, escalabilidad, rendimiento y una mayor seguridad para cubrir las demandas de protección de toda su plataforma tecnológica.

CAPÍTULO I
EL PROBLEMA

I.1.- Planteamiento del Problema

La empresa en estudio se fundó en Venezuela y lleva más de tres décadas dedicándose al sector jurídico, cubriendo las diversa áreas de especialización: Administrativa, Constitucional, Asesoría Tributaria, Corporativa, Económico Regulatorio, Propiedad Intelectual, laboral y seguridad social, entre otras. Su sede se encuentra ubicada en Caracas y está conformada por amplias oficinas con una avanzada estructura tecnológica que permite una atención directa y personalizada a sus clientes.

Sus oficinas cuentan con una red de área local (LAN) conformada por servidores de última generación que operan bajo el Sistema Operativo MS Windows 2000 Server y con las aplicaciones de MS SQL Server 2000, MS ISA Server 2000, MS Exchange 2000 Server y otras herramientas corporativas y administrativas. Estos servidores se encuentran ubicados en un área especial dentro de sus instalaciones, contando con los requerimientos necesarios para su seguridad. En dicha área se encuentra ubicado un rack que contiene un conjunto de switches 3COM interconectados que operan a 100 Mbps, con un backbone de fibra óptica. Esta infraestructura utiliza como protocolo de comunicación la suite TCP/IP para el transporte de datos.

La conexión a Internet se realiza a través de un enlace Frame Relay con una velocidad de transmisión de datos de 512 Kbps, suministrada por CANTV. El acceso a Internet y la administración de seguridad la lleva a cabo la aplicación MS ISA Server 2000 que está instalada en modo integrado firewall/caché. Su función principal es proteger la integridad de la red de cualquier ataque informático proveniente del exterior y ofrecer un ambiente seguro a la organización. Además

permite controlar el acceso a Internet y las páginas que visitan todos los usuarios de la red. También protege la red de accesos indebidos y filtra mensajes no solicitados.

El ISA Server actualmente publica los servidores y equipos que se encuentran en la red privada para que puedan ser accesados desde la red pública de Internet. Este tipo de configuración presenta la debilidad de que los servidores públicos que deben ser accesados desde Internet se encuentran físicamente conectados en la red privada y esto puede representar una posible brecha de vulnerabilidad para conectarse y dañar otros equipos dentro de la LAN violando la confidencialidad de la información

A causa de la necesidad de implementar nuevos servicios en la red privada de datos de la organización y el acceso remoto de forma segura utilizando la red pública Internet, así como la necesidad de aumentar la seguridad de la red privada retirando los equipos y servidores públicos de la misma, se decidió llevar a cabo el proyecto de una plataforma de seguridad para el acceso a Internet con los siguientes requerimientos:

- Proveer seguridad a los recursos informáticos de la red privada de la empresa bajo estudio.
- El sistema de seguridad debe tener alta disponibilidad, lo que conlleva a que debe existir una redundancia del mismo en la plataforma.
- La solución a implementar debe soportar todos los servicios que actualmente no son procesados por el sistema de seguridad.
- Debe preverse la posibilidad de instalar nuevas tecnologías o expandir ante nuevas necesidades, tomando en cuenta las aplicaciones y los servicios que están en proyecto actualmente en la Gerencia de Sistemas.
- La administración de la plataforma debe ser sencilla, amigable y contar con una interfaz gráfica de usuario basada en Web, con ayuda en línea, de manera que se pueda simplificar su administración.

- Debe contar con un puerto DMZ para así crear un área de información protegida desmilitarizada en la red, a fin de que los usuarios externos puedan ingresar a esta área, pero no puedan acceder al resto de la red.
- La solución debe contar con alta disponibilidad de manera de garantizar la continuidad del acceso a los servicios, aplicaciones en línea y la operatividad segura de la red privada.
- Adicionalmente debe soportar conexiones VPN para una conectividad privada virtual basada en IPSec que permita un acceso remoto seguro.

I.2.- Objetivo General

Implementar una plataforma de seguridad para el acceso a Internet en la empresa bajo estudio, con la finalidad de garantizar la integridad de la información confidencial y la disponibilidad de los recursos y servicios de la red, brindando confiabilidad, escalabilidad y rendimiento, logrando así cubrir las demandas de protección en su infraestructura tecnológica.

I.3.- Objetivos Específicos

- Análisis y estudio de la configuración actual del sistema de seguridad de la empresa.
- Evaluación de los posibles problemas de seguridad y de vulnerabilidad en la información de la red privada con el fin de identificar los requerimientos funcionales y operativos del sistema.
- Estudio de las diferentes tecnologías de seguridad existentes para redes privadas con respecto al acceso a Internet.

- Estudio y comparación de las distintas tecnologías de firewall que pueden ser aplicadas como solución al proyecto.
- Estudio y análisis de políticas de seguridad a implementar en el firewall.
- Estudio costo beneficio de los diferentes equipos firewall disponibles en el mercado.
- Selección y compra del equipo firewall ha ser instalado como sistema de seguridad para el acceso a Internet de la empresa.
- Instalación, configuración e implantación de la solución propuesta.
- Realizar pruebas de vulnerabilidad del equipo instalado.
- Documentación del proyecto e inducción del personal encargado de administrar el equipo en la empresa.

I.4.- Justificación

La empresa en estudio está dedicada al sector jurídico y gran parte del negocio se sustenta con el intercambio y consulta de información, por ende los servicios de correo e Internet resultan indispensables para una operación eficiente. Los profesionales del derecho viajan frecuentemente para atender requerimientos de clientes que se encuentran tanto en Venezuela como en el exterior, lo que conlleva que los servicios que prestan los servidores de la empresa deben estar operativos las 24 horas del día y los 365 días del año, permitiendo la disponibilidad de la información en línea y poder así garantizar mayor eficiencia en la toma de decisiones. De aquí la importancia de la continuidad y disponibilidad de un acceso seguro a Internet y demás servicios, logrando así aumentar la calidad y la productividad de los procedimientos implicados en el área de negocios de la empresa.

CAPÍTULO II
MARCO TEÓRICO

II.1.- La Seguridad en Internet y la Seguridad Informática

El fenómeno de la extensión de Internet ha adquirido una velocidad tan rápida y unas proporciones, que el panorama actual y muchos de los efectos que se dan en su seno resultan sorprendentes y difícilmente imaginables hace sólo una década.

Inicialmente Internet nació como una serie de redes para promover el intercambio de información entre investigadores que colaboraban en proyectos conjuntos o compartían resultados usando los recursos de la red. En esta etapa inicial, la información circulaba libremente y no existía una preocupación por la privacidad de los datos ni por ninguna otra problemática de seguridad. Estaba totalmente desaconsejado usarla para el envío de documentos confidenciales o clasificados que pudieran manejar los usuarios, situación muy común, pues hay que recordar que Internet nació como parte de un contrato del Departamento de Defensa Americano para conectar entre sí, tanto las universidades como los centros de investigación que colaboraban de una manera u otra con las Fuerzas Armadas Norteamericanas.

Los protocolos de Internet fueron diseñados de una forma deliberada para que fueran simples y sencillos. El poco esfuerzo necesario para su desarrollo y verificación jugó eficazmente a favor de su implantación generalizada, pero tanto las aplicaciones como los niveles de transporte carecían de mecanismos de seguridad que no tardaron en ser echados en falta.

Más recientemente, la conexión a Internet del mundo empresarial se ha producido a un ritmo vertiginoso muy superior a la difusión de ninguna otra tecnología anteriormente ideada. Ello ha significado que esta red de redes se haya convertido en

"La Red" por excelencia. Esto es, el medio más popular de interconexión de recursos informáticos y embrión de las anunciadas autopistas de la información.

Se ha incrementado la variedad y cantidad de usuarios que usan la red para fines tan diversos como el aprendizaje, la docencia, la investigación, la búsqueda de socios o mercados, la práctica política o, simplemente, el juego. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados.

Podemos ver que las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones. La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios.

También la propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. En medio de esta variedad, han ido aumentando las acciones mal intencionadas contra la privacidad y la propiedad de recursos y sistemas. Las palabras “hacker” y “craker”, entre otras, han hecho aparición en el vocabulario común de los usuarios y de los administradores de las redes.

Es importante entonces tomar medidas concretas de seguridad, pero independientemente de las técnicas y herramientas que se utilicen, hay que recalcar que un componente muy significativo para la protección de las redes informáticas consiste en la atención y vigilancia continua y sistemática por parte de los responsables de la red.

II.1.1.- Concepto de Seguridad

Es mantener la provisión de información libre de riesgo y brindar servicios para un determinado fin. Es tener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

II.1.2.- Objetivo de la Seguridad

El objetivo de la seguridad en la informática es mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información manejada por las computadoras así como todos los recursos informáticos involucrados en el ámbito.

II.1.3.- Aspectos en la Seguridad Informática

Existe información que debe o puede ser pública, siendo esta aquella que puede ser visualizada por cualquier persona, y aquella que debe ser privada, la que sólo puede ser visualizada por un grupo selecto de personas que trabaja con ella. En esta última se debe maximizar el esfuerzo para preservarla de ese modo, reconociendo las siguientes características en la información:

- *Crítica:* Es indispensable para garantizar la continuidad operativa.
- *Valiosa:* Es un activo con valor en sí misma.
- *Confidencial:* Debe ser conocida por las personas que la procesan y sólo por ellas.

La *integridad* de la información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de

integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

La *disponibilidad* u *operatividad* de la Información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

La *privacidad* o *confidencialidad* de la información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la información puede provocar severos daños a su dueño (por ejemplo conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se "filtran" a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes).

El *control* sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuando y como permitir el acceso a la misma.

La *autenticidad* permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

Adicionalmente pueden considerarse algunos aspectos adicionales, relacionados con los anteriores, pero que incorporan algunos aspectos particulares:

Protección contra la réplica: mediante la cual se asegura que una transacción sólo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.

No repudio: mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.

Consistencia: se debe poder asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.

Aislamiento: este aspecto, íntimamente relacionado con la confidencialidad, permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.

Auditoría: es la capacidad de determinar qué acciones o procesos se están llevando a cabo en el sistema, así como quién y cuando las realiza.

Cabe definir *amenaza*, en el entorno informático, como cualquier elemento que comprometa al sistema. Las amenazas pueden ser analizadas en tres momentos: antes del ataque durante y después del mismo. Estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema informático.

- *Prevención (antes):* mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo el cifrado de información para su posterior transmisión.

- *Detección (durante):* mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.
- *Recuperación (después):* mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionamiento normal. Por ejemplo recuperación desde las copias de seguridad (backup) realizadas.

II.1.3.1.- La Seguridad Física

Es muy importante ser consciente que por más que una empresa sea la más segura desde el punto de vista de ataques externos, hackers, virus, etc., la seguridad de la misma será nula si no se ha previsto, por ejemplo, como combatir un incendio.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos aspectos se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de operaciones de la misma, no. Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía red a la misma.

Así, la seguridad física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

II.1.3.2.- La Seguridad Lógica

La seguridad lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y a las aplicaciones, permitiéndolo sólo a las personas debidamennte autorizadas.

Alguien una vez dijo referente a la seguridad informática “todo lo que no está permitido debe estar prohibido” y esto es lo que debe asegurar la seguridad lógica. Los objetivos que persigue la seguridad lógica son los siguientes:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

II.1.4.- Políticas de Seguridad Informática

Las Políticas de Seguridad Informática (PSI) surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos que

permiten a la compañía desarrollarse y mantenerse en su sector de negocios. Las políticas de seguridad informática fijan los mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen. Estas políticas deben diseñarse a la medida para así recoger las características propias de cada organización.

Las políticas de seguridad conforman el conjunto de lineamientos que una organización debe seguir para asegurar la confiabilidad de sus sistemas. Por lo tanto, son parte del engranaje del sistema de seguridad que la organización posee para salvaguardar sus activos.

Las PSI constituyen las alarmas y compromisos compartidos en la organización, que le permiten actuar proactivamente ante situaciones que comprometan su integridad. Por lo cual, deben constituir un proceso continuo y retroalimentado que observe la concientización, métodos de acceso a la información, monitoreo de cumplimiento y renovación, aceptación de las directrices y estrategia de implantación, que lleven a una formulación de directivas institucionales que logren aceptación general.

Las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

II.1.4.1.- Elementos de una Política de Seguridad Informática

Como se comentó anteriormente, una PSI debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere una disposición de cada uno de los

miembros de la gerencia de informática de la empresa para lograr una visión conjunta de lo que se considera importante.

Las PSI deben considerar entre otros, los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos para configuración de la seguridad de los sistemas que cobija el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que él o ella tiene acceso.

Las PSI deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones, transmitir por qué son importantes éstos u otros recursos o servicios. De igual forma, las PSI establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la compañía. Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa. Por otro lado, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el alcance de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer.

De acuerdo con lo anterior, el implementar políticas de seguridad requiere un alto compromiso con la organización, agudeza, destreza y experiencia técnica para detectar fallas y debilidades, y constancia para renovar y actualizar dichas políticas en función del dinámico ambiente que rodea las organizaciones modernas.

II.2.- El Firewall ó Cortafuego

Con el auge de Internet y de las redes corporativas o intranets, los firewalls han pasado a ser una herramienta fundamental para garantizar la seguridad en las redes basadas en protocolos IP. El firewall pasa a ser un elemento imprescindible cuando la red corporativa se interconecta con otras redes de terceros o con redes públicas como Internet.

Un firewall es un sistema que permite ejercer políticas de control de acceso entre dos redes, tales como una red LAN privada e Internet, una red pública y vulnerable. El firewall define los servicios que pueden accederse desde el exterior y viceversa. Los medios a través de los cuales se logra esta función varían notoriamente, pero en principio, un firewall puede considerarse como: un mecanismo para bloquear el tráfico y otro para permitirlo.

Un firewall constituye más que una puerta cerrada con llave al frente de una red. Es un servicio de seguridad particular. Los firewalls son también importantes porque proporcionan un único punto de restricción, donde se pueden aplicar políticas de seguridad y auditoria. Un firewall proporciona al administrador de la red, entre otros datos, información acerca del tipo y cantidad de tráfico que ha fluido a través del mismo y cuántas veces se ha intentado violar la seguridad. De manera similar a un sistema de circuito cerrado de TV, un firewall no sólo bloquea el acceso, sino también monitorea a aquellos que están merodeando y le ayuda a identificar los usuarios que han intentado violar su seguridad.

II.2.1.- Funciones Básicas de un Firewall

Un firewall lleva a cabo tres funciones básicas para proteger una red:

- Bloquea los datos entrantes que pueden contener el ataque de un hacker.
- Oculta la información acerca de la red, haciendo que todo parezca como si el tráfico de salida se originara del firewall y no de la red. Esto también se conoce como NAT (*Network Address Translation*).
- Filtra el tráfico de salida, con el fin de restringir el uso de Internet y el acceso a localidades remotas.

En la siguiente figura se puede observar gráficamente la función de bloqueo de los ataques de un hacker.

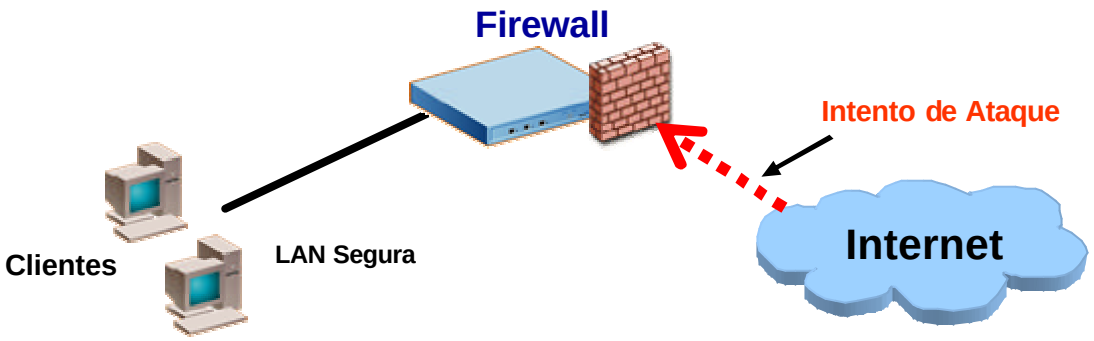


Figura II.1: Bloqueo de ataques externos

En la siguiente figura se puede observar también como el firewall restringe el acceso a Internet a los usuarios internos que no poseen tal derecho en la empresa, según la política de acceso establecida.

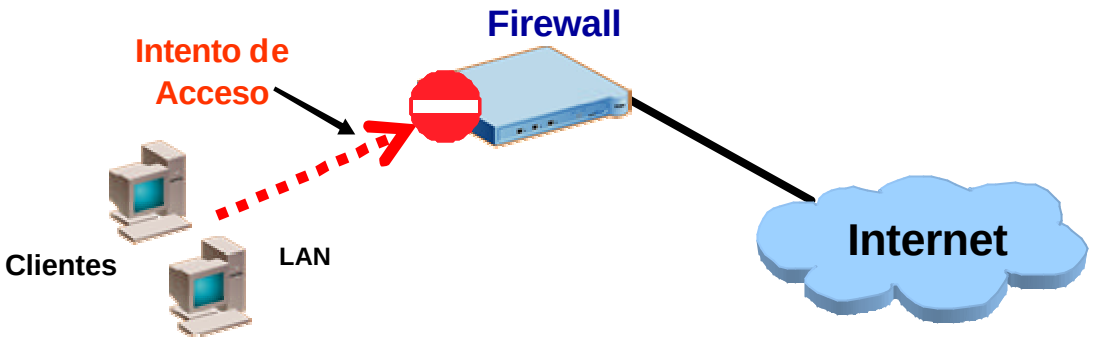


Figura II.2: Bloqueo de acceso a Internet a usuarios internos

II.2.1.1. - Niveles de Filtrado

Un firewall puede filtrar tanto el tráfico que sale como el que entra. Debido a que el tráfico que entra constituye una amenaza mucho mayor para la red, éste es inspeccionado mucho más estrictamente que el tráfico que sale. Existen básicamente tres tipos de filtrado:

- El filtrado que bloquea cualquier dato de entrada que no haya sido específicamente solicitado por un usuario de la red.
- El filtrado basado en la dirección del remitente.
- El filtrado basado en el contenido de la comunicación.

Los niveles de filtrado se pueden comparar con un proceso de eliminación. El firewall inicialmente determina si la transmisión entrante ha sido solicitada por un usuario de la red y, de no ser así, la rechaza. Luego, cualquier dato que haya sido permitido se inspecciona cuidadosamente. El firewall verifica la dirección de la computadora del

remitente, con el fin de certificar que proviene de un sitio confiable. Finalmente, se encarga de verificar el contenido de la transmisión.

II.2.1.2.- Tipos de Ataque

Antes de definir exactamente qué tipo de firewall se debe implementar, es importante entender la naturaleza de los tipos de amenazas de seguridad que existen. Internet es una extensa comunidad, y como tal, existen sujetos buenos y malos. Los sujetos malos abarcan desde individuos incompetentes que provocan daños sin intención, hasta "hackers" habilidosos y maliciosos que planean ataques deliberados a las empresas, utilizando Internet como su arma preferida. Por lo general, existen tres tipos de ataques que pueden potencialmente impactar en forma negativa a una empresa:

- Hurto de información: Robo de información confidencial, tales como registros de clientes y empleados, o hurto de propiedad intelectual de su empresa.
- Sabotaje de información: Cambios a la información, en un intento de dañar la reputación de una persona o empresa. Como por ejemplo, elaborando cambios a los registros educativos y médicos de los empleados o publicando contenido malintencionado en su sitio Web.
- Negación de servicio (DoS: *Denial of Service*): Bloqueo de los servidores o red de su empresa, de forma que los usuarios legítimos no puedan acceder a la información o para impedir la operación normal de su empresa.

Acceso forzado a redes privadas para hurtar o sabotear información

Un "hacker" puede intentar obtener acceso a una red por diversión o ambición. Un intento de lograr acceso, por lo general, comienza con la recolección de información acerca de la red. Luego, esta información se utiliza para realizar un ataque con un propósito específico, ya sea para apoderarse o destruir datos. Un "hacker" puede usar

un scanner de puertos, un software que permite ver la estructura de la red. Esto les permite averiguar cómo está estructurada la red y qué software se está ejecutando en la misma. Una vez que el "hacker" tiene una idea de la estructura de la red, puede aprovecharse de todas las debilidades conocidas del software y utilizar las herramientas de "hacking" para ocasionar estragos en su ambiente de tecnología de información.

Es posible, inclusive, ingresar a los archivos de los administradores y dejar en blanco los discos, aunque una buena clave de acceso por lo general puede dificultar esta tarea. Afortunadamente, un buen firewall es inmune a un escaneo de puertos y, a medida que se desarrollan nuevos scanners de puertos para evadir esta inmunidad, los fabricantes de firewall producen actualizaciones para preservarla.

Ataques de negación de servicio (DoS: Denial of Service)

Los ataques DoS son puramente maliciosos. No producen ningún beneficio para el "hacker", mas que el placer de que las redes, o parte de ellas, queden inaccesibles para sus usuarios. Un ataque DoS sobrecarga el sistema de manera que lo deja inhabilitado, negando así la posibilidad de utilizar los servicios de la red. Los "hackers" envían grandes paquetes de datos o programas que requieren que el sistema responda continuamente a comandos falsos. Para llevar a cabo un ataque DoS, un "hacker" tiene que conocer la dirección IP del sistema que va a atacar, pero un buen firewall no revela su propia dirección IP o las direcciones IP de la red. El "hacker" puede pensar que se ha comunicado con la red, cuando en realidad sólo se ha contactado con el firewall y, desde ese punto, no es posible bloquear la red. Así mismo, cuando un "hacker" lanza un ataque, algunos firewalls pueden identificar los datos como tal, rechazar los datos, alertar al administrador del sistema y realizar un seguimiento del origen de los datos, para capturar al individuo que los envió.

II.2.2.- Tecnologías de Firewall

Para seleccionar un firewall correcto, se debe tomar en cuenta los requerimientos de la empresa y el tamaño de la red. A continuación se resumen los diferentes tipos y tecnologías de firewall y los formatos disponibles en el mercado. Lo esencial es que, independientemente del tipo de firewall o funcionalidad que se escoja, la persona debe asegurarse de que se trata de una solución segura y de que ha sido certificada por una organización confiable, como por ejemplo, la Asociación Internacional de Seguridad de Computadoras (ICSA). ICSA clasifica los firewalls en tres categorías:

- Firewalls de Filtrado de Paquetes.
- Servidores Proxy de Nivel de Aplicación.
- Firewalls de Inspección de Paquetes (SPI: *Stateful Packet Inspection*).

II.2.2.1.- Firewall con Filtrado de Paquetes (Nivel de Red)

Es el firewall más sencillo, de la primera generación, y se basa en permitir o autorizar el tráfico basado en el encabezado de cada paquete. Como no guarda los estados de una conexión, no tiene el concepto de una sesión.

Cada computadora de una red tiene una dirección comúnmente llamada dirección IP. Un firewall con filtrado de paquetes verifica la dirección de donde proviene el tráfico entrante y rechaza cualquier tráfico que no coincida con la lista de las direcciones confiables. El firewall con filtrado de paquetes utiliza reglas para negar el acceso, según la información contenida en el paquete, como por ejemplo: el número del puerto TCP/IP, la dirección IP de la fuente/origen o el tipo de datos. Las restricciones pueden ser tan estrictas o tan flexibles como uno requiera. Un router común de una red puede filtrar el tráfico por dirección, pero los “hackers” tienen un pequeño truco llamado “spoofing” de IP, con el cual los datos parecen provenir de una fuente

confiable o incluso de una dirección de su propia red. Desafortunadamente, el firewall de filtrado de paquetes es propenso al “spoofing” de IP y son muy difíciles de configurar. Cualquier error en su configuración, puede dejarlo vulnerable a los ataques. Como desventajas se destaca lo siguiente: no ofrece autenticación, vulnerable a ataques como spoofing (cambio de dirección del remitente) y difícil de administrar en ambientes complejos.

Para comprender mejor el filtrado de paquetes cabe mencionar lo siguiente: El sistema de filtrado de paquetes enruta paquetes entre host internos y externos, pero de manera selectiva. Permite bloquear cierto tipo de paquetes de acuerdo con la política de seguridad de la red. El tipo de enrutamiento usado para filtrar paquetes en un firewall es conocido como "screening router". El filtrado también se conoce como *screening* y a los dispositivos que lo implementan se les denomina *choke*; el choke puede ser la máquina bastión (también se denominan *gates*) o un elemento diferente.

Se puede selectivamente enrutar paquetes desde o hacia su sitio:

- Bloquear todas las conexiones que entran desde sistemas externos, excepto las conexiones SMTP (solo recibirá correos).
- Bloquear todas las conexiones que provienen de un determinado lugar que se considera peligroso.
- Permitir servicio de mail y FTP, pero bloqueando servicios peligrosos como TFTP, RPC, servicios "r" (rlogin, rsh, etc).

Para entender cómo se filtra un paquete, se necesita conocer la diferencia entre enrutamiento ordinario y screening router. El primeroo simplemente mira la dirección destino de cada paquete y elige el mejor camino que el conoce hacia la dirección destino. La decisión sobre cómo atender el paquete se basa solamente en el destino del paquete. En screening router, en cambio, mira el paquete más detalladamente. Además de determinar si el paquete puede ser enrutado o no a la dirección destino,

determina si debe o no debe ser enrutado de acuerdo a la política de seguridad. La comunicación entre la red interna y externa tiene una enorme responsabilidad. Realizar el enrutamiento y la decisión de enrutar es la única protección al sistema. Si la seguridad falla, la red interna está expuesta. Un screening router puede permitir o rechazar un servicio, pero no puede proteger operaciones individuales dentro del servicio. Casi todos los dispositivos actuales de filtrado de paquetes (enrutadores de selección o compuertas de filtro de paquetes) operan de la siguiente forma:

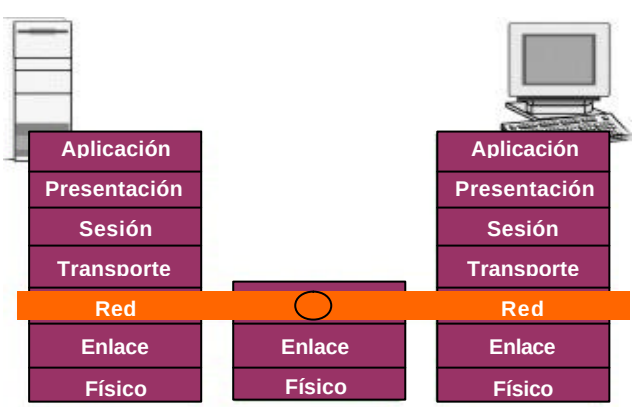
1. El criterio de filtro de paquete debe almacenarse para los puertos del dispositivo usado como filtro de paquetes. El criterio de filtro de paquetes se conoce como reglas del filtro.
2. Cuando un paquete llega al puerto, los encabezados de los paquetes se analizan, por ejemplo los encabezados IP, TCP o UDP.
3. Las reglas del filtro de paquete se almacenan en un orden específico. Cada regla se aplica al paquete en el mismo orden en que la regla del filtro de paquetes se almacenó.
4. Si una regla bloquea la transmisión o recepción del paquete, el paquete no se acepta.
5. Si una regla permite la transmisión o recepción de un paquete, el paquete sigue su camino.
6. Si un paquete no satisface ninguna regla, es bloqueado. Es decir aquello que no esté expresamente permitido, se prohíbe.

Es importante colocar las reglas en orden correcto. Si dichas reglas se colocan en un orden equivocado, podría terminar negando servicios válidos, mientras que permitiría los servicios que desea negar.

A continuación un resumen de la tecnología descrita arriba.

Tecnología Firewall con Filtrado de Paquetes (Nivel de Red)

- Tecnología de firewall de primera generación
- Opera sólo a nivel de red
- Usa reglas para *Permitir* o *Negar* acceso de acuerdo a las direcciones IP
  - Chequea las direcciones de tráfico contra una lista aprobada de direcciones
- La implementación más común es en la forma de listas de acceso en un router "simple".



✓
- Independencia de la aplicación
- Alto desempeño
- Transparente para el usuario final

✗
- Tiene la seguridad más baja; susceptible a IP Spoofing
- Difícil, consume tiempo para configurar

Figura II.3: Tecnología firewall con filtrado de paquetes

II.2.2.2.- Servidor Proxy a Nivel de Aplicación

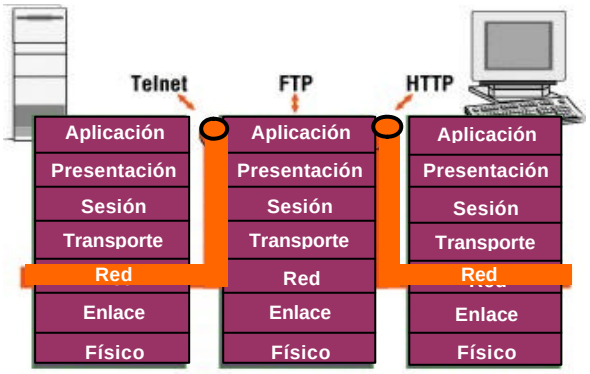
Los firewalls a nivel de aplicación por lo general son hosts corriendo proxy servers, que no permiten el tráfico directo entre redes, realizando una elaborada auditoria y logeo del tráfico que pasa a través de él. Este tipo de firewall puede ser utilizado para realizar las tareas relativas al NAT, debido a que como las comunicaciones van de un lado hacia el otro, se puede esconder la ubicación original. Este tipo tiende a proveer una auditoria más detallada y un mayor grado de seguridad que los de nivel de red.

Un proxy a nivel de aplicación conoce la aplicación o servicio específico para el cual está proporcionando los servicios de proxy, es decir, comprende e interpreta los

comandos en el protocolo de aplicación. Este tipo de firewall examina la aplicación usada por cada paquete IP, con el fin de verificar su autenticidad. El tráfico de cada aplicación, tales como HTTP para la Web, FTP para la transferencia de archivos y SMTP/POP3 para e-mail. Por lo general, requieren de la instalación y configuración de un proxy de aplicaciones diferente. Con frecuencia, los servidores requieren que los administradores reconfiguren su red y aplicaciones (por ejemplo los navegadores de Web) para soportar el proxy, lo cual puede resultar en un proceso muy trabajoso. A continuación un resumen de esta tecnología.

Tecnología Servidor Proxy a Nivel de Aplicación

- Tecnología de firewall de segunda generación
- Examina el nivel de Aplicación en el paquete IP así como la dirección IP
  - Verifica la autenticidad de cada paquete
  - Realiza logging extensos y hace auditoria del tráfico
- No permite tráfico directo entre redes



✓
- Buena seguridad
- Vigilancia completa del nivel de Aplicación

✗
- Desempeño muy pobre
- Soporte limitado para las aplicaciones y proceso trabajoso para configurar

Figura II.4: Tecnología firewall – Servidor proxy a nivel de aplicación

II.2.2.3.- Firewall de Inspección de Paquetes (SPI: Stateful Packet Inspection)

Constituye la última generación en la tecnología de firewall. Los expertos en Internet consideran que SPI es la tecnología más avanzada y segura, gracias a que examina todos los componentes de un paquete IP para decidir si acepta o rechaza la comunicación. El firewall mantiene un registro de todas las solicitudes de información que se originan de la red. Luego, inspecciona toda comunicación entrante para verificar si realmente fue solicitada y rechaza cualquiera que no lo haya sido. Los datos solicitados aprobados proceden al siguiente nivel de inspección y el software determina el estado de cada paquete de datos.

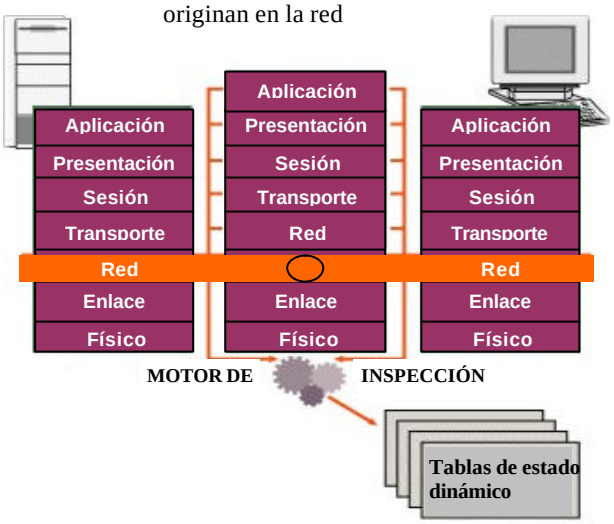
El stateful firewall es un firewall que provee de herramientas como el seguimiento y control del flujo de una sesión de datos dentro y fuera de la red. La información concerniente a cada conexión es almacenada en memoria. Cuando un paquete cruza el filtro, la decisión de desechar o enviar es realizada usando la información de conexión almacenada en memoria (por ejemplo, dirección del destino, número de puerto, información de la secuencia TCP y banderas adicionales).

Una ventaja de un SPI es que en lugar de abrir puertos de red permanentemente para ciertos protocolos que solicitan puertos arbitrarios, sólo abrirá estos puertos durante el tiempo suficiente para que el paquete pase. Esto disminuye drásticamente la oportunidad de un cracker para introducir código destructivo a la red. Además permite definir un límite de tasa de conexión para defenderse contra ataques de negación de servicio (DoS), tal como la inundación de paquetes SYN.

A continuación un resumen de la tecnología descrita anteriormente.

Tecnología firewall de inspección de paquetes
(SPI: Stateful Packet Inspection)

- Tecnología de firewall de tercera generación
- Examina *todas* las partes del paquete IP
- Mantiene un registro de todas las solicitudes de información que se originan en la red



- ✓
- Buena seguridad
- Detección completa del nivel de aplicación
- Alto desempeño
  - Más rápido que la alternativa proxy
- Relativamente fácil de configurar y de hacerle mantenimiento

Figura II.5: Tecnología firewall de inspección de paquetes

II.2.3.- Funciones Adicionales y Arquitecturas de los Firewalls

Además de las capacidades de seguridad estándares, se ha integrado una gran cantidad de características y funciones adicionales a los productos firewall, entre las cuales figuran: soporte para servidores públicos de Web y correo electrónico, por lo general llamada zona desmilitarizada (DMZ), filtrado de contenido, soporte de encriptación de VPN y de antivirus.

II.2.3.1.- Firewalls con Zona Desmilitarizada (DMZ)

Un firewall que provee protección DMZ es una solución efectiva para empresas que ofrecen a sus clientes la posibilidad de conectarse a su red a partir de cualquier medio externo, ya sea a través de Internet o cualquier otra ruta, como por ejemplo, una compañía de hosting de Web o que vende sus productos o servicios por Internet. La decisión de optar por un firewall con DMZ debe basarse en la cantidad de usuarios externos que acceden a la red y la frecuencia con la que lo hacen. Un firewall con DMZ crea un área de información protegida "desmilitarizada" en la red. Los usuarios externos pueden ingresar al área protegida, pero no pueden acceder al resto de la red. Esto permite a los usuarios externos acceder a la información que se quiere que vean, pero previene que obtengan información no autorizada. Esta red se conoce como *Red perímetral* y se define como una red adicional entre una red protegida y una red externa a fin de proporcionar una seguridad adicional; a este tipo de redes se les conoce por las siglas DMZ (De-Militarized Zone o zona desmilitarizada).

II.2.3.2.- Arquitectura Screened Subnet

Esta es la arquitectura más popular. Agrega un nivel extra de seguridad que la arquitectura Screened Host (descrita más adelante) ya que añade un perímetro a la red, que aísla fuertemente a la red interna de Internet.

Los hosts bastión son las máquinas más vulnerables en la red. Un host bastión es una máquina que debe estar altamente protegida porque es vulnerable a un ataque debido a que está expuesta a Internet o cualquier otra red pública, y es el punto principal de contacto para usuarios de redes internas. En otras palabras, es la máquina que es vista por la red externa. El host bastión contiene la información que queremos hacer accesible a través de Internet; un ejemplo de un host bastión puede ser un servidor de correo o un servidor HTTP. Si una red interna es muy abierta pasa a ser un objetivo tentador para un hacker. No hay otra defensa entre esta máquina y las máquinas

internas. Al aislar el host bastión en un perímetro, se puede reducir el impacto de atacar al host bastión.

La arquitectura Screened Subnet tiene dos "screening router", cada uno conectado al perímetro. Uno esta situado entre el perímetro y la red interna y otro entre el perímetro y la red externa. Para penetrar a una red interna con este tipo de arquitectura, el atacante debe pasar por ambos routers. Si un atacante logra penetrar al host bastión, deberá lograr pasar por el router interno. También se puede crear una serie de perímetros entre el mundo externo y la red. Los servicios más peligrosos son pasados de los perímetros más externos a los más internos. La idea es que un ataque a una máquina en el perímetro más externo tendrá una tarea ardua para atacar a las máquinas internas porque deberá penetrar todos los niveles de seguridad de todos los demás perímetros. A continuación se muestra un ejemplo gráfico de la arquitectura screened subnet.

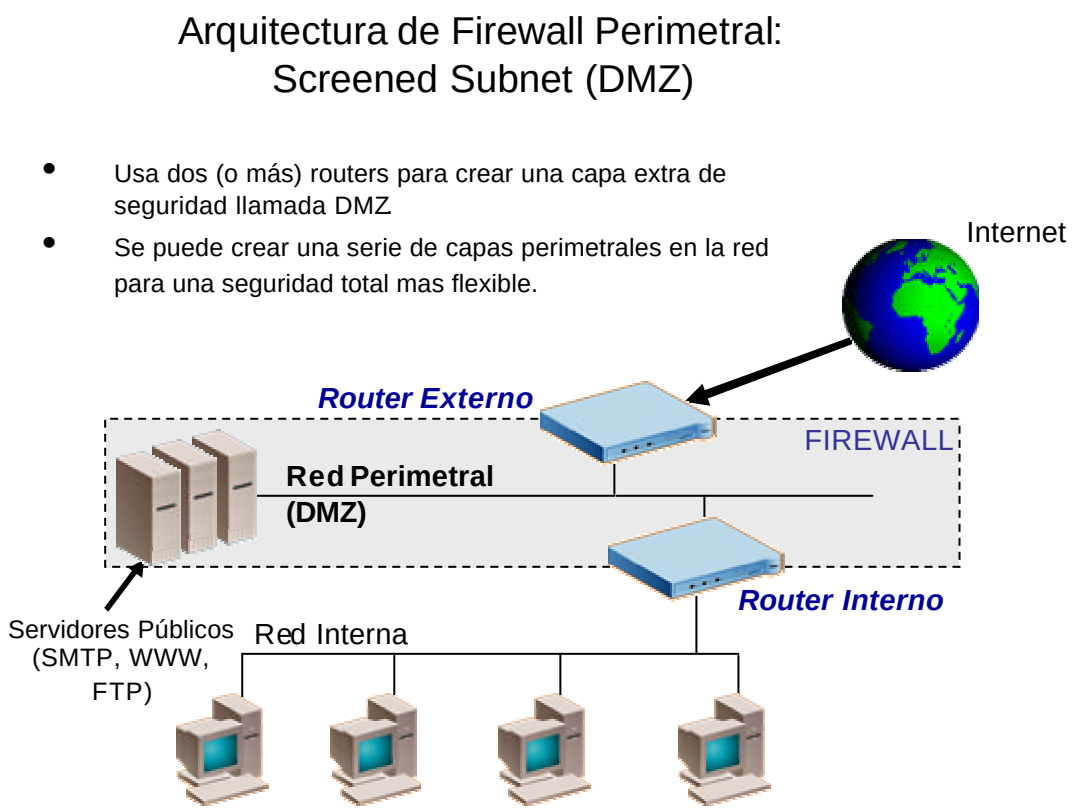


Figura II.6: Arquitectura de firewall Screened Subnet

En la siguiente figura se muestra gráficamente la arquitectura screened subnet fusionada usando un solo dispositivo que actúa como router y firewall empleando la tecnología de inspección de paquetes (SPI: Stateful Packet Inspection).

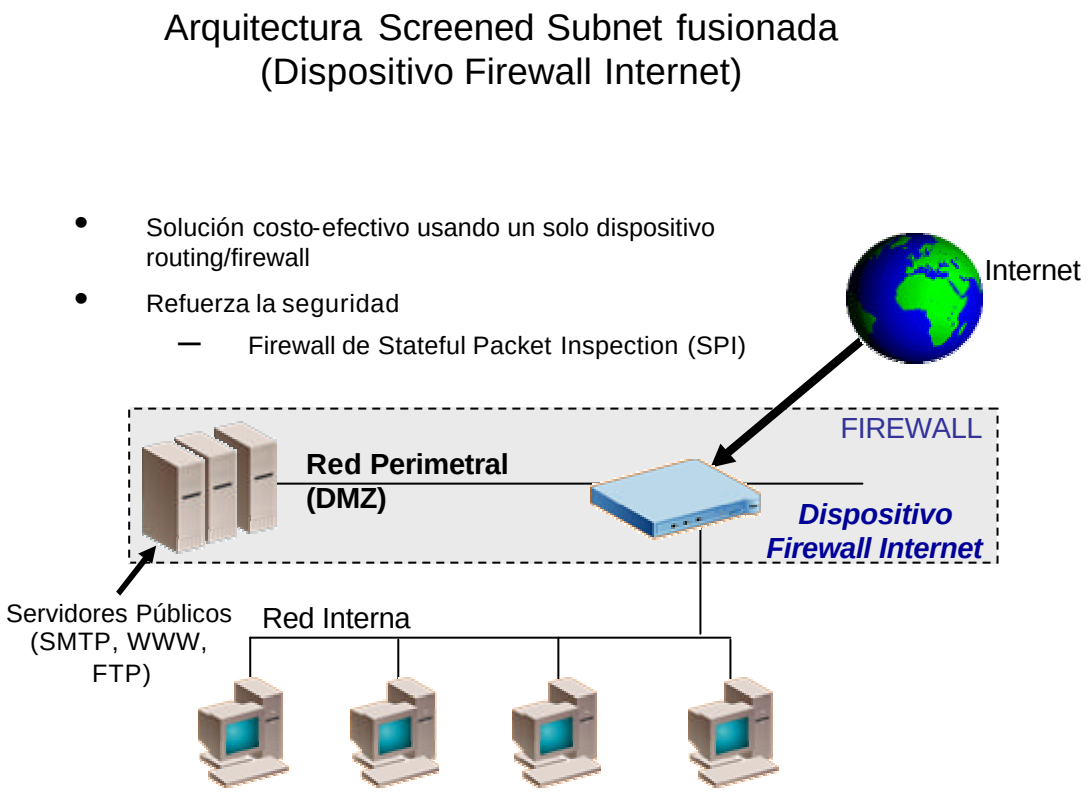


Figura II.7: Arquitectura de firewall Screened Subnet fusionada

II.2.3.3.- Arquitectura Screened Host

Esta arquitectura provee servicios desde un host que está en la red interna, usando un router separado. La principal seguridad está dada por el filtrado de paquetes. Un host bastión está situado en la red interna. Los paquetes filtrados por el screening router son configurados de tal manera que el host bastión es la única máquina de la red interna a la que los host de Internet pueden abrir conexiones. Sólo cierto tipo de

conexiones son permitidas. Cualquier sistema externo que intente acceder al sistema interno deberá conectarse con este host. El host bastión necesita entonces tener un alto nivel de seguridad. El filtrado de paquetes también debe permitir al host bastión abrir conexiones al mundo exterior. La configuración del filtrado de paquetes en un screening router puede hacerse de la siguiente manera:

- Permitir a otros hosts internos conexiones con otros hosts de Internet para ciertos servicios (permitiendo esos servicios con paquetes filtrados).
- No permitir todas las conexiones desde hosts internos (forzar a esos hosts a usar el servicio de proxy vía el host bastión).

Se pueden mezclar estas políticas para diferentes servicios: algunos pueden ser permitidos directamente filtrando paquetes, mientras que otros directamente vía proxy. Existen algunas desventajas; la principal es que si un ataque penetra el host bastión, esto no es notado por la red interna. El router también presenta un punto de falla: si el router está comprometido, la red entera está disponible para ser atacada.

II.2.3.4.- Arquitectura Dual-Homed Host

Una arquitectura dual-homed host está construida a partir de un host con dos interfaces de red. Tal host actúa como router entre las dos redes que el conoce y es capaz de rutear paquetes IP desde una red a otra. Pero los paquetes IP de una red a la otra no son enrutados directamente. El sistema interno al firewall puede comunicarse con el dual-homed host, y los sistemas fuera del firewall también pueden comunicarse con él, pero los sistemas no pueden comunicarse directamente entre ellos. El dual-homed host puede proveer varios niveles altos de control. Si no se permite que los paquetes pasen entre redes externas e internas, puede tenerse la seguridad que cualquier paquete en la red interna que tenga como origen una dirección externa es evidencia de algún problema de seguridad.

II.2.4.- Firewalls con Filtrado de Contenido

Un filtro de sitios Web o filtro de contenido extiende las capacidades del firewall para bloquear el acceso a ciertos sitios Web. Se puede usar esta función adicional para asegurarse de que los usuarios no accedan contenido inapropiado, como por ejemplo, material pornográfico o racista. Esta funcionalidad permite definir categorías de material inadecuado y obtener un servicio que lista miles de sitios Web que incluyen dicho tipo de material. Adicionalmente, se puede escoger si se quiere bloquear totalmente el acceso a estos sitios o permitir su uso, pero manteniendo un registro del mismo. Tal servicio debe actualizar automática y regularmente la lista de sitios Web que no pueden ser accedidos.

II.2.5.- Firewalls con Protección Antivirus

Todos debemos preocuparnos seriamente por las amenazas de los virus, uno de los esquemas más nocivos de "hacking" de computadoras. Los usuarios pueden dañar rápidamente toda una red si, inadvertidamente, bajan material desconocido o diseminan virus peligrosos en las redes. Empresas de todo tipo y tamaño han perdido enormes cantidades de dinero, debido al impacto negativo en la productividad y los costos de reparación de la red causados por un virus. Los firewalls no están diseñados para remover o limpiar virus. No obstante, pueden ayudar a detectarlos, lo cual es un factor esencial de cualquier plan de protección contra virus. Es importante observar que el firewall sólo puede proteger la red a partir del dispositivo de WAN al cual está conectado. Un servidor de acceso remoto o una PC con un módem puede servir como puerta de acceso a la red, el cual puede burlar las medidas de seguridad del firewall. Lo mismo puede ocurrir cuando un empleado introduce un diskette infectado con un virus en su PC. El lugar más apropiado para instalar el software antivirus es en la PC de cada usuario. No obstante, un firewall puede contribuir a la detección de virus, exigiendo que cada usuario que ingrese a Internet o baje correo electrónico, utilice, como mínimo, la última versión del software antivirus.

II.2.6.- Firewalls con VPN (Red Privada Virtual)

Una VPN es una red privada de datos que utiliza la infraestructura de la red pública, es decir, Internet. El propósito de una red VPN es ofrecer a las empresas las mismas capacidades de las redes privadas, pero a un costo mucho menor. Una red VPN permite compartir recursos públicos en forma segura, mediante el uso de técnicas de encriptación, garantizando así que solamente los usuarios autorizados puedan ver o entrar en la red privada de la empresa. Hoy en día, las redes VPN son consideradas por las empresas como un medio rentable de conectar en forma segura sus sucursales, trabajadores remotos, socios y clientes principales a sus redes LAN privadas. Una creciente cantidad de firewalls ahora cuenta con capacidades de encriptación VPN, ya sea integradas o como característica opcional. Este recurso ofrece a las empresas una alternativa sencilla y rentable, en comparación con las líneas dedicadas tradicionales o el acceso remoto a través de módem. Al momento de implementar una VPN, es necesario asegurarse de que todos los dispositivos soporten el mismo nivel de encriptación y que proporcione suficiente seguridad. Uno de los factores que se debe tener en cuenta, es que entre más avanzado sea el nivel de encriptación, mayor capacidad de procesamiento requerirá el firewall. Algunos proveedores ofrecen ahora la aceleración de VPN por hardware, con el fin de optimizar el rendimiento del tráfico VPN.

II.2.6.1.- Definición y Estructura de una VPN

Una VPN (Red Privada Virtual) es un mecanismo de comunicación que permite conectar una o más redes privadas mediante una red pública, generalmente Internet, de forma que estas redes parezcan sólo una (Virtual) y mantenga la privacidad.

La privacidad de las comunicaciones se obtiene encriptando los datos que circulan por los canales públicos que actúan realmente como soportes intermediarios. Mediante un esquema de encriptación y autentificación se crean túneles, circuitos

virtuales que aíslan los flujos de datos determinados de cualquier otro tráfico que circule por el mismo medio de transmisión. De esta forma, sobre un medio completamente público, se logra la misma seguridad y características de operación que hay disponible en los circuitos de comunicación de carácter privado. A continuación se muestra un ejemplo gráfico de una VPN.

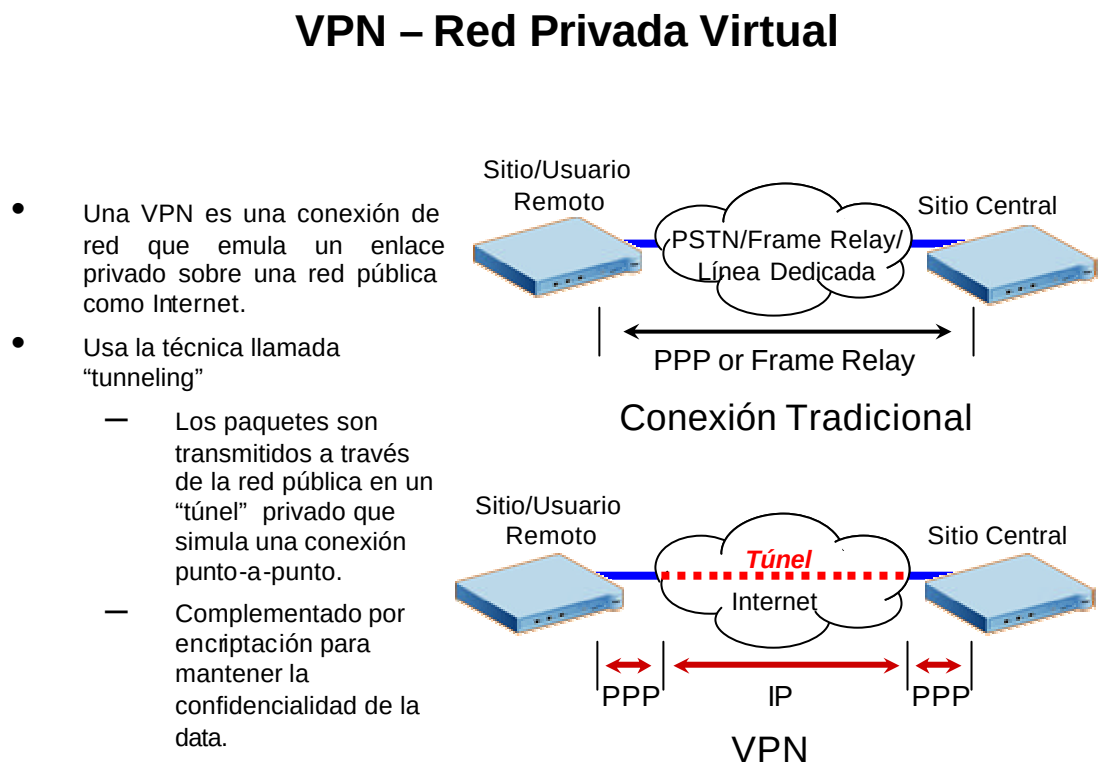


Figura II.8: RedPrivada Virtual

La tecnología de túneles ("tunneling") es un modo de transferir datos en la que se encapsula un tipo de paquetes de datos dentro del paquete de datos de algún protocolo, no necesariamente diferente al del paquete original. Al llegar al destino, el paquete original es desempaquetado volviendo así a su estado original. En el traslado a través de Internet, los paquetes viajan encriptados. La encriptación debe ser

realizada en tiempo real. Por eso, los flujos a través de una red son encriptados utilizando mecanismos de clave secreta con claves que son solamente buenas para sesiones de flujo.

Las técnicas de autenticación son esenciales en las VPNs, ya que aseguran a los participantes de la misma que están intercambiando información con el usuario o dispositivo correcto. La autenticación es llevada a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no haya algún tercer participante que se haya entrometido en la conversación. La autenticación también puede ser usada para asegurar la integridad de los datos. Los datos son procesados con un algoritmo de hashing para derivar un valor incluido en el mensaje como checksum. Cualquier desviación en el checksum indica que los datos fueron dañados durante la transmisión o interceptados y modificados en el camino. A continuación se muestra gráficamente los componentes de un túnel VPN.

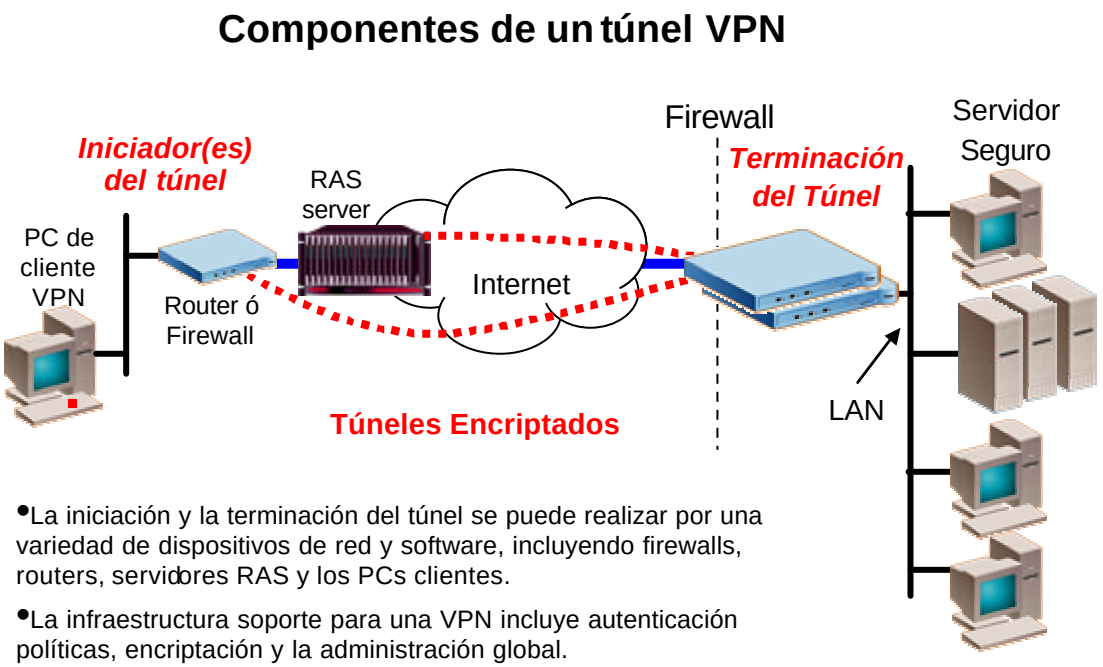


Figura II.9: Componentes de un túnel VPN

II.2.6.2. - Requisitos Funcionales de las VPN

Para que una VPN proporcione la comunicación que se espera, el sistema que se implante ha de contemplar varios aspectos de funcionamiento para determinar que será una buena solución.

- *Transparente a las aplicaciones:* Es decir que las aplicaciones no necesiten adaptarse a este nuevo mecanismo sin afectar el correcto funcionamiento de las aplicaciones.
- *Confidencialidad:* Los datos que circulan por el canal sólo pueden ser leídos por el emisor y el receptor. La manera de conseguir esto es mediante técnicas de encriptación.
- *Autentificación:* Emisor y receptor son capaces de determinar de forma inequívoca sus identidades, de tal manera que no exista duda sobre las mismas. Esto puede conseguirse mediante firmas digitales o aplicando mecanismos desafío-respuesta.
- *Integridad:* Capacidad para validar los datos, esto es, que los datos que le llegan al receptor sean exactamente los que el emisor transmitió por el canal. Para esto se pueden utilizar firmas digitales.
- *No repudio:* Cuando un mensaje va firmado, el que lo firma no puede negar que el mensaje lo emitió él.
- *Control de acceso:* Capacidad para controlar el acceso de los usuarios a distintos recursos.
- *Viabilidad:* Capacidad para garantizar el servicio. Por ejemplo para las aplicaciones de tiempo real.

II.2.6.3. - Protocolos en la VPN

Si el "tunneling" es el método para crear la red virtual, el túnel es el camino lógico por el que los datos son encaminados desde un extremo a otro del circuito que se crea. Para que pueda establecerse un túnel es necesario que los extremos implicados utilicen los mismos protocolos de tunneling.

MPPE (Microsoft Point-to-Point Encryption, descrito en el RFC 3078): Es un protocolo que se basa en encriptar los datos de PPP (Point to Point Protocol). El algoritmo de cifrado que emplea es el RSA RC4 para proporcionar la confidencialidad de los datos. La longitud de la clave para la sesión puede ser negociada, actualmente soporta claves de sesión de 40 bits y 128 bits.

IPIP (IP in IP Tunneling, descrito en el RFC 1853): La encapsulación IP en IP ha sido empleada por bridges que tienen diferentes capacidades o políticas. Pero también se puede emplear para implementar técnicas de tunneling. La técnica de encapsulación es muy simple. Una cabecera IP exterior es añadida antes que la cabecera IP original. Entre ellas hay otras cabeceras para la ruta, por ejemplo cabeceras de seguridad que configuran el túnel.

PPTP (Point-to-Point Tunneling Protocol, descrito en el RFC 2637): Protocolo de encapsulado de PPP sobre IP. Es una especificación desarrollada por un consorcio de fabricantes, entre ellos estaban Microsoft, 3Com y U.S. Robotics. El protocolo se diseñó originalmente como una forma de encapsular protocolos no TCP/IP (como IPX) para poder ser transmitidos por Internet usando GRE (Generic Routing Encapsulation). Es una especificación genérica, que permite la adición de diversos mecanismos de autentificación y algoritmos de encriptación. Estas técnicas de seguridad no están dentro del protocolo, sino que se añaden a posteriori.

L2TP (Layer 2 Tunneling Protocol, descrito en el RFC 2661): Es una extensión del PPTP (Point-to-Point Protocol), mezclando lo mejor de los protocolos PPTP de Microsoft y L2F de Cisco. Los dos componentes principales del L2TP son: el LAC (L2TP Access Concentrator), que es el dispositivo que físicamente termina una llamada; y el LNS (L2TP Network Server), que es el dispositivo que autentifica y termina el enlace PPP. L2TP utiliza redes conmutadas de paquetes para hacer posible que los extremos de la conexión estén ubicados en distintas computadoras. El usuario tiene una conexión L2 al LAC, el cual crea el túnel de paquetes PPP. Así, los paquetes pueden ser procesados en el otro extremo de la conexión, o bien, terminar la conexión desde un extremo.

MS-CHAP (descrito en el RFC 2433): Microsoft creó MS-CHAP para autentificar estaciones remotas Windows. Proporciona la funcionalidad a la cual los usuarios LAN están acostumbrados, integrando algoritmos de cifrado y hash sobre redes Windows.

IPSec (IP Seguro, descrito en el RFC 2411): Protocolo que sirve para establecer una sesión segura entre dos hosts que se comuniquen a través de IP, proporcionando encriptación a nivel de la capa de red. IPSec trata de remediar algunas carencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.

IPSec proporciona una base estable y duradera para proporcionar seguridad de capa de red y soporta todos los algoritmos criptográficos que se utilizan hoy en día y también puede ajustarse a algoritmos nuevos, más potentes que vayan surgiendo. El protocolo IPSec cubre las siguientes cuestiones de seguridad principales:

- *Autenticación de origen de datos:* Verifica que cada datagrama ha sido originado por el remitente indicado.

- *Integridad de datos:* Verifica que el contenido de un datagrama no se ha cambiado por el camino, ni deliberadamente ni debido a errores aleatorios.
- *Confidencialidad de datos:* Oculta el contenido de un mensaje, normalmente mediante cifrado.
- *Protección de reproducción:* Impide que un agresor pueda interceptar un datagrama y reproducirlo posteriormente.
- *Gestión automatizada de claves criptográficas y asociaciones de seguridad:* Permite implementar la política VPN en toda la red con poca o ninguna configuración manual.

Los principales protocolos IPSec se listan a continuación:

- **AH -** Autentication Header (Cabecera de Autenticación)
- **ESP –** Encapsulating Security Payload (Carga útil de Seguridad Encapsulada)
- **IKE –** Internet Key Exchange (Intercambio de Claves de Internet)

Protocolo AH - Autentication Header (Cabecera de Autenticación)

El protocolo AH ofrece autenticación del origen de los datos, integridad de los datos y protección contra la reproducción. Sin embargo, AH no ofrece confidencialidad de datos, lo que significa que todos los datos se enviarán como texto legible.

AH asegura la integridad de los datos mediante la suma de comprobación que genera un código de autenticación de mensajes. Para asegurar la autenticación del origen de los datos, AH incluye una clave compartida secreta en el algoritmo que utiliza para la autenticación. Para asegurar la protección contra la reproducción, AH utiliza un campo de números de secuencia dentro de la cabecera AH. Es importante observar que a menudo estas tres funciones distintas se concentran y se conocen como

“autenticación”. En términos más sencillos, AH asegura que no se han manipulado los datos mientras se dirigían a su destino final.

A pesar de que AH autentica el datagrama IP en la mayor medida posible, el destinatario no puede predecir los valores de ciertos campos de la cabecera IP. AH no protege estos campos, conocidos como campos mutables. Sin embargo, AH siempre protege la carga útil del paquete IP.

Formas de utilizar AH

Se puede aplicar AH de dos formas: modalidad de transporte o modalidad de túnel. En la modalidad de transporte, la cabecera IP del datagrama se encuentra en la parte más externa de la cabecera IP, seguida de la cabecera AH y, a continuación, la carga útil del datagrama. AH autentica el datagrama entero, a excepción de los campos mutables. Sin embargo, la información que contiene el datagrama se transporta como texto legible y, por lo tanto, está sujeto a lecturas. La modalidad de transporte necesita menos actividad general del proceso que la modalidad de túnel, pero no proporciona tanta seguridad.

La modalidad de túnel crea una nueva cabecera IP y la utiliza como parte más externa de la cabecera IP del datagrama. La cabecera AH continúa en la nueva cabecera IP. El datagrama original (tanto la cabecera IP como la carga útil original) aparece en último lugar. AH autentica el datagrama entero, por lo tanto, el sistema que responde puede detectar si el datagrama ha cambiado por el camino.

Si ambos extremos de una asociación de seguridad hay una pasarela, se utiliza la modalidad de túnel. En la modalidad de túnel, las direcciones de origen y destino de la parte más externa de la cabecera IP no tienen necesariamente que ser iguales que las direcciones de la cabecera IP original. Por ejemplo, dos pasarelas de seguridad

pueden operar un túnel AH para autenticar todo el tráfico entre las redes que conectan. De hecho, esta es una configuración muy habitual.

La principal ventaja de utilizar esta modalidad de túnel es que esta modalidad protege totalmente el datagrama IP encapsulado. Además, la modalidad de túnel hace posible utilizar direcciones privadas.

Cabe mencionar que en muchos casos, los datos sólo necesitan autenticación. Aunque el protocolo ESP puede realizar la autenticación, AH no afecta al rendimiento de su sistema como lo hace ESP. Otra ventaja de utilizar AH es que ésta autentica el datagrama entero. ESP, por otra parte, no autentica la parte inicial de la cabecera IP o cualquier otra información que preceda a la cabecera ESP. Además, para poder implementar ESP hay que disponer de algoritmos criptográficos de 128 KB. La criptografía de 128 KB está restringida en algunos países, mientras que AH no está regulada y puede utilizarse libremente en todo el mundo.

Protocolo ESP – Encapsulating Security Payload (Carga útil de Seguridad Encapsulada):

El protocolo ESP ofrece confidencialidad de datos y, de forma opcional, ofrece autenticación del origen de los datos, comprobación de la integridad y protección contra la reproducción. La diferencia entre ESP y el protocolo AH es que ESP ofrece cifrado, mientras que ambos protocolos ofrecen autenticación, comprobación de la integridad y protección contra la reproducción. Con ESP, ambos sistemas de comunicación utilizarán una clave compartida para cifrar y descifrar los datos que intercambian.

Si se decide utilizar tanto el cifrado como la autenticación, el sistema que responde autentica el paquete en primer lugar y, a continuación, si el primer paso tiene éxito, el sistema procede con el descifrado. Este tipo de configuración reduce la actividad

general de proceso y asimismo reduce la vulnerabilidad frente a ataques de denegación de servicio.

Formas de utilizar ESP

Se puede aplicar ESP de dos formas: modalidad de transporte o modalidad de túnel. En la modalidad de transporte, la cabecera ESP sigue a la cabecera IP del datagrama IP original. Si el datagrama ya dispone de una cabecera IPSec, la cabecera ESP precederá a ésta. La cola ESP y datos de autenticación opcionales siguen a la carga útil.

La modalidad de transporte no autentica o cifra la cabecera IP, que podría dejar en evidencia la información de direccionamiento al alcance de posibles agresores mientras el datagrama está en tránsito. La modalidad de transporte necesita menos actividad general del proceso que la modalidad de túnel, pero no proporciona tanta seguridad. En la mayor parte de casos, los sistemas principales utilizan la ESP en modalidad de transporte.

La modalidad de túnel crea una nueva cabecera IP y la utiliza como parte más externa de la cabecera IPdel datagrama, seguido de la cabecera ESP y, a continuación, el datagrama original (tanto la cabecera IP como la carga útil original). La cola de ESP y datos de autenticación opcionales se añaden a la carga útil. Cuando se utiliza el cifrado y la autenticación, la ESP protegerá completamente el datagrama original porque ahora se habrán convertido en los datos de la carga útil del nuevo paquete ESP. ESP, sin embargo, no protege la nueva cabecera IP. Las pasarelas deben utilizar la ESP en modalidad de túnel.

Protocolo IKE (Internet Key Exchange):

Un concepto fundamental en IPSec es el de asociación de seguridad (SA): es un canal de comunicación unidireccional que conecta dos nodos, a través del cual fluyen los datagramas protegidos por mecanismos criptográficos previamente acordados. Al identificar únicamente un canal unidireccional, una conexión IPSec se compone de dos SAs, una para cada sentido de la comunicación.

Es necesario que cada extremo de la comunicación tenga en su poder las claves que van a ser utilizadas para enviar y recibir datagramas en AH o ESP , es decir, ambos extremos deben estar de acuerdo en los algoritmos criptográficos y los parámetros de control a utilizar para las transmisiones. Esto se puede realizar de forma manual o mediante algún protocolo de control que se encargue de negociar de forma automática de los parámetros necesarios, a esto se le llama negociación de SAs.

Para estandarizar esta operación el IETF ha definido el protocolo IKE, el cual realiza automáticamente la gestión automática de claves. Una característica destacada del protocolo IKE es que su utilidad no se limita al protocolo IPSec sino que es un protocolo estándar utilizable en otras situaciones.

IKE es un protocolo híbrido que se obtuvo como resultado de la integración de dos protocolos complementarios: ISAKMP y Oakley. El primero de ellos define de forma genérica el protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE, mientras que el segundo especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente.

El objetivo principal de IKE consiste en establecer una conexión cifrada y autenticada entre dos entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad IPSec. Para llevar a cabo esta negociación hay dos fases:

- **1 Fase:** Común a cualquier aplicación, en ella ambos establecen un canal seguro y autenticado. El canal seguro se consigue mediante el uso del algoritmo cifrado simétrico y un algoritmo HMAC. Las claves necesarias se derivaran de una clave maestra obtenida mediante un algoritmo de intercambio de claves de Diffie-Hellman. Este procedimiento todavía no garantiza la identidad de los nodos, por eso es necesario añadir algún procedimiento de autenticación.

- **2 Fase:** Esta fase el canal seguro IKE es utilizado para negociar los parámetros de seguridad específicos asociados a un protocolo determinado, IPSec. Aquí se negocian las características de la conexión ESP o AH y todos los parámetros necesarios. El equipo que haya iniciado la comunicación ofrece todas las posibles opciones que tiene configuradas en su política de seguridad y sus prioridades correspondientes. El sistema receptor aceptará la primera que coincida con los parámetros de seguridad que tenga definidos. Además, ambos nodos se informan del tráfico que van a intercambiarse a través de dicha conexión.

En las siguientes figuras se muestran gráficamente un resumen de los protocolos de tunneling VPN / Encapsulación y los modos IPSec.

Protocolos de túnel VPN y encapsulación

Túnel Capa 2

- Protocol de red encapsulado dentro del PPP
- Paquete entero PPP encapsulado dentro del protocolo de túnel
- Protocolo de túnel envía el paquete al destino a través de la red compartida
- L2TP y PPTP se construyen a partir del PPP

Túnel Capa 3

- Encapsula paquetes IP en un encabezado IP adicional
- Protocolo de túnel envía paquete al destino a través de la red compartida
- El modo de túnel IPSec es un protocolo de túnel de Capa 3

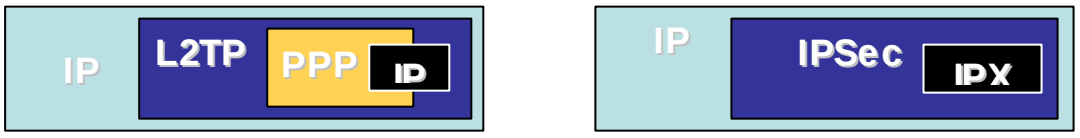


Figura II.10: Protocolos de túnel VPN y encapsulación

Protocolos de túnel VPN: Modos IPSec

El IPSec provee dos "modos" de operación

- **Modo de Transporte**
  - Protege el protocolo de la capa superior de un payload IP
  - Sin túnel; apropiada para Intranets seguras
  - Comunicaciones Peer-to-Peer

- **Modo de Túnel**
  - Protege el Datagrama IP completo
  - Provee el túnel para paquetes IP
  - Host-to-Gateway ó Gateway-to-Gateway

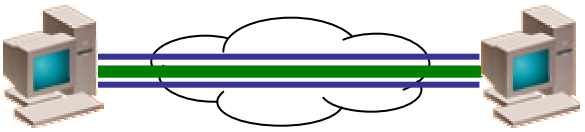


Figura II.11: Protocolos de túnel VPN: Modos IPSec

II.2.7.- Tipos de Firewall

Las funciones de un firewall pueden implementarse ya sea como software o como una adición a un router o gateway. Alternativamente, la demanda de los dispositivos dedicados de firewall están creciendo, principalmente debido a su facilidad de uso, mejor rendimiento y bajo costo.

II.2.7.1.- Firewalls basados en Routers / Firmware

Algunos routers proveen capacidades limitadas de firewall. Estas pueden incrementarse con software u opciones de firmware adicional. No obstante, es importante tener cuidado de no sobrecargar un router con servicios adicionales de firewall. Además, es posible que algunas funciones de firewall, como VPN, DMZ, filtrado de contenido o protección a través de antivirus, no estén disponibles o sean muy costosas de implementar.

II.2.7.2.- Firewalls basados en Software

Por lo general, los firewalls basados en software son aplicaciones sofisticadas y complejas que se ejecutan en servidores dedicados UNIX o NT. Estos productos se tornan aún más costosos cuando se suman los costos de software, sistema operativo, hardware de servidor y mantenimiento continuo requerido para soportar la implementación. Resulta esencial también que el administrador del sistema monitoree constantemente e instale las actualizaciones más recientes de seguridad y del sistema operativo, tan pronto como se encuentren disponibles. Sin estas actualizaciones que cubren los nuevos peligros de seguridad, el software de firewall puede volverse totalmente inservible.

II.2.7.3.- Dispositivos de Firewall dedicados

La mayoría de los dispositivos de Firewall son sistemas de hardware dedicados. Estos dispositivos son menos susceptibles a las fallas de seguridad inherentes de los sistemas operativos Windows NT o UNIX, gracias a que integran sistemas operativos desarrollados específicamente para utilizarse como firewall. Estos firewalls de alto rendimiento han sido diseñados para satisfacer los altos requerimientos de rendimiento o del procesador, exigidos por los firewalls SPI. Debido a que no es necesario fortalecer el sistema operativo, por lo general, los dispositivos de firewall

son más fáciles de instalar y configurar que los productos de firewall de software. Estos ofrecen potencialmente un nivel de instalación plug-and-play, requieren mínimo mantenimiento y una solución completa. También constituyen una solución rentable en comparación con otras implementaciones de firewall.

II.2.7.4.- Ventajas de un Firewall

A parte de las funciones adicionales de los firewalls, a continuación se mencionan en líneas generales las ventajas de los mismos.

- *Protección de la Red:* Mantiene alejados a los crakers (piratas informáticos) de la red al mismo tiempo que permite acceder a todo el personal de la oficina.
- *Control de acceso a los recursos de la red:* Al encargarse de filtrar, en primer nivel antes que lleguen los paquetes al resto de las computadoras de la red, el firewall es idóneo para implementar en él los controles de acceso.
- *Control de uso de Internet:* Permite bloquear el material no adecuado, determinar los sitios que puede visitar el usuario de la red interna y llevar un registro.
- *Concentra la seguridad:* El firewall facilita la labor a los responsables de seguridad, dado que su máxima preocupación es encarar los ataques externos y vigilar, manteniendo un monitoreo.
- *Control y Estadísticas:* Permite controlar el uso de Internet en el ámbito interno y conocer los intentos de conexiones desde el exterior y detectar actividades sospechosas.
- *Choke-Point:* Permite al administrador de la red definir un embudo manteniendo al margen los usuarios no autorizados fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques.

- *Genera Alarmas de Seguridad:* El administrador del firewall puede tomar el tiempo para responder una alarma y examinar regularmente los registros de base.
- *Audita y registra Internet:* Permite al administrador de red justificar el gasto que implica la conexión a Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda.

II.2.7.5.- Limitaciones de un Firewall

Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación, en este caso:

- Conexión dial-out sin restricciones que permita entrar a la red protegida; el usuario puede hacer una conexión SLIP o PPP al Internet. Este tipo de conexiones deriva de la seguridad provista por firewall construido cuidadosamente, creando una puerta de ataque.
- El firewall no puede protegerse de las amenazas a que está sometido por traidores o usuarios inconscientes.
- El firewall no puede protegerse contra los ataques de la ingeniería social, en este caso, un craker que quiera ser un supervisor o aquel que persuade a los usuarios menos sofisticados.
- El firewall no puede protegerse de los ataques posibles a la red interna por virus informativos a través de archivos y software.
- Tampoco puede protegerse contra los ataques en la transferencia de datos, estos ocurren cuando aparentemente datos inocuos son enviados o copiados a un servidor interno y son ejecutados despachando el ataque.

La siguiente figura muestra una limitación del firewall donde un usuario sin restricción hace una conexión PPP a Internet creando un hueco de seguridad.

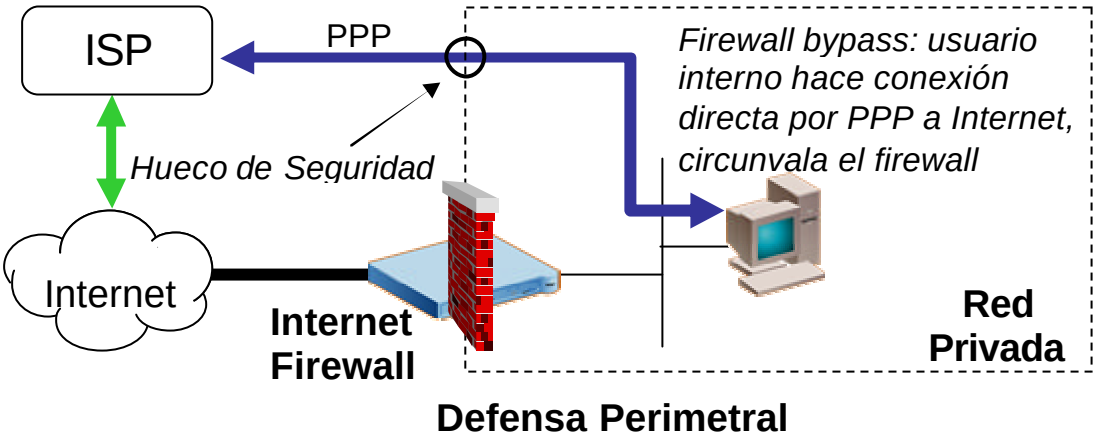


Figura II.12: Limitación del firewall por conexión PPP de usuario interno

CAPÍTULO III
SISTEMA ACTUAL

III.1.- Enfoque del Sistema Actual

El sistema de seguridad actual está basado en el software comercial Microsoft ISA Server 2000, instalado en modo integrado Firewall/Cache, el cual proporciona un nivel de seguridad para el acceso a Internet y las conexiones remotas a la red de datos que permiten el intercambio de información con algunos servicios implementados sobre la plataforma de la empresa en estudio. Dicho sistema controla el acceso a Internet de todos los usuarios de la red de datos y las páginas Web que visitan. Controla y limita diferentes servicios ofrecidos en Internet, como por ejemplo, el Messenger, Kazaa, ICQ, etc. Tiene habilitado solamente aquellos puertos que se usan en la red y brinda seguridad al acceso remoto del correo (Outlook Web Access). También protege la red de accesos indebidos y filtra mensajes no solicitados. Controla el acceso de usuarios remotos a la red corporativa a través del Remote Access Server y ofrece un nivel de seguridad a los servidores de Televigilancia que existen en la corporación.

La empresa en estudio dedicada al sector jurídico, está ubicada en Caracas y posee alrededor de 150 empleados. Recientemente al área de negocios, conformada por abogados y paralegales, les fueron cambiados los PCs que tenán como estaciones de trabajo por equipos portátiles de última generación (laptop), de manara que pudieran transportarlos a las oficinas de los clientes y ser utilizados desde sus casas bajo la modalidad de “Home Office”, convirtiéndose en una herramienta que les da más productividad y eficiencia a su trabajo. Debido a que gran parte del negocio se sustenta con el intercambio y consulta de información, los servicios de correo e Internet son indispensables para su eficiente operación. Los profesionales del derecho viajan frecuentemente para atender requerimientos de clientes que se encuentra en el

exterior, específicamente en Estados Unidos, Europa y algunos países de Sur América, lo que conlleva que los servicios que prestan los servidores de la empresa deben estar operativos las 24 horas del día y los 365 días del año permitiendo la disponibilidad de la información en línea y poder así garantizar una eficiente productividad en el momento de la toma de decisiones. La labor ágil, oportuna y segura de los trámites judiciales, procesales y administrativos que deben llevar los abogados, requieren de soluciones informáticas efectivas.

Cabe destacar la importancia de Internet y su continua disponibilidad. La empresa se encuentra en la actualidad suscrita a varios servicios de información legal a nivel nacional e internacional. Entre ellas está Microjuris (www.microjuris.com), uno de los portales más utilizado por los profesionales del derecho. Fue creada con la colaboración de empresas nacionales e internacionales expertas en sistemas de información jurídica, para facilitar el acceso rápido y universal a una masiva bibliografía legal de Venezuela, incluyendo leyes y reglamentos, sentencias de tribunales, normativa administrativa, tratados internacionales y noticias. En esta página también se encuentra integrado el sistema "Indice de Consulta Legal" (Incoleg), la más completa base de información referencial existente en Venezuela, con más de 14.000 fichas a todas las normas vigentes. Adicionalmente tiene incorporada "HiperLex", una base contentiva de más de 500 leyes y reglamentos vigentes, en texto completo, así como la Gaceta Oficial desde 1989. Actualmente se discute con la Corte Suprema de Justicia y la Biblioteca Nacional la incorporación de sus documentos jurídico-legales a la red, de manera de integrar en un sólo sitio la más completa biblioteca jurídica virtual del país.

De aquí la importancia de la continuidad y disponibilidad de un acceso seguro a Internet y demás servicios, lo cual aumentará la calidad y la productividad de los procedimientos implicados en el área de negocios de la empresa.

III.2.- Plataforma Tecnológica del Sistema de Seguridad Actual

El estudio y análisis que se le realizó a la plataforma tecnológica del sistema de seguridad actual permitió evaluar alternativas que conllevaron a reforzar la seguridad del acceso a Internet de la organización para mejorar y brindar una mayor protección a las conexiones remotas y al acceso a la información en servidores publicados en Internet.

A continuación se muestra un esquema general de la plataforma tecnológica de seguridad actual y posteriormente el detalle de la misma.

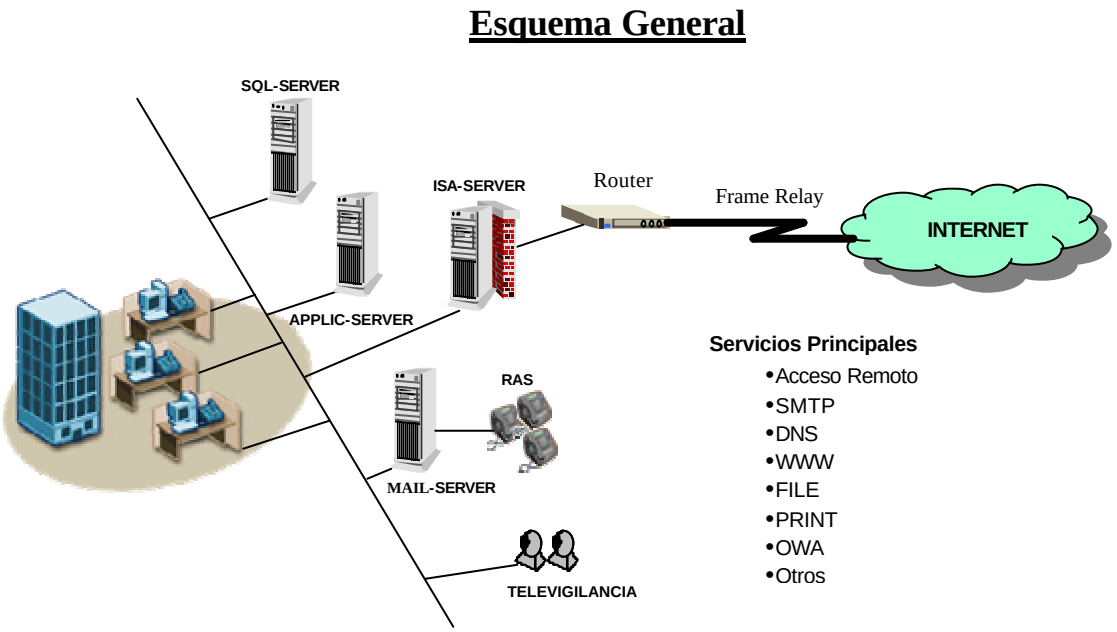


Figura III.1: Esquema general de la plataforma tecnológica de seguridad

III.2.1.- Sistema de Acceso

III.2.1.1.- Acceso a Internet

El acceso a Internet está configurado de la siguiente manera:

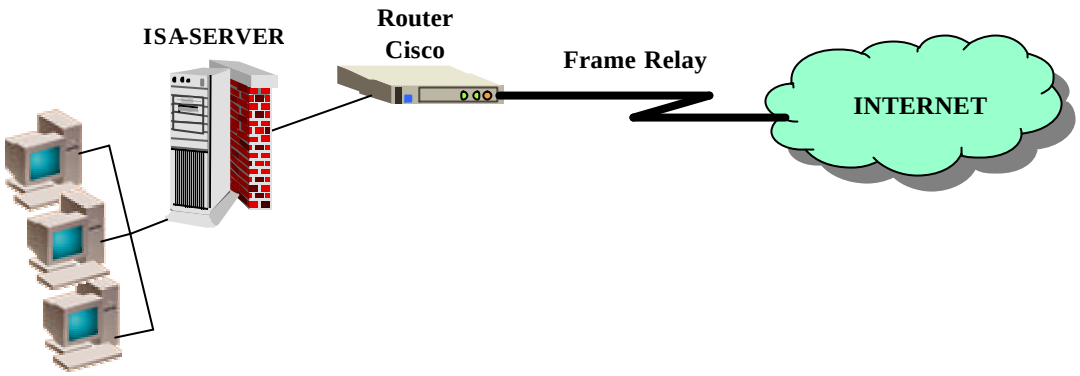


Figura III.2: Acceso a Internet

Tipo de Enlace:

Frame Relay de 512 Kbps con el proveedor CANTV

Router:

- Router Cisco modelo 1720
- Soporte para direcciones IP
- Soporte NAT
- Soporte de conexiones Fame Relay
- Soporte de enrutamiento a través de rutas estáticas
- Puerto WAN síncrono que soporta la velocidad del enlace con interfaz V.35

III.2.1.2.- Acceso Remoto Dial-Up

El acceso remoto dial-up está configurado de la forma siguiente:

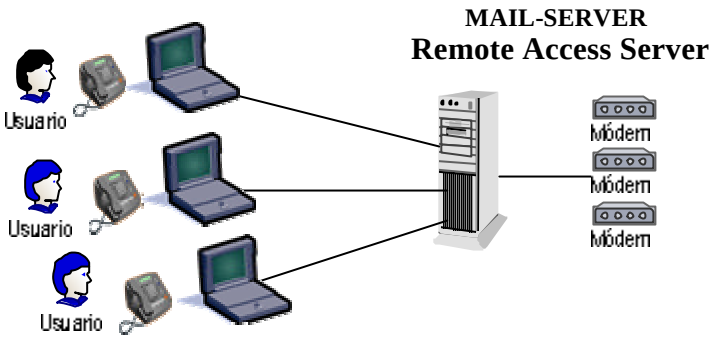


Figura III.3: Acceso remoto dial-up

MAIL-SERVER

Servidor de Acceso Remoto (RAS)

Hardware

- Servidor IBM XSeries 235
- Intel Pentium IV 2.4 GHz
- 1 GB RAM
- 4 Discos Duro SCSI de 18GB c/u
- Tarjeta PCI Multi-Puerto Digi AccelePort 8r 920 (Maneja 8 modems)

Software

- Sistema Operativo Microsoft Windows 2000 Server
- Microsoft Exchange 2000 Server
- Symantec Norton Antivirus For Exchange, Corporate Edition
- Remote Access Server
- DNS Server
- DHCP Server

III.2.2.- Sistema de Seguridad Firewall

El sistema actual de seguridad firewall está configurado como se muestra a continuación.

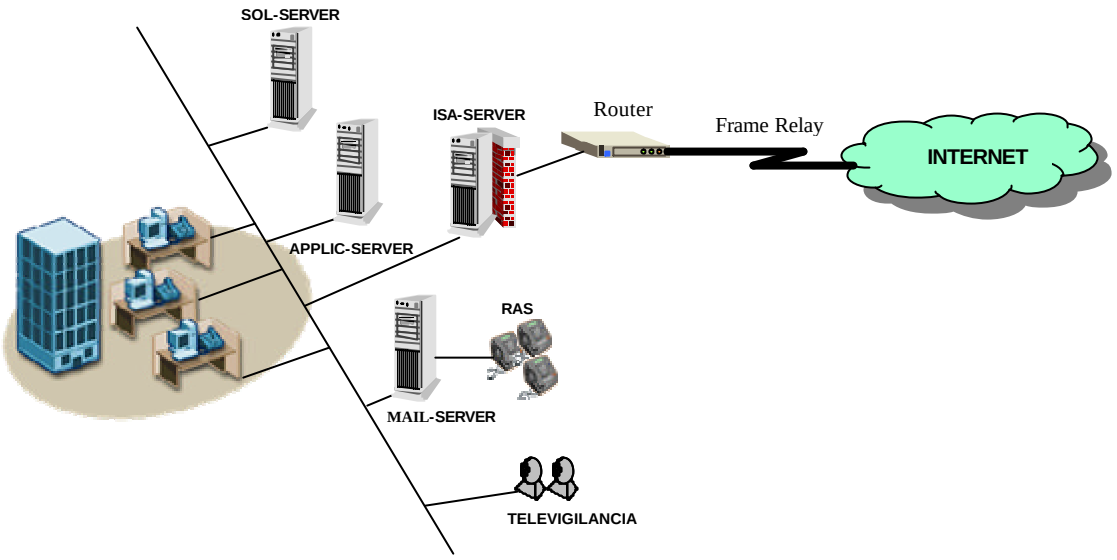


Figura III.4: Sistema de seguridad firewall

Sistema ISA SERVER 2000

Internet Security and Acceleration Server

Hardware

- Servidor IBM Netfinity 5100
- Intel Pentium III 731 MHz
- 1 GB RAM
- 6 Discos Duro SCSI de 18.5 GB c/u
- 2 Tarjetas de Red – NIC Interna / NIC Externa

Software

- Sistema Operativo Microsoft Windows 2000 Server
- Microsoft ISA Server 2000, Modo Integrado / Firewall y Cache
- Symantec Norton Antivirus Server, Corporate Edition

Clientes:

Hardware

- Laptops Hewlett Packard nx9010
- Intel Pentium IV 2.8 GHz
- 256 MB RAM
- Disco Duro 40 GB
- DVD, CD/RW
- MODEM 56 Kbps, RJ45, Salida TV, Floppy 3.5

Software

- Sistema Operativo Microsoft Windows XP Professional
- Microsoft Firewall Client
- Norton Antivirus Client
- Microsoft Office XP
- Software Corporativo

Hardware

- DeskTops IBM Netvista
- Intel Pentium III 667 MHz
- 128 MB RAM
- Disco Duro 10 GB
- CD ROM
- RJ45, Floppy 3.5

Software

- Sistemas Operativos Microsoft Windows 98 / Microsoft Windows ME
- Microsoft Firewall Client
- Norton Antivirus Client
- Microsoft Office 2000
- Software Corporativo

III.2.2.1.- Direccionamiento IP

Actualmente la empresa cuenta con un rango de direcciones IP válidas asignadas por su Proveedor de Servicios de Internet, CANTV, cuyas características son las siguientes.

Segmento de Red:	XXX.XX.XXX.8/29
Red Clase:	"C"
Dirección:	XXX.XX.XXX.8
Máscara:	255.255.255.248
Rango de Host:	XXX.XX.XXX.9
	XXX.XX.XXX.14
Broadcast:	XXX.XX.XXX.15
Router WAN:	XXX.XX.XXX.10

La plataforma actual de seguridad de acceso a Internet consta de segmentos de redes diferentes con direcciones IP privadas, un segmento "Externo" que corresponde a la salida hacia Internet y un segmento "Interno" que corresponde a la red interna de la empresa.

El segmento “Externo” está constituido por las interfaces del router y la tarjeta NIC externa del ISA-Server, que es el actual firewall.

Segmento de Red:	XXX.XXX.X.1/16
Red Clase:	“B”
Dirección:	XXX.XXX.X.1
Máscara:	255.255.0.0
Rango de Host:	XXX.XXX.0.2
	XXX.XXX.255.254
Router LAN:	XXX.XXX.X.2
NIC Externa ISA:	XXX.XXX.X.3

El segmento “Interno” está constituido por la interfaz de red del firewall (NIC interna del ISA-Server) y el resto de los elementos conectados a la red interna.

Segmento de Red:	XXX.XX.X.1/16
Red Clase:	“B”
Dirección:	XXX.XX.X.1
Máscara:	255.255.0.0
Rango de Host:	XXX.XX.0.2
	XXX.XX.255.254
NIC Interna ISA:	XXX.XX.X.3

Como se puede observar, hay una separación entre la red interna de la empresa y la red pública de Internet brindando un nivel de seguridad a los usuarios y servicios.

III.2.3.- Especificaciones del Sistema Firewall Actual

El sistema de muro de seguridad instalado está basado en la aplicación Microsoft ISA Server 2000 y corre bajo el sistema operativo Windows 2000 Server. El mismo está instalado en un Servidor IBM Netfinity 5100 que posee dos adaptadores de red. La tarjeta de red interna tiene asignada una dirección IP correspondiente al rango "Interno" de direcciones IP privadas. La tarjeta externa tiene asignada una dirección IP correspondiente al rango "Externo" de direcciones IP privadas que a su vez tiene un NAT estático en el router con una dirección IP válida asignada por CANTV. La interfaz LAN del router también tiene asignada una dirección IP perteneciente al rango "Externo". Para proteger la privacidad de la red interna mediante el ocultamiento de las direcciones IP privadas a la vista pública, están definidas en el router las reglas para la ejecución de NAT, Network Address Translation.

La aplicación ISA Server 2000 está instalada actualmente como servidor de seguridad firewall y de caché integrado. El caché fue implementado para que los usuarios accedan rápidamente las páginas que visitan con más frecuencia. Internet es muy utilizado por todos los usuarios dentro de la organización, por ende hay un gran volumen de tráfico que cruza las puertas de enlace de la red. Pero las funciones de caché Web del servidor ISA han mejorado el rendimiento del acceso a Internet debido al almacenamiento en disco de las páginas Web. Además, mediante los controles de acceso basados en políticas se ha restringido el acceso a determinados usuarios y conexiones a ciertas páginas según la hora del día y el contenido Web. La configuración del almacenamiento en caché y el control de acceso en el servidor ISA ayudan a mejorar la productividad de los usuarios que necesitan un acceso a Internet rápido, seguro y eficiente. Adicionalmente el servidor ISA utiliza un caché de almacenamiento en memoria RAM con un eficiente sistema de entrada y salida de archivos.

El servidor ISA también tiene configurado varias políticas de seguridad. Entre ellas están las siguientes:

Política de Acceso al Exterior: Esta política tiene configurada reglas para sitios, contenido y protocolos que permiten controlar el acceso de los usuarios internos a Internet. Las reglas de sitios y contenido especifican a qué sitios y a qué contenido se puede tener acceso. Las reglas de protocolo indican si se puede utilizar un determinado protocolo para las comunicaciones entrantes o salientes. Por ejemplo, está configurado el acceso o restricción a contenidos tales como audio (mp3, mp2, rmi, etc.), videos (mpeg, asf, wmf, vid, etc.) por grupos y horarios. Entre los protocolos controlados se encuentran el HTTP, FTP, SMTP, POP3, H.323, MSN Messenger, PNM, RTSP, etc.

Política de Detección de Intrusos: Esta política cuenta con los mecanismos integrados de detección de intrusos que avisan cuando se inicia un determinado tipo de ataque contra la red. Por ejemplo, se tiene configurado para que notifique si se detecta un intento de exploración de puertos, IP spoofing.

Política de Filtros de Paquetes: El servidor ISA actualmente analiza y controla el tráfico específico de paquetes mediante filtros que inspeccionan los datos y distinguen cada aplicación. Por ejemplo, DNS lookup, ICMP all outbound, ICMP ping response, ICMP source quench, ICMP timeout, ICMP unreachable, RDP.

Adicionalmente, el servidor ISA está utilizando las siguientes características para publicar el servicio OWA (Outlook Web Access).

Publicación Segura en Web. Las reglas de publicación en Web permiten el acceso seguro al servidor Web interno, en este caso, el mail server que tiene el servicio OWA. Así mismo, concede a los usuarios remotos acceso a este servidor interno, al tiempo que lo protege frente a accesos no autorizados.

Publicación Segura en Servidor de aplicaciones. Las reglas de publicación en servidores permiten que determinados usuarios tengan acceso a los servidores internos. Se tiene publicado actualmente, el Exchange RPC Server, NNTP Server, IMAP4 Server, POP3 Server y SMTP Server.

El sistema de seguridad cuenta también con una serie de alertas, logs, monitoreos y reportes que le son útiles al departamento de Sistemas. Se monitorea las sesiones de los usuarios para determinar quienes están usando el ISA Server, identificándolos por nombre de computadora y dirección IP. Se tienen alertas de DNS Intrusion, Intrusion Detected, IP spoofing, POP Intrusión, Service not responding, Service shutdown, Service started, SMTP Filter event, Firewall communication failure, IP Protocol violation, entre otros.

Cabe mencionar que el ISA-Server también trabaja como servidor antivirus. Tiene instalado la aplicación Symantec Norton Antivirus Corporate Edition la cual actualiza automáticamente desde Internet la última huella publicada por Symantec, y se encarga de distribuirla en todas las estaciones de trabajo de la empresa. El servidor de correos cuenta con la versión Symantec Antivirus For Exchange, que controla mediante reglas y filtros los virus entrantes vía email, además de generar logs, estadísticas y reportes útiles para llevar un mejor control y educar a los usuarios en cuanto al uso correcto del servicio de correo corporativo.

III.2.4.- Limitaciones en el Entorno del Sistema de Seguridad Actual

Un aspecto a considerar es que si por algún motivo el ISA-Server queda fuera de servicio por fallas técnicas ó problemas a nivel de software por un tiempo prolongado, la empresa quedaría sin servicios de correo e Internet. Debido a que el área de negocio no puede quedar sin dichos servicios, provisionalmente se pudiera conectar el cable UTP de la tarjeta interna del ISA-Server al puerto LAN del router y cambiar la dirección IP del puerto LAN del router por una perteneciente al segmento

de red de la NIC interna del ISA-Server. Pero esto traería como consecuencia que la red completa quedara expuesta a cualquier ataque externo, poniendo en peligro la integridad de la información confidencial y la infraestructura de la red.

Cabe mencionar que el ISA-Server publica servidores y equipos que se encuentran en la red privada para que puedan ser accesados desde la red pública de Internet. Este tipo de configuración presenta la debilidad de que los servidores públicos que deben ser accesados desde Internet se encuentran físicamente conectados en la red privada y esto puede representar una posible brecha de vulnerabilidad para conectar y dañar otros equipos dentro de la LAN violando la confidencialidad de la información.

Otro punto a tomar en cuenta es que actualmente la empresa tiene en proyecto aperturar unas oficinas remotas, lo que implica que debe existir una infraestructura de seguridad robusta en su sede principal.

Además, próximamente se va a instalar un servidor Web que prestará un servicio a los clientes de la empresa vía Internet donde ellos podrán consultar sus casos legales, sus estados de cuenta y pagos realizados. Por tratarse de información altamente confidencial y que estará disponible por Internet, dicho servidor debe contar con una buena seguridad.

Adicionalmente está en proyecto migrar la plataforma de los sistemas de facturación y de documentación. Este último es un sistema que ofrece al área de negocios las consultas de leyes, jurisprudencias, expedientes, ordenanzas, publicaciones periódicas, modelos de contratos, libros de compañías, gacetas públicas, entre otros. Estos sistemas estarán implementados en un servidor Web.

Otro aspecto importante a considerar es que actualmente la Gerencia de Sistemas no cuenta con la misma cantidad de personas que tenía hace un año debido a la situación política económica. Esto ha traído como consecuencia una carga de trabajo adicional a las personas existentes en el departamento, lo que ha implicado dejar a un lado las

actividades de monitoreo y revisión de logs y registros de eventos. Si no se cuenta con un sistema que brinde alta seguridad, dejar a un lado estas actividades puede traer consecuencias lamentables.

Un punto adicional a mencionar también es que la empresa Microsoft a principios de este año publicó algunas vulnerabilidades detectadas en el ISA Server 2000, y liberó nuevos parches para corregir fallas de seguridad en su software. La vulnerabilidad en ISA Server 2000 se catalogó por la propia Microsoft como crítica. Microsoft ha recomendado que se instale el Service Pack2 del ISA Server 2000, el cual ofrece las actualizaciones más recientes de dicha aplicación y un mayor nivel de seguridad, fiabilidad y estabilidad para los clientes. El Service Pack2 incluye lo siguiente:

- Todas las revisiones y actualizaciones de seguridad emitidas desde el lanzamiento del servidor ISA para su fabricación.
- Soluciones para los problemas habituales indicados por los clientes a través de los servicios de soporte técnico de Microsoft.
- Una estabilidad mejorada de la herramienta de administración y los servicios del servidor ISA en una serie de entornos.
- Soluciones recomendadas mediante una revisión por parte de expertos de seguridad de otras empresas.

Pueden existir otras vulnerabilidades que aún no han sido descubiertas en el ISA Server 2000 y de aquí la importancia de reforzar la seguridad del acceso a Internet en la organización.

Como se puede observar, la empresa bajo estudio cuenta con servicios y aplicaciones que requieren de un sofisticado sistema seguro de acceso a Internet que pueda brindar confiabilidad, escalabilidad, rendimiento y una mayor seguridad. Por ende los servicios adicionales que se implementarán a corto plazo a través de Internet

requieren de una evaluación de la plataforma de seguridad actual para cubrir y satisfacer las demandas de protección en la estructura tecnológica de la organización.

III.2.5.- Requerimientos de la Plataforma de Seguridad Actual

El análisis y estudio que se le realizó a la plataforma de seguridad de la empresa bajo estudio, conjuntamente con la información de los proyectos nuevos de la Gerencia de Sistemas y la investigación documental sobre las diferentes tecnologías de firewall que se ofrecen actualmente en el mercado, condujo a identificar las necesidades y requerimientos del sistema de seguridad actual. Estos requerimientos se exponen a continuación:

- El sistema de seguridad debe tener alta disponibilidad, lo que conlleva a que debe existir una redundancia del mismo en la plataforma.
- La solución a implementar debe soportar todos los servicios que actualmente no son procesados por el sistema de seguridad.
- Debe preverse la posibilidad de instalar nuevas tecnologías o expandir ante nuevas necesidades, tomando en cuenta las aplicaciones y los servicios que están en proyecto en la Gerencia de Sistemas.
- La administración de la plataforma debe ser sencilla, amigable y que cuente con una interfaz gráfica de usuario basada en Web, con ayuda en línea, de manera que pueda simplificar su administración sin consumir mucho tiempo.
- El dispositivo de seguridad debe contar con una amplia garantía, con soporte técnico de la compañía que lo fabrica y poseer una certificación avalada por algún organismo de seguridad internacional.
- Debe contar con un puerto DMZ para crear un área de información protegida desmilitarizada en la red, a fin de que los usuarios externos puedan ingresar al área protegida, pero no puedan acceder al resto de la red.

- La solución debe contar con alta disponibilidad de manera de garantizar la continuidad del acceso a los servicios, aplicaciones en línea y la operatividad segura de la red privada.
- Adicionalmente debe soportar conexiones VPN para una conectividad privada virtual basada en IPSec que permita un acceso remoto seguro.

CAPÍTULO IV
SISTEMA PROPUESTO

IV.1.- Bases para el Diseño del Firewall del Sistema Propuesto

Una vez hecho el análisis y definido los requerimientos de la plataforma de seguridad de la organización se consideraron los siguientes aspectos como base para el diseño del firewall:

- Posturas sobre la política de diseño del firewall
- Las políticas de seguridad para la plataforma
- El costo del producto firewall
- Los componentes del firewall

Para la selección del producto a implementar en la solución se buscó un firewall que proporcionara el nivel apropiado de protección y rentabilidad. Para ello se tomaron en cuenta los siguientes puntos:

Características de Seguridad

Atañe a la capacidad que un producto firewall tiene para ofrecer seguridad basándose y ajustándose a los objetivos y a las políticas de seguridad de la empresa.

- *Garantía de seguridad:* Se refiere a la garantía independiente acerca de la tecnología relevante del firewall que garantiza que cumplirá con sus especificaciones y que está instalada en forma adecuada. Que el producto esté certificado por un organismo como la ICSA (Internacional Computer Security Association).

- *Control de privilegios:* El grado al cual el producto puede imponer restricciones de acceso a los usuarios.
- *Autenticación:* El tipo de control de acceso que ofrece el producto. Si soporta las autorizaciones.
- *Capacidad de auditoría:* La capacidad del producto para supervisar el tráfico de la red para generar registros y para proporcionar informes estadísticos y alarmas.

Características de Implantación

Se refiere a la capacidad del producto para satisfacer los requerimientos y preocupaciones de administración de red.

- *Flexibilidad:* El firewall deberá ser lo bastante abierto como para ajustarse a la política de seguridad de la compañía, además de que deberá permitir cambios en esta característica.
- *Desempeño:* El firewall deberá ser lo bastante rápido como para que los usuarios no se quejen por la examinación de paquetes. El volumen de transferencia total de datos y la velocidad de transmisión asociada con el producto deberán ser razonables y consistentes con el ancho de banda que establece la conexión con Internet.
- *Escalabilidad:* El producto deberá ser capaz de adaptarse a múltiples plataformas e instancias dentro de la red protegida. Esto incluye los sistemas operativos, las máquinas y las configuraciones para la seguridad.

Características de Implantación al detalle

- El firewall debe ser capaz de aceptar una política de diseño, tomando en cuenta que debe permitir determinados servicios y aún así mantener un nivel de seguridad sano para la organización.

- El firewall debe aceptar la política de seguridad del administrador, no forzar una.

- El firewall debe ser flexible en el sentido que debe poder modularse para que se ajuste a las necesidades de la política de seguridad de la compañía y ser sensible a los cambios organizacionales.

- El firewall debe poseer medidas de autenticación avanzadas o debe ser expansible para acomodarse a estas autenticaciones en el futuro.

- El firewall debe emplear técnicas de filtrado que permitan o nieguen el permiso a servicios para sistemas de servidor específicos según se requiera.

- El lenguaje de filtrado IP debe ser flexible, amigable para programar y capaz de filtrar tantos atributos como sea posible, incluyendo las direcciones IP origen y destino, el tipo de protocolo, los puertos TCP/UDP origen y destino.

- El firewall debe adaptar el acceso público al sitio, de tal manera que los servidores de información pública puedan estar protegidos mediante el firewall, pero puedan estar separados de los sistemas del sitio que no requieren acceso público.

- El firewall debe poseer mecanismos para registrar el tráfico y la actividad sospechosa, y también debe contener mecanismos para la reducción de bitácora, siendo así legibles y comprensibles.

- El firewall debe desarrollarse de una manera tal que su solidez y exactitud puedan verificarse. Debe tener un diseño simple, para facilitar su comprensión y mantenimiento.

- El firewall y cualquier sistema operativo correspondiente debe actualizarse y mantenerse oportunamente con parches al sistema operativo y correcciones a errores de programación.

IV.2.- Solución de Seguridad Firewall

La propuesta de seguridad que se escogió como solución para este proyecto fue el firewall 3Com SuperStack 3.

El 3Com SuperStack 3 confiere seguridad a la red frente a accesos no autorizados y otras amenazas externas con origen en Internet. Esta solución de seguridad, homologada por los laboratorios ICSA, se configuró para detectar y repeler ataques de negación de servicio (DoS) y de negación distribuida de servicio (DDoS) por parte de hackers, incluyendo Ping of Death, SYN Flood, Land Attack e IP spoofing. Por su inspección completa de estado de paquetes, el firewall deniega cualquier intento no autorizado de acceder a la red y genera alertas e informes en tiempo real. Este dispositivo permite validar todo el tráfico entrante a la red privada LAN según las políticas definidas en el mismo. El equipo es un firewall dedicado del tipo Stateful Packet Inspection y consta de tres puertos Ethernet: WAN, DMZ y LAN de 10/100. El puerto WAN se utiliza para la conexión a Internet a través de un router. El puerto DMZ esta diseñado para conectar de manera segura los servicios y servidores públicos y el puerto LAN se utiliza para conectar la red privada a ser protegida. La conexión de los servidores públicos en la zona desmilitarizada DMZ del firewall permitirá aumentar la seguridad de la red privada LAN debido a que dichos equipos se encontrarán en una red físicamente distinta a la red privada y para su acceso desde Internet no es necesario accesar la red LAN. A su vez, el firewall permite accesar los servicios que se encuentran en la zona Desmilitarizada DMZ desde la red privada LAN.

Adicionalmente, el equipo permite implementar redes privadas virtuales VPN, lo que garantiza un acceso seguro a la LAN utilizando Internet como medio de comunicación. La transmisión desde el cliente VPN hasta la red privada se realiza de forma encriptada para evitar que terceros puedan descifrar la transmisión. Este equipo cuenta con un procesador especializado para el proceso de encriptación VPN, el cual aumenta el rendimiento de este tipo de tecnología.

Para ayudar a gestionar el uso de la red, el SuperStack 3 Firewall es capaz también de filtrar los URL por nombre de dominio o por palabras clave, bloquear el acceso dependiendo del momento del día y bloquear las puertas frente a troyanos, incluyendo cookies y applets Java y ActiveX. El filtro opcional de sitios Web para SuperStack 3 Firewall, por su parte, bloquea el acceso a cualquiera de sus 12 categorías de contenidos, incluyendo juegos de azar, pornografía o intolerancia racial. En esta opción se incluye la lista CyberNOT basada en suscripciones y notifica la recepción automática de las actualizaciones semanales.

Funciones Principales del Firewall 3Com SuperStack 3

- Seguridad firewall y DMZ
- Filtro de Web URL
- Logs y alertas
- Acceso remoto de usuarios
- Compartido automático de direcciones IP/configuración
- VPN de firewall

Características del firewall 3Com SuperStack 3

- *Alta Seguridad:* Provee a la LAN de la seguridad más avanzada, incluyendo la inspección completa de estado de paquetes para repeler automáticamente los ataques de hackers.

- *Altas Prestaciones y Disponibilidad:* Su procesador RISC y la tecnología Fast Ethernet de 3Com permiten caudales de 100 Mbps en todos los puertos.

- *Asequible:* Proporciona seguridad asequible y del máximo nivel, homologada por ICSA, así como soporte integrado basado en Internet para redes privadas virtuales (VPN).

- *Capacidad Integrada para VPN:* Su avanzada tecnología para VPN IPSec ofrece acceso escalable, rápido y seguro para sucursales, teletrabajadores, clientes, proveedores y socios, con un caudal de hasta 45 Mbps.

- *Filtrado Avanzado de Contenidos:* Permite establecer y aplicar políticas de acceso a Internet; filtra los URL en base al nombre de dominio o a palabras clave. El filtrado opcional le permite bloquear en función de la categoría de contenidos.

- *Facilidad de Uso:* La configuración del SuperStack 3 Firewall es fácil de manejar y viene con una preconfiguración de seguridad de alto nivel e interfaz basado en Web.

- Inspección y bloqueo del tráfico no deseado dentro y fuera de la red.

- Camuflaje de las direcciones internas del host IP frente a las redes externas.

- NAT seguro y NAT en la DMZ
- Alto desempeño.
- Administración remota basada en Web.
- Soporte para DHCP.
- El sistema de notificación envía una alerta en caso de ataques y suplantaciones.
- Inspección completa de estado en paquetes.
- NAT estático y dinámico.
- Soporte para DNS.
- El sistema operativo en tiempo real reforzado elimina los agujeros de seguridad del OS.
- El puerto DMZ proporciona un acceso seguro a servidores públicos.
- La interfaz gráfica de usuario basada en web y la ayuda en línea ayudan a simplificar la administración.
- La conectividad privada virtual basada en IPSec permite un acceso remoto seguro.
- El procesador de hardware especializado en encriptación VPN ayuda a incrementar el rendimiento.
- Técnicas VPN de encriptación ARC4 (56-bit), DES (56-bit), 3DES (168-bit).
- Uso de criptografía simétrica (la llave en ambos extremos del túnel VPN deben coincidir exactamente).

- Soporta exportación del registro de tráfico.
- Monitoreo SNMP

Especificaciones Técnicas

Interfaces

Tres puertos RJ-45: Ethernet/Fast Ethernet 10/100 BASE-T (WAN, LAN, y DMZ) con negociación automática de velocidad y modo duplex. Todos los puertos se pueden seleccionar como enlace cruzado o normal (MDI/MDIX). Viene con un conector para fuente de alimentación redundante Tipo 1.

Dimensiones y Peso

Ancho: 440 mm (17,3")
Fondo: 230 mm (9,0")
Altura: 44 mm (1,7")
Peso: 2,55 kg (5,6 libras)

Prestaciones:

Hasta 30.000 sesiones IP concurrentes
Hasta 1.000 túneles VPN concurrentes
100 Mbps de caudal en puertos de firewall
45 Mbps de caudal de cifrado VPN DES y 3DES
21 Mbps de caudal de cifrado VPN ARC4

Clientes VPN soportados: 64.000 simultáneos (modo de clave manual)

Sistema:

CPU: procesador StrongARM RISC a 233 MHz
RAM: 16 MB

Flash ROM: 4 MB
Aceleración: Crypto-procesador VPN
Reloj de tiempo real: batería de ión litio

Fiabilidad:

Tiempo Medio Entre Fallas (MTBF, MIL): 446.000
horas a 25º C/289.000 horas a 50º C

Requisitos Ambientales:

Temperatura de funcionamiento: de 0º a +50º C
(de 32º a 122º F)
Temperatura de almacenaje: de -10º a +70º C
Humedad: de 10 a 95% (sin condensación)

Alimentación:

Tensión de entrada: 90-264 VAC
Frecuencia de funcionamiento: 47-63 Hz

Indicadores LED:

Energía, alerta, indicación de velocidad Ethernet/enlace de puerto, actividad de puerto/configuración duplex.

Vista física del Firewall SuperStack 3

Figura IV.1: Panel frontal del Firewall 3Com

- Tres puertos Ethernet RJ-45 10/100 BASE-T
  - Puertos LAN, WAN y DMZ
  - Cable CAT-5, Conectores RJ-45
- Procesador 233 MHz StrongARM RISC
  - Para VPN hardware acceleration
- 16 MB RAM
- 4 MB Flash ROM
- Indicadores LED

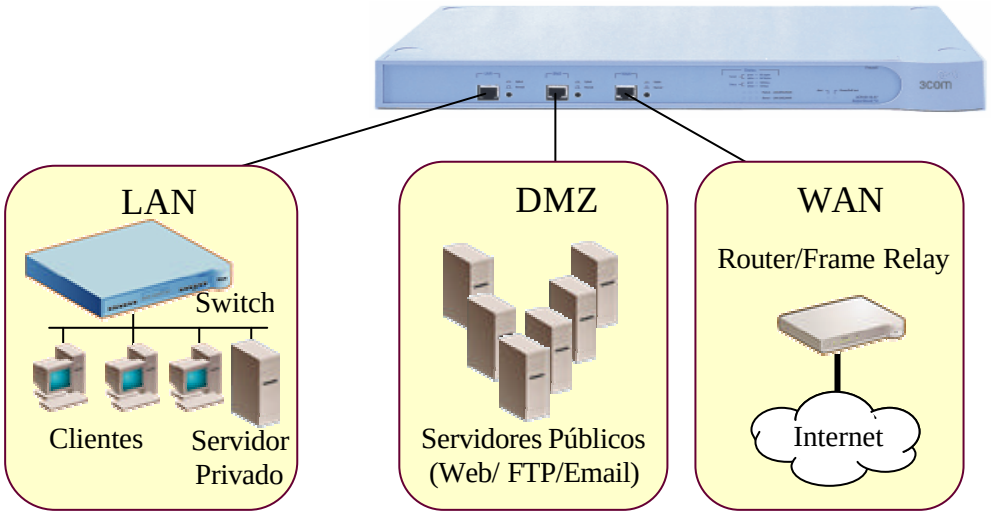


Figura IV.2: Funciones del panel frontal del Firewall 3Com

Figura IV.3: Indicadores LED del panel frontal

- **Status:** Indica la velocidad en que opera (10/100 Ethernet) cada puerto (LAN, WAN ó DMZ) hacia el dispositivo próximo en la red.
- **Packet:** Indica si el tráfico en cada puerto es transmitido en modo half-duplex ó full-duplex.
- **Power:** Indica que la unidad está en "On" ó si hay una falla con una unidad RPS conectada.
- **Alert:** Indica una falla en el auto-test, que el firmware no está cargado ó intentos de ataques a la red.

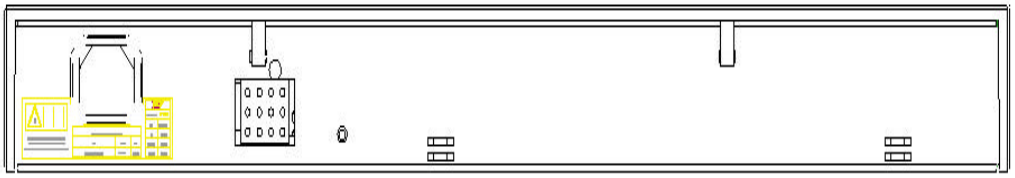


Figura IV.4: Panel posterior del Firewall 3Com

- Puerto de alimentación de poder.
- Switch de reset.
- Puerto redundante de alimentación de poder Tipo 1.

IV.3.- Diseño de la Solución

Tomando en cuenta bs problemas presentados en la situación actual y basado en los requerimientos planteados en el capitulo anterior, se elaboró el siguiente diseño para la nueva plataforma de acceso a Internet de la corporación.

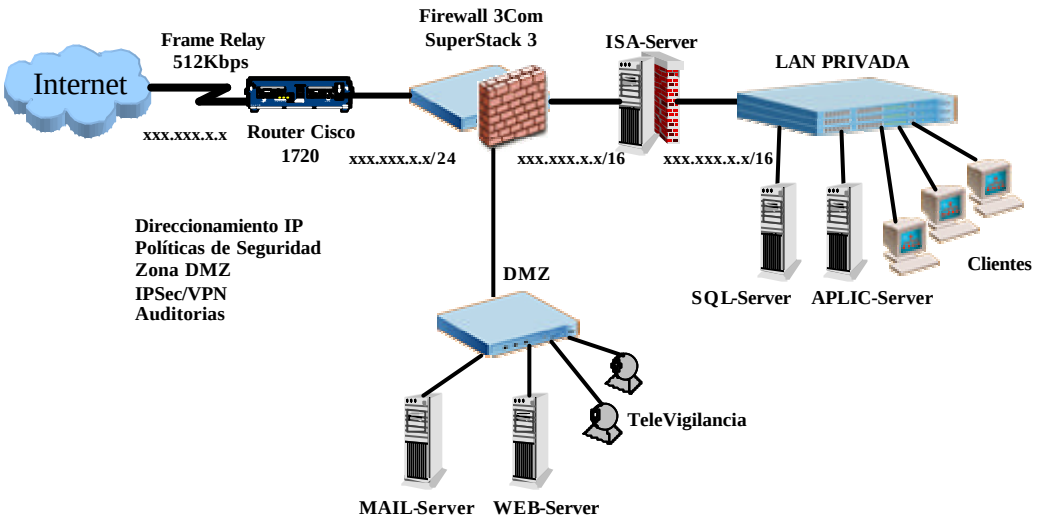


Figura IV.5: Diseño de la solución

IV.4.- Estrategia y Ejecución de la Solución

La ejecución del proyecto consistió en la puesta en marcha de una serie de pasos que para fines descriptivos y logísticos se clasificaron en siete fases principales:

1. Cambios y configuración del ISA-Server

2. Cambios y configuración del Mail-Server
3. Cambios y configuración del servicio Televigilancia
4. Cambios y configuración del router de Internet
5. Configuración del Firewall 3Com SuperStack 3
6. Configuración de las Redes Privadas Virtuales - VPN
7. Pruebas de los servicios

IV.4.1.- Cambios y configuración del ISA-Server

Para aumentar la seguridad de la red privada LAN fue necesario retirar el servidor de correo electrónico, MS Exchange Server 2000, y los servidores de Televigilancia de la LAN y ubicarlos dentro de la zona desmilitarizada DMZ del firewall 3Com SuperStack 3. Cabe resaltar que en dicha zona DMZ también serán agregados unos servidores Web nuevos con servicios adicionales descritos en el capítulo anterior. El principal cambio que generó este movimiento en la configuración del Internet Security and Acceleration Server (ISA-Server) fue la eliminación de la publicación del Mail-Server. Este proceso se realizó en el ISA Management, retirando las reglas de publicación Web y las reglas de publicación de servidores públicos. Los protocolos afectados fueron el Exchange RPC Server, NNTP Server, IMAP4 Server, POP3 Server y SMTP Server. El servicio OWA (Outlook Web Access) fue retirado también.

Adicionalmente en el ISA-Server se permitió el tráfico TCP/IP en ambos sentidos, (Inbound y Outbound) para todos los servicios implementados, únicamente desde la LAN hacia la zona DMZ del firewall. Para los usuarios de la red privada LAN, los servicios de la zona desmilitarizada se encuentran fuera de su rango de direcciones IP, en un segmento de red distinto, por lo cual se hizo necesario permitir el acceso desde el ISA-Server a los puertos TCP/IP que utilizan estas aplicaciones tanto en sentido entrante como en sentido saliente.

Los puertos TCP/IP utilizados por la aplicación MS Exchange Server 2000 son los siguientes:

80/tcp	HTTP World Wide Web Publishing Service
80/udp	HTTP World Wide Web Publishing Service
110/tcp	POP3 Post Office Protocol - Version 3
110/udp	POP3 Post Office Protocol - Version 3
25/tcp	SMTP Simple Mail Transfer Protocol
25/udp	SMTP Simple Mail Transfer Protocol
143/tcp	IMAP Interim Mail Access Protocol
143/udp	IMAP Interim Mail Access Protocol
993/tcp	IMAP over SSL Secure Sockets Layer
995/tcp	POP3 over SSL Secure Sockets Layer
135/tcp	RPC Remote Procedure Call
593/tcp	RPC Remote Procedure Call over HTTP
119/tcp	NNTP Network News Transfer Protocol
119/udp	NNTP Network News Transfer Protocol

Los servidores de Televigilancia utilizan los puertos 2500, 2501, 2502 y 2503 para su funcionamiento. El servidor 1 utiliza el puerto 2500 para el browser y el puerto 2501 para la salida de video; el servidor 2 utiliza el puerto 2502 para el browser y el puerto 2503 para la salida de video.

Estos cambios se realizaron en el ISA Management a través del Access Policy configurando las reglas de protocolos. Dicha configuración en el ISA-Server quedó de la siguiente manera:

#	Acción	Servicio	Puerto	Destino
1	Permitir	Send Email (SMTP)	25	Inbound-Outbound
2	Permitir	Retrieve Email (POP3)	110	Inbound-Outbound

3	Permitir	IMAP4	143	Inbound-Outbound
4	Permitir	IMAP over SSL	993	Inbound-Outbound
5	Permitir	POP3 over SSL	995	Inbound-Outbound
6	Permitir	Web (HTTP)	80	Inbound-Outbound
7	Permitir	RPC	135	Inbound-Outbound
8	Permitir	RPC over HTTP	593	Inbound-Outbound
9	Permitir	NNTP	119	Inbound-Outbound
10	Permitir	TeleServer1	2500	Inbound-Outbound
11	Permitir	TeleServer1	2501	Inbound-Outbound
12	Permitir	TeleServer2	2502	Inbound-Outbound
13	Permitir	TeleServer2	2503	Inbound-Outbound

Cuadro IV.1: Reglas de protocolos del ISA-Server

El Internet Security and Acceleration 2000 Server en su nueva configuración tendrá como función principal un segundo nivel de seguridad como firewall, manteniendo sus otras políticas de seguridad descritas en el capítulo anterior.

IV.4.2.- Cambios y configuración del Mail-Server

Como se explicó anteriormente el Mail-Server, MS Exchange Server 2000, es un equipo público que debe ser accesado desde Internet a través del servicio OWA, igualmente debe ser accesado desde la red privada LAN para suministrar todos los servicios relacionados con el correo electrónico. El Mail-Server se encontraba publicado en Internet por medio del ISA-Server; dicho equipo se pasó desde la red privada hacia la zona desmilitarizada DMZ para obtener mayor seguridad. Esto implicó un cambio a nivel de las direcciones IP del equipo ya que el mismo fue cambiado a un segmento de red distinto perteneciente a la zona desmilitarizada DMZ.

El siguiente cuadro muestra los cambios de las direccionamiento IP en el Mail-Server.

Direccionamiento IP	Dirección Anterior	Dirección Nueva
Dirección IP:	XXX.XX.X.X	XXX.XXX.XXX.XX
Mascara:	255.255.0.0	255.255.255.0
Default Gateway:	XXX.XX.X.X	XXX.XXX.XXX.X
DNS Primario:	XXX.XX.X.X	XXX.XX.XX.XX
DNS Secundario:	XXX.XX.X.X	XXX.XX.XX.XX

Cuadro IV.2: Direccionamiento IP del Mail-Sever

Adicional a los cambios de direccionamiento IP se eliminaron algunos servicios no relacionados con el correo electrónico que prestaba el equipo Mail-Server dentro de la red privada LAN. Dicho equipo actuaba como Remote Access Server; este servicio fue eliminado del Mail-Server e instalado en el servidor de aplicaciones, APPLIC-Server. De igual manera el Mail-Server actuaba como Servidor DNS secundario para la red privada; este servicio fue eliminado del Mail-Server, convirtiendo al servidor SQL-Server en Servidor DNS Secundario. El Mail-Server también funcionaba como DHCP Server, el cual fue migrado hacia el servidor de aplicaciones, APPLIC-Server.

En su actualidad el Mail-Server se encontraba configurado como un Domain Controller secundario; el mismo fue degradado a Member Server ya que un servidor público no debe contener información del Active Directory por razones de seguridad. Este cambio no afectó a la estructura de la red debido a que existe otro servidor que funciona como Domain Controller secundario.

Otro cambio realizado en el Mail-Server fue la forma de conectarse a Internet; el mismo utilizaba el ISA-Sever para dicha conexión. Ahora con su ubicación en la zona desmilitarizada DMZ, la dirección IP del ISA-Server le es desconocida, por lo que le fue deshabilitada la configuración proxy del Explorador de Internet para que use su default gateway y poder tener conexión a Internet, permitiendo la salida de los correos hacia el exterior.

IV.4.3.- Cambios y configuración del servicio Televigilancia

Los dos servidores de Televigilancia fueron desconectados de la red privada LAN y colocados en la zona desmilitarizada DMZ del Firewall 3Com. Sus direcciones IP privadas fueron cambiadas al rango de la red de la zona desmilitarizadas.

Los cambios en el direccionamiento IP fueron los siguientes:

Direccionamiento IP	Anterior	Nueva	IP Válida
TeleServer1	XXX.XX.X.XX	XXX.XXX.XXX.XX	XXX.XX.XXX.XX
TeleServer2	XXX.XX.X.XX	XXX.XXX.XXX.XX	XXX.XX.XXX.XX

Cuadro IV.3: Direccionamiento IP de Televigilancia

IV.4.4.- Cambios y configuración del Router de Internet

El Router de conexión a Internet es un equipo Cisco 1720 el cual tiene una conexión serial con el proveedor de servicios CANTV y una conexión LAN hacia la red privada.

Los cambios de configuración que se realizaron en este equipo se deben fundamentalmente a dos razones. La primera es un cambio en la dirección IP del puerto LAN del router debido a que se generó una nueva red IP entre el puerto WAN del firewall y el puerto LAN del router, utilizando las siguientes direcciones IP válidas: XXX.XX.XXX.XX para el puerto LAN del router y XXX.XX.XXX.XX para el puerto WAN del firewall. La segunda razón se debe a cambios en la configuración

NAT (Network Address Translation): el router tenía la función de NAT dinámico (many to one) para que los usuarios de la red privada LAN pudieran navegar en Internet. Este proceso convierte cualquier dirección IP privada de los usuarios internos de la LAN en una única dirección IP válida. El router convertía las direcciones IP internas de los segmentos XXX.XXX.0.0 y XXX.XX.0.0 en la dirección IP XXX.XX.XXX.XX válida para la navegación. Este rol lo asume ahora el firewall 3COM en la nueva estructura de red, por lo que se eliminó esta función del router.

Adicionalmente se realizaron otros cambios a nivel de configuración NAT en el router. Este equipo convertía mediante NAT estático (one to one) direcciones IP válidas a direcciones internas de la red privada utilizadas por los servidores públicos para su acceso desde Internet. El servidor de correo electrónico utiliza la siguiente dirección IP válida en Internet XXX.XX.XXX.XX. Esta dirección se convertía en la dirección IP privada XXX.XXX.X.X, que es la dirección de la tarjeta externa del ISA Server, la cual permitía publicar el Mail-Server. En la nueva estructura de la red, el firewall 3Com se encarga de realizar el NAT estático, razón por la cual se eliminó esta configuración del router.

El cambio en el direccionamiento IP del Puerto LAN del router fue el siguiente:

Direccionamiento IP	**Anterior**	**Nueva**
Dirección IP:	XXX.XXX.X.X	XXX.XX.XXX.XX
Mascara:	255.255.0.0	255.255.255.248

Cuadro IV.4: Direccionamiento IP puerto LAN router

Configuración Anterior del Router Cisco 1720

```
Current configuration: 1820 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname XXXXX
!
logging buffered 12000 debugging
enable secret 5 $1$W3Vd$cI6m8AmN1b5QDQfmmx9K70
enable password XXXXX
!
memory-size iomem 25
ip subnet-zero
ip name-server XXX.XX.XX.XX
ip name-server XXX.XX.XX.XX
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
!
!
interface FastEthernet0
 ip address XXX.XXX.X.X 255.255.0.0
 ip nat inside
 speed auto
!
interface Serial0
 no ip address
 encapsulation frame-relay
 no fair-queue
 frame-relay traffic-shaping
 frame-relay lmi-type ansi
!
interface Serial0.219 point-to-point
 description Conexion a INTERNET (CANTV) Circuito XXXXX
 ip address XXX.XX.XXX.XXX  255.255.255.252
 ip nat outside
 frame-relay interface-dlci 219
  class enlace
```

```
!
ip nat pool internet xxx.xx.xxx.xx  xxx.xx.xxx.xx netmask 255.255.255.248
ip nat inside source list 101 pool internet overload
ip nat inside source static XXX.XX.X.XX XXX.XX.XXX.XX
ip nat inside source static XXX.XX.X.XX XXX.XX.XXX.XX
ip nat inside source static XXX.XXX.X.X XXX.XX.XXX.XX
ip nat inside source static XXX.XX.X.X XXX.XX.XXX.X
ip classless
ip route 0.0.0.0 0.0.0.0 XXX.XX.XXX.XXX
ip route XXX.XXX.X.X 255.255.255.0 XXX.XXX.X.X
ip route XXX.XX.X.X 255.255.0.0 XXX.XX.X.X
no ip http server
ip pim bidir-enable
!
!
map-class frame-relay enlace
 frame-relay cir 512000
 frame-relay bc 5120
 frame-relay be 0
 frame-relay mincir 512000
 no frame-relay adaptive-shaping
access-list 101 permit ip XXX.XX.X.X 0.0.255.255 any
access-list 101 permit ip XXX.XX.X.X 0.0.255.255 any
access-list 101 permit ip XXX.XX.X.X 0.0.255.255 any
access-list 101 permit ip XXX.XX.X.X 0.0.255.255 any
snmp-server community XXXXXX XX
!
line con 0
line aux 0
line vty 0 4
 password XXXXXXXXXX
 login
!
end
```

Configuración Actual del Router Cisco 1720

```
Current configuration: 1747 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
```

```
no service password-encryption
!
hostname XXXXX
!
logging buffered 12000 debugging
enable secret 5 $1$W3Vd$cI6m8AmN1b5QDQfmmx9K70
enable password XXXXX
!
memory-size iomem 25
ip subnet-zero
ip name-server XXX.XX.XX.XX
ip name-server XXX.XX.XX.XX
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
!
!
interface FastEthernet0
 ip address XXX.XX.XXX.XX 255.255.255.248
 ip nat inside
 speed auto
!
interface Serial0
 no ip address
 encapsulation frame-relay
 no fair-queue
 frame-relay traffic-shaping
 frame-relay lmi-type ansi
!
interface Serial0.219 point-to-point
 description Conexion a INTERNET (CANTV) Circuito XXXXXX
 ip address XXX.XX.XXX.XXX  XXX.XXX.XXX.XXX
 ip nat outside
 frame-relay interface-dlci 219
  class enlace
!
ip classless
ip route 0.0.0.0 0.0.0.0 XXX.XX.XXX.XXX
ip route XXX.XXX.X.0 255.255.255.0  XXX.XXX.X.X
ip route XXX.XX.0.0 255.255.0.0  XXX.XX.X.X
no ip http server
ip pim bidir-enable
!
```

```
!
map-class frame-relay enlace
 frame-relay cir 512000
 frame-relay bc 5120
 frame-relay be 0
 frame-relay mincir 512000
 no frame-relay adaptive-shaping
access-list 101 permit ip XXX.XXX.X.X 0.0.255.255 any
access-list 101 permit ip XXX.XX.X.X 0.0.255.255 any
access-list 101 permit ip XXX.XX.X.X 0.0.255.255 any
access-list 101 permit ip XXX.XX.X.X 0.0.255.255 any
snmp-server community XXXXXXX
!
line con 0
line aux 0
line vty 0 4
 password XXXXXXXX
 login
!
end
```

IV.4.5.- Configuración del Firewall 3Com SuperStack 3

La configuración del firewall 3com SuperStack 3 está basada en la protección de los recursos informáticos de la empresa contra intrusos provenientes de Internet. Por defecto el firewall bloquea todo el tráfico proveniente de Internet hacia el puerto LAN y sólo permite el tráfico Web hacia la DMZ. En sentido contrario permite todo el tráfico desde la LAN hacia la WAN y la DMZ.

A dicho firewall le fue asignada la dirección IP XXX.XXX.X.X /16 en el puerto LAN, lo que facilita su administración desde cualquier explorador HTTP. El nombre de usuario y la contraseña que le fueron asignados para efecto de su administración son los siguientes:

Username: XXXXXXXX

Password: XXXXXXXX

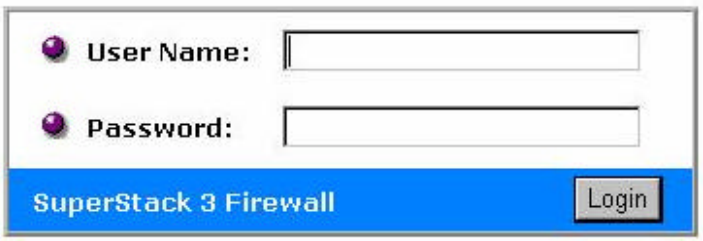


Figura IV.6: Conexión al firewall 3Com SuperStack 3

Configuración Network

La configuración Network del equipo incluye direcciones IP y el modo de direccionamiento de la red. El modo de direccionamiento de la red utilizado en el firewall 3Com es el modo NAT Enabled, el cual permite implementar un NAT dinámico (many to one) y utilizar una única dirección IP para navegar en Internet. Esta configuración permite asumir la función de NAT dinámico que anteriormente cumplía el router Cisco. La dirección IP válida utilizada para navegar en Internet es la XXX.XX.XXX.XX. Esta última es la dirección IP asignada al puerto WAN del firewall y es la que utiliza el firewall para generar el NAT dinámico. La puerta de enlace del firewall (Default Gateway) hacia Internet es el puerto LAN del router Cisco cuya dirección IP es la XXX.XX.XXX.XX.

Network Addressing Mode (Modo de Direccionamiento de la Red): **NAT Enabled:**

LAN IP Address: **XXX.XXX.X.X/16 (Dirección IP Puerto LAN)**
Lan Subnet Mask: **255.255.0.0 (Sub-mascara Puerto LAN)**
WAN Gateway: **XXX.XX.XXX.XX (Puerta de enlace)**
WAN IP Address: **XXX.XX.XXX.XX (Dirección IP Puerto WAN)**

A continuación una vista de la pantalla donde se realizó dicha configuración.

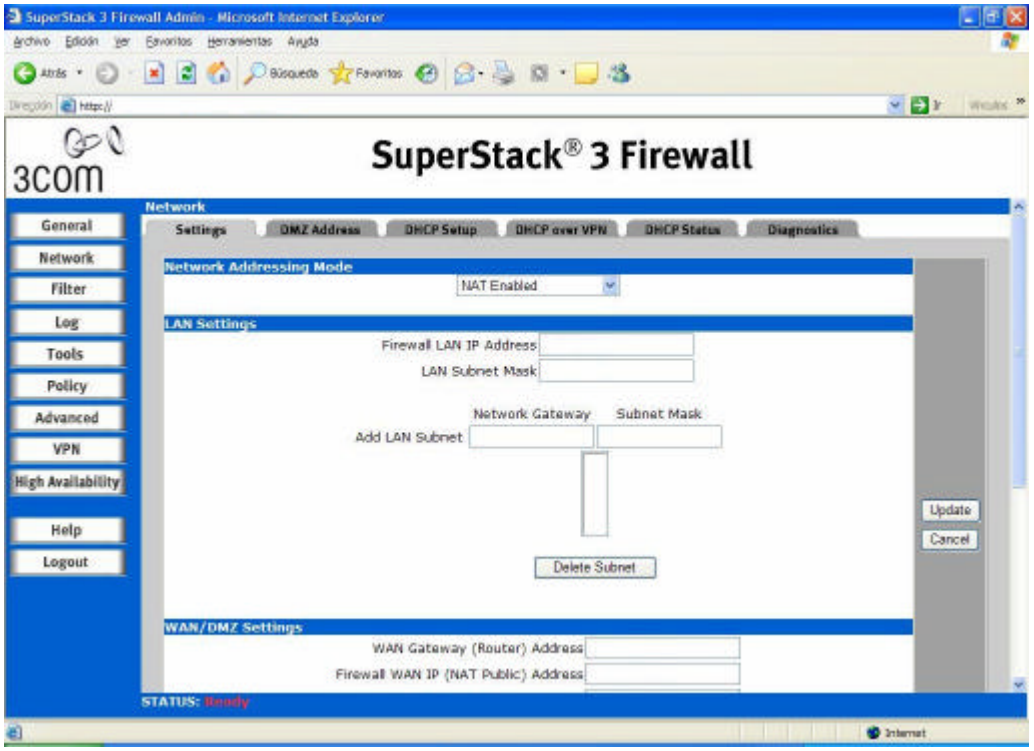


Figura IV.7: Modo NAT enabled en Firewall 3Com

La zona desmilitarizada DMZ se configuro en el modo NAT con la finalidad de aumentar el grado de seguridad de los equipos publicados en esta red. El segmento de red asignado a esta la zona es el XXX.XXX.XXX.0 255.255.255.0 y los equipos configurados aquí son el servidor de correo electrónico, los servidores de Tele vigilancia y el servidor Web. Mediante el NAT estático se ocultaron las direcciones IP válidas de dichos equipos como se muestra a continuación.

NAT estático configurado en el puerto DMZ del firewall 3Com:

Dirección IP Válida	Dirección IP Privada	Equipos Públicos
XXX.XX.XXX.XX	XXX.XXX.XXX.XX	TeleServer1
XXX.XX.XXX.XX	XXX.XXX.XXX.XX	TeleServer2
XXX.XX.XXX.XX	XXX.XXX.XXX.XX	Mail-Server
XXX.XX.XXX.X	XXX.XXX.XXX.X	Web-Server

Cuadro IV.5: NAT estático en la DMZ

A continuación una vista de las pantallas donde se realizó dicha configuración.

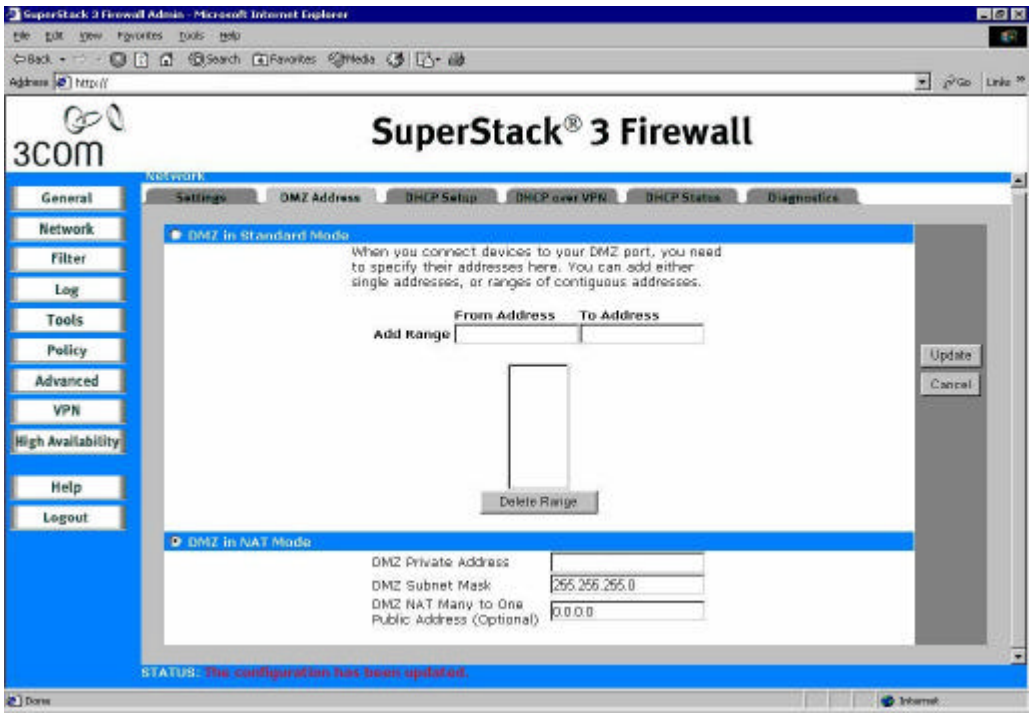


Figura IV.8: Modo NAT en la DMZ

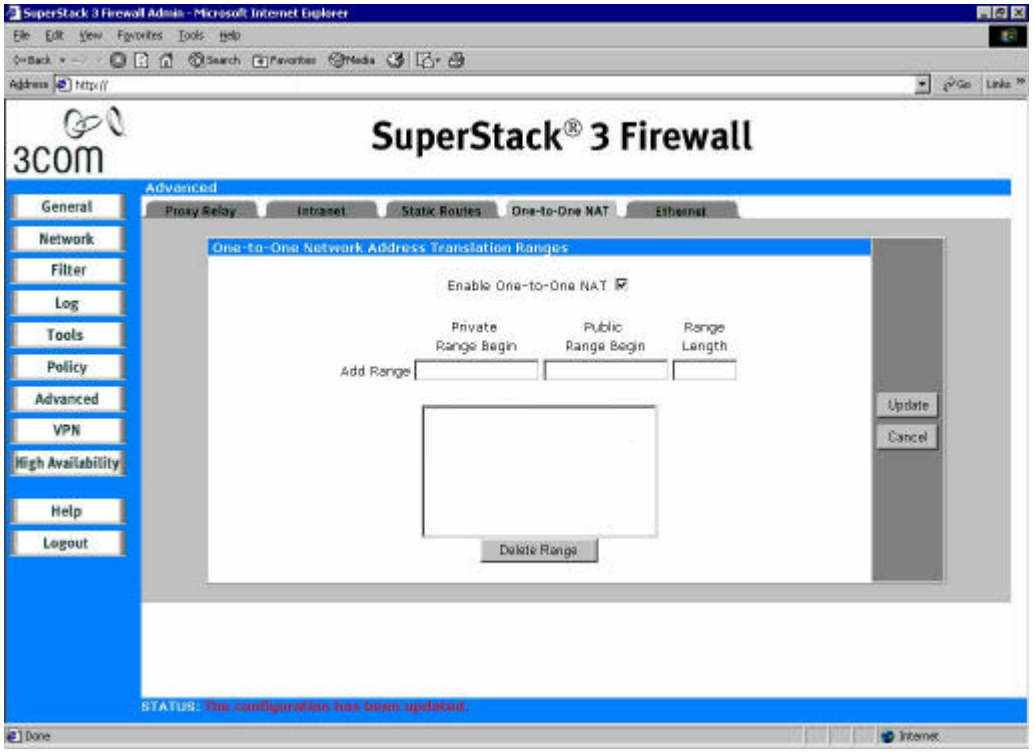


Figura IV.9: NAT estático en la DMZ

Configuración de filtrado Web

Para el caso del Firewall 3Com no se configuró ningún tipo de filtrado Web debido a que esta función la lleva a cabo en su totalidad el ISA-Server. En este sentido se permite cualquier tipo de acceso a la Web ya que el mismo viene filtrado desde el ISA-Server.

Configuración de Políticas

Las políticas configuradas en el firewall 3Com definen cuales servicios de red son bloqueados y cuales servicios son autorizados por el equipo; esto permite regular el tráfico TCP/IP a través de los diferentes puertos del firewall. Como se comentó anteriormente, el firewall en su configuración por defecto bloquea todo el tráfico TCP/IP en sentido entrante (desde la WAN hacia la LAN, desde la DMZ hacia la LAN, y desde la WAN a la DMZ) y permite todo el tráfico TCP/IP en sentido saliente (desde la LAN hacia la WAN y desde la LAN hacia la DMZ). Esto se logra mediante políticas generales definidas en la sección "Network Policy Rules". El servicio "Default" asume todos los puertos TCP/IP, mientras que "*" implica cualquier puerto, bien sea TCP/IP o puerto Ethernet del Firewall.

Las políticas generales del Firewall 3Com se resumen a continuación:

#	Acción	Servicio	Puerto	Origen	Destino
1	Negar	Default	*	*	LAN
2	Permitir	Default	*	LAN	*
3	Negar	Default	*	WAN	DMZ
4	Permitir	Default	*	DMZ	WAN

Cuadro IV.6: Políticas generales del firewall 3Com

Dependiendo de las aplicaciones de red que sean necesarias implementar, se autoriza o se niega un determinado servicio (puertos TCP/IP) entre dos diferentes puertos del firewall. Esto permite controlar el tráfico entre los puertos del equipo de una forma segura evitando posibles puntos de acceso a la red innecesarios, los cuales son utilizados por hackers para efectuar ataques a la red privada LAN. Al realizar este tipo de configuración hay que tener sumo cuidado de cuales servicios se permiten y

cuales se bloquean, ya que una mala configuración puede permitir vulnerar la seguridad de la red privada o bloquear por completo el acceso a Internet.

En este sentido, las aplicaciones principales tomadas en cuenta para la configuración del Firewall 3Com son: el servicio de correo electrónico MS Exchange Server 2000, el servicio de Televigilancia, el servicio VPN y los servicios prestados por el servidor Web.

Debido a que el Mail-Server se instaló en la zona desmilitarizada DMZ fue necesario permitir el tráfico TCP/IP utilizado por la aplicación Exchange 2000 en sentido entrante WAN-DMZ; esto con la finalidad de que el servidor de correo pueda ser accesado por los usuarios remotos a través de Internet usando el OWA (Outlook Web Access). En sentido saliente LAN-DMZ no fue necesario realizar cambios en la configuración debido a que la política por defecto permite todo tráfico TCP/IP de la LAN hacia la DMZ.

Los puertos TCP/IP utilizados por la aplicación Microsoft Exchange Server 2000 son los siguientes:

80/tcp	World Wide Web HTTP
80/udp	World Wide Web HTTP
110/tcp	POP3 Post Office Protocol - Version 3
110/udp	POP3 Post Office Protocol - Version 3
25/tcp	SMTP Simple Mail Transfer
25/udp	SMTP Simple Mail Transfer
143/tcp	IMAP Interim Mail Access Protocol
143/udp	IMAP Interim Mail Access Protocol
993/tcp	IMAP over SSL Secure Sockets Layer
995/tcp	POP3 over SSL Secure Sockets Layer
135/tcp	RPC Remote Procedure Call

593/tcp RPC over HTTP

119/tcp NNTP Network News Transfer Protocol

119/udp NNTP Network News Transfer Protocol

La configuración de las políticas en el firewall 3Com para el acceso al servidor de correo electrónico se resume a continuación:

#	Acción	Servicio	Puerto	Origen	Destino
1	Permitir	Send Email (SMTP)	25	WAN	DMZ
2	Permitir	Retrieve Email (POP3)	110	WAN	DMZ
3	Permitir	IMAP4	143	WAN	DMZ
4	Permitir	IMAP over SSL	993	WAN	DMZ
5	Permitir	POP3 over SSL	995	WAN	DMZ
6	Permitir	Web (HTTP)	80	WAN	DMZ
7	Permitir	RPC	135	WAN	DMZ
8	Permitir	RPC over http	593	WAN	DMZ
9	Permitir	NNTP	119	WAN	DMZ

Cuadro IV.7: Políticas de los servicios del correo electrónico en el firewall 3Com

Los servidores de Televigilancia también fueron colocados en la zona desmilitarizada DMZ. Estos utilizan los puertos 2500, 2501, 2502 y 2503 para su funcionamiento. El servidor 1 utiliza el puerto 2500 para ser accedido vía browser y el puerto 2501 para la salida de video. El servidor 2 utiliza el puerto 2502 para ser accedido también vía browser y el puerto 2503 para la salida de video. Estos puertos fueron configurados en el Firewall en la sección "Add Service". Los nombres asignados a dichos servicios fueron los siguientes:

Puertos 2500 – 2501 TeleServer1

Puertos 2502 - 2503 TeleServer2

Para permitir el acceso y la salida de video de los servicios de Televigilancia se configuraron dichos puertos en ambos sentidos entrante y saliente, desde la WAN a la DMZ y desde la LAN a la DMZ.

La configuración de las políticas en el firewall para el acceso a los servidores de Televigilancia quedó de la siguiente manera:

#	Acción	Servicio	Puerto	Origen	Destino
1	Permitir	TeleServer1	2500-2501	WAN	DMZ
2	Permitir	TeleServer1	2500-2501	DMZ	LAN
3	Permitir	TeleServer2	2502-2503	WAN	DMZ
4	Permitir	TeleServer2	2502-2503	DMZ	LAN

Cuadro IV.8: Políticas de los servicios de Televigilancia en el firewall 3Com

También fueron configuradas en el firewall las políticas de las redes virtuales privadas VPN. Para implementar las redes virtuales privadas VPN fue necesario permitir el servicio Key Exchange (IKE) desde la WAN hacia la LAN.

Las políticas quedaron configuradas de la siguiente forma:

#	Acción	Servicio	Puerto	Origen	Destino
1	Permitir	HTTPS Management	*	LAN	XXX.XXX.X.X
2	Permitir	Key Exchange (IKE)	*	WAN	XXX.XXX.X.X

Cuadro IV.9: Politicas VPN en el firewall 3Com

Una vez definidos los permisos de los servicios de los puertos TCP y UDP que conforman el tráfico entre los puertos del firewall se procedió a habilitar el tráfico Netbios desde la LAN hacia la DMZ en la sección de servicios de las políticas del firewall.

Windows Networking (NetBIOS) Broadcast Passthrough from LAN to DMZ: Permite el tráfico Netbios desde la LAN hacia la DMZ, dejando que maquinas de la LAN puedan ver en el entorno de red de Microsoft los equipos conectados en la DMZ.

IV.4.6.- Configuración de la Redes Privadas Virtuales - VPN

La configuración VPN se implementó para crear túneles VPN desde los usuarios remotos "Clientes VPN" hacia el firewall 3Com. El elemento que inicia la transmisión cifra los datos para que estos sean transmitidos de forma encriptada, el receptor los descifra mediante el uso de una llave que también es transmitida de forma segura. Para este procedimiento se utilizó el grupo de protocolos de seguridad IPsec (Internet Protocol Security).

Los clientes VPN pueden ser básicamente de 3 tipos: Clientes Windows XP, clientes Windows 2000 y clientes Windows NT4, 98 y Me. Los clientes Windows XP utilizan el protocolo nativo de Microsoft con seguridad L2TP/IPsec para generar el túnel VPN. Los clientes Windows 2000 utilizan por defecto la tecnología L2TP sin IPSec, aunque pueden utilizar IPSec solo ó L2TP/Ipsec con la instalación de un parche. Los clientes NT4, 98 y Me pueden utilizar la tecnología L2TP/IPsec o IPSec únicamente.

La empresa 3COM recomienda que para los clientes NT4, 98 y Me se genere el túnel VPN utilizando el software Safenet Soft-PK VPN client, incluido en el CD del Firewall 3 Com, que utiliza la tecnología IPSec únicamente. Por otra parte

recomienda que los clientes Windows 2000 generen el túnel VPN utilizando el protocolo L2TP/IPsec nativo de Microsoft con la instalación de un parche. Para los clientes Windows XP se genera el túnel VPN con el protocolo nativo L2TP/IPSec.

Configuración para clientes VPN Windows XP L2TP/IPSec

Para generar el túnel VPN entre el cliente Windows XP y el Firewall 3Com fue necesario crear una asociación de seguridad en el Firewall del tipo "Group VPN Security Association". Este tipo de asociación de seguridad se utilizó igualmente para clientes IPSec únicamente.

El protocolo para generar las llaves de seguridad IPSec se configuró en el modo IKE (Internet Key exchange) pre-shared secret.

El proceso de encriptación y autenticación se realiza utilizando una de las siguientes tecnologías:

DES & MD5 (menor seguridad mayor velocidad de respuesta)
DES & SHA1
3DES & MD5
3DES & SHA1 (mayor seguridad menor velocidad de respuesta)

3COM recomienda utilizar los métodos DES & SHA1 y 3DES & SHA1. Se escogió el método DES & SHA1 ya que ofrece una seguridad intermedia y una velocidad de red aceptable. Este método de encriptación y autenticación fue el que se configuró en el firewall. Adicionalmente se definió un tiempo de vida para la asociación de seguridad del túnel VPN. Este parámetro se dejó en su valor por defecto 28800 segundos 8 horas; luego de transcurrido este tiempo se debe generar una nueva asociación de seguridad. Otro parámetro que se configuró para la asociación de seguridad fue el "shared secret", el cual es utilizado por el método de encriptación

para ocultar la transmisión que se realiza en el túnel VPN. El shared secret puede ser un campo alfanumérico de 4 a 128 caracteres; se debe tomar la precaución de no divulgar dicho valor ya que puede comprometer la seguridad del túnel VPN.

La autenticación del usuario es obligatoria para los clientes L2TP/IPSec. Los clientes L2TP/IPSec envían una cuenta de usuario y un password al iniciarse el túnel VPN para poder conectarse al Firewall. La cuenta de usuario y el password deben ser configuradas para cada usuario localmente en el firewall o seleccionando un servidor RADIUS que permita efectuar la autenticación. Para unir el Active Directory de Windows con la autenticación del firewall se puede configurar el servicio (IAS) Internet Authentication Services de Microsoft; este sería el servidor RADIUS de Windows.

Inicialmente se configuraron los usuarios VPN directamente en el firewall utilizando la sección de "User Privileges" en las políticas del firewall. Para cada cliente se configuró una cuenta de usuario y el password, y se habilitó la opción "Access from L2TP VPN Client". Se recomienda implementar el servidor RADIUS acoplando el Active Directory de Windows con el firewall.

Para la configuración del direccionamiento IP del túnel VPN se utilizó la sección de L2TP Server en la interfaz administrativa del firewall. A cada usuario que se conecta remotamente a la red privada por un túnel VPN se le asigna una dirección IP mediante el servidor L2TP. En primer lugar se habilitó el Servidor L2TP, *Enable L2TP Server*. Las direcciones IP pueden ser asignadas directamente por un pool de direcciones configuradas en el servidor L2TP o por el servidor RADIUS; se utilizó un pool local de direcciones IP del servidor L2TP, desde la dirección XXX.XXX.X.11 hasta la XXX.XXX.X.200.

Para la configuración del equipo cliente VPN Windows XP se corrió el Wizard de nuevas conexiones de red en el panel de control del sistema operativo. Se seleccionó

la opción "conexión a mi lugar de trabajo" a través de VPN y se le colocó un nombre a dicha conexión. Luego, en las propiedades del icono de la conexión creada, en la sección de seguridad, se escogió "IPSec settings" y se colocó el "shared secret" configurado previamente en el firewall 3Com. Para finalizar la configuración se seleccionó el tipo de túnel VPN en la sección de "redes": L2TP/IPSec VPN.

Configuración para clientes Windows NT4, 98 y Me IPSec

Para los clientes que utilizan el protocolo IPSec únicamente, la configuración del firewall 3Com es exactamente la misma que para los clientes L2TP/IPSec, con la excepción de la opción "L2TP Server". Se configuró la asociación de seguridad del tipo "Group VPN" y se seleccionó el modo IKE pre-shared secret para generar la llave de seguridad (IPSec Keying mode). También se configuró el mismo modo de encriptación y autenticación DES & SHA1 y se colocó el shared secret para ocultar por medio de la encriptación la transmisión por el túnel VPN. Para este tipo de cliente se permite exportar un archivo con los valores de la configuración a ser utilizados en la instalación y la configuración del cliente. A diferencia de la configuración del cliente L2TP/IPSec de Windows XP, la autenticación del usuario no es obligatoria en IPSec.

Para configurar el cliente IPSec se utilizó el programa Setup.exe ubicado en el subdirectorio VPN Client del CD mencionado anteriormente. Este producto no requiere llave de instalación ya que es una licencia ilimitada de clientes VPN. Para finalizar la instalación se usó el archivo exportado en la configuración del firewall.

IV.4.7.- Pruebas de los servicios

Se realizaron las pruebas necesarias para verificar que todos los servicios involucrados en el proceso de la implantación de la nueva plataforma de seguridad estuvieran operando satisfactoriamente. Entre las pruebas de funcionalidad se tienen las siguientes:

	Prueba	Propósito
	Correo Electrónico	Verificación de los protocolos POP3 y SMTP, mediante la entrada y salida de los correos desde y hacia Internet.
	Internet	Verificación del acceso correcto de Internet.
	OWA	Verificación del acceso al servicio Outlook Web Access.
	VPN	Pruebas de conexión mediante las redes privadas virtuales. Adición y eliminación de usuarios autorizados.
	TeleVigilancia	Verificación del correcto funcionamiento del servicio de Tele vigilancia.
	Reglas de Protocolos	Demostración del funcionamiento correcto de las reglas configuradas. Demostración de cambios en la configuración mediante la adición, eliminación y modificación de las reglas.
	Tráfico	Verificación del registro de tráfico en los archivos logs (paquetes rechazados y no rechazado).
	Autenticación	Demostración de autenticación rechazada y autorizada y su notificación.
	Direccionamiento IP	Verificación de la comunicación entre los segmentos de redes diferentes LAN, DMZ y WAN.
	DNS	Verificación del correcto funcionamiento del servicio DNS.
	DHCP	Verificación del correcto funcionamiento del servicio DHCP.
	Notificaciones	Verificación de las notificaciones vía e-mail.

Cuadro IV.10: Pruebas de funcionalidad de los servicios

CONCLUSIONES

La seguridad en el acceso a Internet se ha convertido en un tema prioritario y de actualidad para muchas empresas ya que involucra el uso de nuevas plataformas tecnológicas con la inversión de gran cantidad de dinero, todo con un mismo fin, proteger la integridad, autenticidad y confidencialidad de la información. Esta inversión en la adquisición y actualización de nuevas tecnologías debe ser considerada como un patrón fundamental en el momento de definir un plan estratégico de seguridad.

La implantación de una plataforma de seguridad para el acceso a Internet en la empresa estudiada en este Trabajo de Grado ha permitido brindar una conexión a Internet más sólida y eficiente con un intercambio de información confiable y seguro. Esto radica fundamentalmente en la instalación y configuración de un equipo firewall avanzado y a la definición de políticas de seguridad ajustadas a los requerimientos de la organización.

Esta nueva plataforma se ha convertido en el centro neurálgico de comunicación de toda la información que entra y sale de Internet, de allí radica su gran importancia ya que cuenta con un dispositivo de última generación que no sólo es capaz de ofrecer seguridad y confiabilidad sino que permite expandir la infraestructura tecnológica y soportar nuevas tecnologías en el campo de las redes de datos.

En la evaluación y selección del equipo firewall y su incorporación como sistema de seguridad en la red de datos de la empresa, es importante destacar varios aspectos y criterios que se tomaron en cuenta, partiendo como base las necesidades de la organización. Los costos de adquisición, las características de seguridad, las características de implantación y las bondades tecnológicas pueden mencionarse entre los aspectos más resaltantes. Muchas empresas colocan como factor principal los

costos pero estos se encuentran estrechamente relacionados con los beneficios y las bondades tecnológicas del equipo firewall; en el presente proyecto no se planteó de esta manera, ya que no se escatimaron esfuerzos en los costos de adquisición, prevaleciendo las características de seguridad, de implantación y las bondades tecnológicas como primeras opciones.

Adicionalmente a la seguridad y a las políticas implementadas cabe destacar el estudio y configuración de las VPN utilizando como medio de comunicación la conexión a Internet, ofreciendo la gran ventaja de permitirles a los usuarios una conexión segura y estable a través de un túnel en donde la información viajará encriptada entre la red privada interna y la red pública (Internet).

Se puede concluir que la seguridad de una red no se basa en una única técnica exclusiva de adquisición e instalación de un firewall, sino que debe venir complementada con la definición estratégica de políticas de seguridad que permitan gestionar cada uno de los aspectos críticos de la red.

RECOMENDACIONES

Todas las etapas de desarrollo que se han realizado en el presente proyecto desde la evaluación y selección del equipo firewall hasta la instalación, configuración y su puesta en funcionamiento, han permitido mejorar notablemente el acceso y la seguridad de todo el intercambio de información desde y hacia Internet. Cabe destacar que la seguridad no depende única y exclusivamente de la implantación de esta nueva plataforma, ya que se hace indispensable mantener un óptimo nivel de seguridad, actualizando las normas, procedimientos y políticas de acuerdo a la dinámica en que vayan surgiendo nuevas estrategias de ataque contra las redes y sus activos de información.

Para lograr esto se deben definir y mantener políticas que permitan una eficiente administración en el nuevo sistema de seguridad, tomando en consideración los siguientes puntos:

- El control y monitoreo periódico de la información suministrada por los archivos (log) del firewall que permitan detectar y corregir posibles vulnerabilidades del sistema.

- La ejecución de pruebas externas que simulen posibles ataques hacia la red privada, logrando identificar de manera precisa los huecos de seguridad que puedan existir.

- La definición de un conjunto de planes de seguridad que minimicen los riesgos y brinden protección ante cualquier contingencia.

- Finalmente debe mencionarse como punto importante, las actualizaciones periódicas que se le tienen que hacer al firmware del firewall 3Com

SuperStack 3. Las mismas deben ser ejecutadas desde la página Web de 3Com, seleccionando la última versión disponible para este dispositivo. Estas actualizaciones garantizan un funcionamiento óptimo del software y la posibilidad de que éste dispositivo adquiera nuevas herramientas de administración y seguridad.

GLOSARIO DE TÉRMINOS Y ABREVIATURAS

A

- Acceso Remoto: Como su nombre lo indica, el acceso remoto permite conectarse a una red por medio de una conexión telefónica o vía Internet a través de una VPN. Una vez conectado, se puede hacer lo mismo que si se estuviera trabajando en un equipo conectado físicamente a la red.

- Active X: Un lenguaje de programación apoyado en controles OLE, Visual Basic y Librerías del entorno Windows (OCX) de Microsoft. Active X permite que interactúen aplicaciones Windows con el World Wide Web.

- AH: *Authentication Header.* Cabecera de Autenticación. Modo de autenticación que se encarga de proporcionar soporte para la autenticación e integridad de datagramas IP. Su propósito es detectar alteraciones del contenido de un paquete y autenticar la identidad del que lo envía, bien como usuario o por su dirección IP.

- Algoritmos de Cifrado: Es un procedimiento matemático o lógico para lograr un fin determinado (no sólo en criptografía). Los algoritmos de cifrado, tienen como entrada los datos del texto claro, un procedimiento que utiliza la clave que se va a utilizar y una salida que es el texto enigmático. Hay muchos algoritmos posibles para el cifrado (e incluso combinaciones de algoritmos), y su implementación tiene gran importancia comercial y política.

- AP: *Access Point*. Punto de Acceso.

- ARP: *Address resolution protocol.* Protocolo utilizado en las redes de difusión para resolver la dirección de IP en base a la dirección de trama de capa 2.

B

- Backbone: Literalmente: Columna vertebral. En redes constituye el conjunto de vías principales por donde viajan los datos de una empresa, de un país, etc. pueden considerarse equivalentes a las grandes arterias viales, de ahí el término "autopistas de la información".

- Bit: *Binary Digit o Dígito Binario*. Es un dígito en base a 2, es decir, 0 ó 1. Un bit es la unidad más pequeña de información que la computadora es capaz de manejar. El ancho de banda se suele medir en bits por segundo.

- Bps: ***B**its **P**er **S**econd*. Unidad utilizada para medir la velocidad de transferencia de información, usualmente en miles (Kbps).

- Bridge: Consiste en un equipo que contiene dos puertos de comunicación, crea unas tablas en memoria que contienen todas las direcciones de MAC (direcciones de las tarjetas de comunicaciones), de ambos extremos, de tal manera que restringen el trafico de datos de un segmento a otro, no permitiendo el paso de tramas que tengan como destino una dirección del mismo segmento al que pertenece la estación de origen. Es conveniente el uso de los mismos cuando se requiere la interconexión de dos LAN's locales o remotas.

- Browser: Nombre genérico de los navegadores para Internet o programas que le facilitan la exploración en el Web. Primero fue el Netscape Navigator el cual estableció una serie de estándares, y poco después el Microsoft Internet Explorer.

C

- Cache: La Memoria "cache" es un bloque de memoria de rápido intercambio entre la RAM principal y el CPU que disminuye el "cuello de botella" entre la velocidad del CPU y la transferencia de datos con el resto de los dispositivos.

- Checksum: Es un mecanismo no criptográfico para detectar errores en las transmisiones.

- Circuitos Virtuales: El concepto de circuito virtual se refiere a una asociación bidireccional, a través de la red, entre dos ETD (Equipo Terminal de Datos), circuito sobre el cual se realiza la transmisión de los paquetes. Al inicio, se requiere una fase de establecimiento de la conexión, denominado: "llamada virtual" .Durante la llamada virtual los ETDs se preparan para el intercambio de paquetes y la red reserva los recursos necesarios para el circuito virtual. Los paquetes de datos contienen sólo el número del circuito virtual para identificar al destino.

- Clave de Acceso: Es una combinación de letras, números y signos que debe teclearse para obtener acceso a un programa o partes de un programa determinado, un terminal o computador personal (PC), un punto en la red, etc. Muchas veces se utiliza la terminología inglesa (password) para referirse a la clave de acceso.

- Cliente: Un sistema o proceso que solicita a otro sistema o proceso que le preste un servicio. Una estación de trabajo que solicita el contenido de un

archivo a un servidor es un cliente de este servidor.

- Conexión SLIP: Sserial Line Internet Protocol (SLIP) se creó como una forma de acceder a Internet a través de una línea telefónica. Debido a su facilidad para implementar y a que proporciona funcionalidad no disponible en ningún otro sitio, SLIP es admitido en una gran variedad de sistemas operativos, incluyendo muchas variantes de UNIX. Slip tiene muchas limitaciones, no proporciona detección de errores, lo que convierte en inservible para su uso en líneas telefónicas ruidosas. Tampoco proporciona capacidades de diagnóstico.

- Cookie: Procedimiento ejecutado por el servidor que consiste en guardar información acerca del cliente para sus posterior recuperación. En la práctica la información es proporcionada desde el visualizador al servidor del Word Wide Web vía una forma o un método interactivo que puede ser recuperado nuevamente cuando se accede al servidor en el futuro. Es utilizado por ejemplo para el registro a un servicio.

- Cracker (intruso): Un "cracker" es una persona que intenta acceder a un sistema informático sin autorización. Estas personas tienen a menudo malas intenciones, en contraste con los "hackers", y suelen disponer de muchos medios para introducirse en un sistema.

- Cracking: Acceso de una persona a un sistema informático sin autorización para romper el sistema de seguridad, copiar datos, contraseñas y beneficiarse de alguna manera.

D

- Datagramas: Usualmente se refiere a la división de la información en unidades de menor tamaño para que el protocolo TCP/IP las pueda transmitir. Esto proporciona grandes ventajas en el manejo de los datos que se transfieren y, por otro lado, esto es algo común en cualquier protocolo de comunicaciones. Estos datos en conjunto se envían como mensajes independientes.

- DDoS: Una variante más potente a la de los ataques de Denegación de Servicio, son los DDoS, o ataques de denegación de servicio distribuidos, que se basan en realizar ataques DoS de forma masiva a un mismo objetivo desde diferentes localizaciones en la red, de forma que la potencia de ataque sea mucho mayor. Si un ataque desde una fuente es potente, desde 1000 lo será mucho más, es decir, es la aplicación del “divide y vencerás” a la técnica DoS.

- Dial-out: La tecnología dial-out permite a una persona acceder al servicio Internet a través de una línea telefónica analógica y un modem estando dentro de una red.

- Dial-up: Término actualmente utilizado como sinónimo de dial-in. Conexión a Internet que se establece a través de un módem y una línea telefónica.

- Dirección IP: Es la dirección única de cada máquina, formada por números separados por puntos. Por ejemplo, 128.253.153.54.

- DoS: *Denial of Service.* Es un tipo de ataque cuya meta fundamental es la de negar el acceso del atacado a un recurso determinado o a sus propios recursos.

E

- E-mail Spoofing: Consiste en alterar la identidad de la cuenta que envía el e-mail, logrando que sea más difícil determinar quién está enviando realmente el correo.

- Encapsulación: Es la habilidad de una parte de un programa para ocultar sus datos al resto del código, impidiendo así accesos incorrectos o conflictos con los nombres de otras variables.

- Encriptación: Alteración de los datos para que sólo alguien con acceso a códigos específicos para descifrarlos pueda comprender la información.

- Escaneo de Puertos: El escaneo es la determinación de las características de una red o sistema remotos, con el objetivo de identificar los equipos disponibles y alcanzables desde Internet, así como los servicios que ofrece cada uno. Permite saber los sistemas existentes, los servicios ofrecidos por ellos, cómo están organizados los equipos, que sistemas operativos ejecutan, cual es el propósito de cada uno.

- ESP: *Encapsulating Security Payload*. Datos seguros encapsulados que sirven de refuerzo de seguridad en la transmisión de datos en los protocolos IP. Es utilizado para mantener la confidencialidad, integridad, autenticación y cifrado de los datos.

F

- Fibra Óptica**:** Conductor de impulsos luminosos digitales de muy alta velocidad y confiabilidad, que tiene muchas ventajas sobre el cableado tradicional de cobre.

- Finger: Programa que muestra información acerca de un usuario específico, o acerca de todos los usuarios, conectado a un sistema o remoto. Habitualmente se muestra el nombre y apellidos, hora de la última conexión, tiempo de

conexión sin actividad, línea del terminal y situación de éste. Puede también mostrar archivos de planificación y de proyecto del usuario.

- Firewall: (Pared de Fuego). Dispositivo diseñado para proveer seguridad en la periferia de una red. Se trata de cualquier programa (Software) ó dispositivo (Hardware) que protege a una red de otra red. El firewall da acceso a una maquina en una red local a Internet pero Internet no ve mas allá del firewall.

- Firmware: Concepto intermedio entre el hardware y el software. En las computadoras y ciertos dispositivos electrónicos existen una serie de microprogramas contenidos en la memoria ROM que sirven de ayuda a la unidad de control del equipo. A estos programas permanentemente almacenados en la memoria de sólo lectura se les denomina firmware.

- Frames: Tramas. Estructura utilizada para encapsular los paquetes IP.

- FTP: *File Transfer Protocol.* Método utilizado para transferir múltiples archivos entre dos sitios de Internet. Existen muchos sitios que permiten a los usuarios ingresar libremente a sus máquinas para obtener programas shareware u otro tipo de información.

G

- Gateway: Pasarela, puerta de acceso. Dispositivo que permite conectar entre si dos redes normalmente de distinto protocolo o un host a una red.

- Gbps: *Gigabits por segundo*. Velocidad de transmisión de mil millones de bits por segundo.

- Gopher: Es un mecanismo de las etapas iniciales de Internet que permitía hallar recursos disponibles mediante el uso de sencillos menús. Ya prácticamente no se usa.

H

- Hacker: Persona que tiene un conocimiento profundo acerca del funcionamiento de redes y que puede advertir los errores y fallas de seguridad del mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo.

- Hacking: Acceso de una persona no autorizada a un sistema informático con la intención de explorar los detalles de los sistemas programables y ver cómo ensanchar sus capacidades.

- Hardware Equipos: Parte tangible de los equipos de computación. Todos los componentes tales como periféricos, CPUs, etc.

- Hash: Valor de identificación producido mediante la realización de una operación numérica llamada función hash sobre un elemento de datos. El valor no sólo identifica al dato sino que requiere mucho menos espacio de almacenamiento; por tal razón, la computadora puede buscar valores de hash más rápidamente que los datos mismos, de mayor extensión.

- Host: En redes de computadoras y telecomunicaciones, es un servidor que realiza funciones centralizadas, como poner al alcance de las demás computadoras los programas y los archivos de datos disponibles.

- Host Bastión: Es un sistema informático que deber ser altamente seguro porque es vulnerable a un ataque, por lo general debido a que está expuesto a Internet o cualquier otra red pública y es el punto principal de contacto para usuarios de redes internas. El host bastión contiene la información que queremos hacer accesible a través de la red pública de datos como por ejemplo sería el caso de un servidor de correo o un servidor HTTP.

- Hosting: Espacio para un sitio o página de Internet en un servidor activo. Es decir, es un espacio en un disco rígido de una computadora conectada las 24 horas del día a Internet para que el autor del sitio pueda darse a conocer en la red.

- HTTP: *Hyper Text Transfer Protocol.* Servicio orientado a conexión que ofrece la posibilidad de observar documentos de Hyper Texto o Texto Enriquecido (Hyper Text Markup Language, HTML) ubicados en un servidor remoto.

- Hubs: Concentradores. Retransmiten cualquier paquete que llegue a uno de sus puertos a sus otros puertos.

I

- ICMP: *Internet Control Messaging Protocol:* Protocolo considerado a nivel de IP, ya que es empleado por éste para notificar mensajes de error o situaciones que requieren cierta atención. Debido a que los paquetes ICMP viajan en paquetes IP es a veces considerado un nivel por encima. Existen numerosos tipos de mensajes que permiten tanto notificar situaciones de error, como realizar peticiones de información. Asimismo, un mensaje ICMP siempre contiene los 8 primeros bytes del paquete IP que dio lugar a su generación, así el sistema receptor al extraerlo de la red sabrá a qué módulo asociárselo: TCP, UDP. Los mensajes ICMP de error más habituales son el

tipo 3 que permite especificar que no se puede llegar a una red destino, *destination unreachable*, que a su vez dispone de múltiples códigos, aplicados a la red, al *host*, al servicio, etc. Asimismo, ICMP proporciona la funcionalidad de adquirir información mediante pares de paquetes petición / respuesta, por ejemplo, para adquirir la máscara de red de un sistema o preguntar por la hora, mediante el manejo de *timestamps*. Por último, en numerosas ocasiones se emplea para comprobar la existencia de conectividad, como en la utilidad *ping*, empleando paquetes ICMP *echo* y *echo reply.*

- ICSA: *Internacional Computer Security Association.*

- IEEE: *Institute of Electrical and Electronics Engineers, Inc*. Autoridad que se encarga de establecer ciertos estándares en el ámbito de ingeniería de computación, tecnología biomédica, telecomunicaciones, energía eléctrica, ingeniería aerospacial y electrónica, entre otros.

- IMAP: *Internet Mail Access Protocol.* Provee la misma funcionalidad de POP3 pero añade otros útiles recursos.

- Interfaz en Software: Se denomina así a los componentes y facilidades de los programas que manejan la comunicación con el usuario.

- Intranet: Se llaman así a las redes tipo Internet pero que son de uso interno o privado, por ejemplo, la red corporativa de una empresa que utiliza el protocolo TCP/IP y servicios similares como WWW.

- IP: *Internet Protocol.* Es el protocolo principal de TCP/IP, encargado de la transmisión y enrutamiento de los paquetes de datos al equipo destino. Es un protocolo no fiable, es decir, que no asegura la recepción final en el equipo destinatario de la información. Para el control de los posibles errores dispone de un protocolo de aviso, ICMP. La fiabilidad de la comunicación debe proporcionarla los protocolos superiores, como TCP.

- IPSec*: Internet Protocol Security.* Seguridad de Protocolo de Internet.

- IP Spoofing: Se basa en actuar en nombre de otro usuario tal y como si se fuese él mismo (*impersonation*). En el caso de TCP/IP, se basa en la generación de paquetes IP con una dirección origen falsa. El motivo para realizar el envío de paquetes con esa IP puede ser, por ejemplo, que desde la misma se disponga de acceso hacia un sistema destino objetivo, porque existe un dispositivo de filtrado (screening router o firewall) que permite el tráfico de paquetes con esa dirección IP origen, o porque existe una relación de confianza entre esos dos sistemas.

- IPX: *Internet Packet Exchange*. Intercambio de Paquetes entre redes. Inicialmente protocolo de Novell para el intercambio de información entre aplicaciones en una red Netware.

- ISP: *Internet Service Provider*. Proveedor de Servicios de Internet.

J

- JAVA: Un lenguaje de programación que permite ejecutar programas escritos en un lenguaje muy parecido al C++, llamados applets, a través del World Wide Web. La diferencia contra un CGI es que la ejecución se realiza totalmente en la computadora cliente, en lugar del servidor. Java fue originalmente desarrollado por Sun Microsystems. El principal objetivo de JAVA fue hacer un lenguaje que fuera capaz de ser ejecutado de una forma segura a traves de Internet. Esta característica requiere la eliminación de muchas contrucciones y usos de C y C++. El más importante es que no existen punteros. Java no puede acceder arbitrariamente a direcciones de memoria. Java es un lenguaje compilado en un código llamado "codigo-byte" (byte-code). Este código es interpretado "en vuelo" por el intérprete Java.

L

- LAN: *Local Area Network*. Red de Area Local. Red de computadoras ubicadas en El mismo ambiente, piso o edificio.

- Land Attack: Este ataque permite bloquear un sistema, mediante el envío de un paquete SYN cuya dirección IP fuente y destino es la misma. Existe una variación de este ataque, basada en que los puertos origen y destino también son iguales. Para ello es necesario enviar paquetes IP mediante la técnica de spoofing.

- L2F: Transmisión de nivel 2. Es un protocolo de transmisión que permite a los servidores de acceso por marcación estructurar el tráfico de marcación en un PPP y transmitirlo a través de enlaces WAN a un servidor L2F. Después, el servidor L2F abre los paquetes y los transmite a través de la red. A diferencia del PPTP y del L2TP, el L2F no tiene un cliente definido. Asimismo, el L2F sólo funciona en túneles obligatorios.

M

- MAC: *Media Access Control.* Control de Acceso al Medio. Contienen 48 bits de longitud y son únicas, es un componente superior de la Capa de Enlace de Datos (OSI).

- MAN: *Metropolitan Area Network*. Redes de Area Metropolitana.

- Mbps: *Megabits por segundo*. Unidad de medida de la capacidad de transmisión por una línea de telecomunicación. Cada megabit está formado por 1.048.576 bits.

- Módem: *(MOdulator,DEModulator)*. Codificador y decodificador de señales digitales en señales analógicas susceptibles de trasladarse por una línea de telecomunicaciones. Es un dispositivo que se conecta a la computadora y a la línea telefónica y permite comunicarse con otras computadoras a través del sistema telefónico. Básicamente, los módems sirven a las computadoras de la misma manera que los teléfonos sirven a las personas.

- MP3 / MP4: El MP3 es un formato de compresión de audio que permite el download de música para ser almacenada en un disco duro o en un reproductor compatible (como el RIO). El MP4 no es necesariamente una mejora del MP3, actúa ejecutando algoritmos de AT&T con la misma finalidad de manejar música en Internet.

- MPEG: *Motion Picture Expert Group*. Es un estándar para la decodificación y descompresión de imágenes y sonidos digitales en archivos muy grandes. El MPEG-1 (Audio Layer 3) está estrechamente vinculado al MP3. El MPEG-2 es utilizado fundamentalmente por las tecnologías de discos DVD.

N

- NAT: Network Address Traslation. La técnica basada en la traducción de direcciones de red o NAT, así como su variante que permite la traducción adicional de los puertos, PAT (Port Address Traslation). Estas técnicas permiten no conocer desde el exterior las direcciones IP reales empleadas en la red interna, mostrando una visión particular y concreta de los sistemas y servicios visibles desde el exterior (direcciones IP y puertos). Por tanto, dificultarán la identificación y obtención de información de técnicas como footprinting.

- NetBIOS: Es un protocolo de transporte de datos (basado en sesiones) característico de los entornos Windows. Asimismo añade la funcionalidad de resolución de nombres en este entorno, a través del puerto UDP 137.

- Net Flood: El objetivo de este ataque es degradar la capacidad de conexión a la red de un sistema, saturando sus enlaces de comunicaciones. Por ejemplo, si el enlace de una organización dispone de un ancho de banda de 34 Mb. y un atacante dispone de un enlace de 155 Mb., prácticamente la totalidad del tráfico cursado por la organización pertenecerá al atacante, por lo que no

podrá enviarse tráfico útil.

- NIC: *Network Interface Card*. Tarjetas de interfaz de red.

- Nivel de Red: Es responsable del direccionamiento de mensajes y de la conversión de las direcciones lógicas y nombres, en direcciones físicas. Está encargado también de determinar la ruta adecuada para el trayecto de los datos, basándose en condiciones de la red, prioridad del servicio, etc. El nivel de red agrupa pequeños fragmentos de mensajes para ser enviados juntos a través de la red.

O

- OSI: Open Systems Interconnection. Modelo que estandariza la representación de las redes a través de capas.

P

- Paquetes: Fracciones de un mensaje de tamaño predefinido, donde cada fracción o paquete contiene información de procedencia y de destino, así como información requerida para el reensamblado del mensaje.

- Paquetes SYN: Se encargan de sincronizar los números de secuencia. Se utilizan al crear una conexión para indicar al otro extremo cual va a ser el primer número de secuencia con el que va a comenzar a transmitir.

- Password: Palabra clave utilizada para obtener acceso a una computadora, a una red o a un sistema. Un password generalmente contiene una combinación de números y letras que no tienen ninguna lógica.

- Peer To Peer: En una red se refiere a una conexión punto a punto de extremos distantes en los cuales ningún nodo es el principal, y por lo general todos los nodos poseen la misma autoridad sobre el canal.

- PGP: *Pretty Good Privacy*. Un sistema de encriptación por clave pública y sirve para que nadie, salvo uno mismo y el destinatario o destinatarios a los que vaya dirigido el mensaje puedan leerlo, al ir el mensaje codificado.

- PING: *Packet internet Groper*. (Búsqueda de Direcciones de Internet) Programa que se utiliza para comprobar si un destino está disponible.

- Ping of Death: Conocido como ping de la muerte, este ataque se basa en enviar un paquete de ping (ICMP echo request) de un tamaño muy grande. Teniendo en cuenta que el tamaño máximo de paquete en TCP/IP es de 64

Kbytes (65535 bytes), la implementación de la pila TCP/IP asigna un buffer en memoria de este tamaño. En el caso de que la información sea mayor, el buffer puede desbordarse. El resultado obtenido en muchas ocasiones es que el sistema destino deja de proveer servicio al bloquearse, ya sea rearrancándose (reboot) o incluso apagándose (shutdown). Lo que sucede realmente es que el paquete emitido es fragmentado, a nivel de IP, en las redes intermedias, los fragmentos van siendo encolados en el sistema destino hasta que se reciben los último pedazos (un paquete de 65536 bytes es suficiente), que son los que desbordan el buffer, provocando un comportamiento anómalo.

- Plug and Play: *PnP*. Modalidad de estandarización que persigue la facilidad de conexión, en el sentido de que los equipos detecten automáticamente las características de un periférico y actúen en consecuencia, sin necesidad de complejas instalaciones.

- Políticas de Seguridad: Las políticas de seguridad son las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños informáticos.

- POP3: *Post Office Protocol.* Servicio orientado a conexión que permite al usuario obtener su correo electrónico entrante.

- PPP: *Point-to-Point Protocol.* Protocolo Punto-a-Punto. Protocolo que le permite a la computadora usar una línea telefónica y un módem para realzar una conexión TCP/IP y así simular que está realmente dentro de Internet.

- Protocolo: Conjunto de reglas que posibilitan la transferencia de datos entre dos o más computadores.

- Protocolo IP: *Internet Protocol.* Es un protocolo connectionless (no intercambia información de control para establecer una conexión nodo a nodo antes de transmitir), se encarga de definir el esquema de direccionamiento de Internet y mueve los datos entre la capa de acceso de red y la capa de transporte host-to-host. No corrige ni detecta errores en la información.

- Proxy Servers: Servidores Proxy. Servidores que ejecutan un programa sencillo específicamente diseñado para la seguridad de redes. Este permite que el código fuente de la aplicación pueda revisar y analizar posibles intrusos y fugas de seguridad. Un servidor Proxy mantiene la información detallada y auditada de todos los registros del trafico, cada conexión y la duración de cada una. El registro de audición es una herramienta esencial para descubrir y finalizar el ataque de un intruso.

- Puerto: Es un número de 16 bits, por lo que existen 65536 puertos en cada

computadora. Las aplicaciones utilizan estos puertos para recibir y transmitir mensajes.

R

- RADIUS: *Remote Authentication Dial-In User Service.* Servicio de usuario de acceso telefónico de autenticación remota. Suministra servicios de autenticación, autorización y cuentas al acceso telefónico a redes distribuidas.

- RAM: *Random Access Memory*. Memoria de acceso aleatorio. Es el área primaria de memoria donde se ejecutan los programas y se almacenan archivos (o parte de ellos) mientras el equipo está encendido y operando. Las operaciones en esta memoria se ejecutan a muy alta velocidad y es volátil, es decir al apagarse el equipo se borra todo lo que está ahí.

- Red: Se tiene una red cada vez que se conectan dos o más computadoras de manera que pueden compartir recursos.

- Redes Conmutadas: son aquellas que no requieren conexiones permanentes entre dos puntos fijos. En su lugar, permite a los usuarios establecer conexiones temporales entre múltiples puntos cuya duración corresponde a la de la transmisión de datos. Dicha red esta formada por un conjunto de nodos que encaminan la información de origen a destino.

- Red de perímetro: Se trata de una red adicional entre una red protegida y una red externa a fin de proporcionar una seguridad adicional. A este tipo de redes también se las conoce por las siglas DMZ (De-Militarized Zone, zona desmilitarizada).

- RJ45: Conector tipo teléfono para redes, que tiene 8 conductores correspondientes a los 4 pares de los cables UTP-5.

- Rlogin: Es un protocolo cliente-servidor que utiliza TCP como medio de transporte. Permite a un usuario identificarse remotamente desde un host a otro, y si el host destino confía en el origen no pedirá la contraseña. En lugar de esto, habrá comprobado la identidad del cliente analizando su dirección IP. Por tanto, se podrá usar *rlogin* para acceder remotamente desde A a B o viceversa sin necesidad de introducir contraseñas.

- Router: Son dispositivos que permiten unir varias redes (más de dos, a diferencia de los bridges), tomando como referencia la dirección de red de cada segmento. Al igual que los bridges, los routers restringen el trafico local

de la red permitiendo el flujo de datos a través de ellos solamente cuando los datos son direccionados con esa intención.

- RPC: *Remote Procedure Call.* El RPC es una interfaz de programación de aplicación(API) disponible para el desarrollo de aplicaciones distribuidas. Permite que los programas llamen a subrutinas que se ejecutan en un sistema remoto. El programa llamador, denominado (llamado *client*) envía una *mensaje de llamada* al proceso *proceso servidor* y espera por un *mensaje de respuesta*. La llamada incluye los parámetros del procedimiento y la respuesta los resultados.

- RSA: Es un sistema criptográfico con clave pública tanto para encriptado como para autenticación que fue inventado por Ron Rivest, Adi Shamir y Leonard Adleman en 1977.

S

- Scanner de puertos: Un escáner es un programa que detecta puntos débiles de un sistema remoto de manera automática, en un servidor local o remoto. Con ello, un usuario conectado a Internet sería capaz de descubrir fallos de seguridad en cualquier servidor conectado a Internet, independientemente de su situación geográfica.

- Servidor (Hardware): Equipos centralizadores y de enlaces para la constitución de redes, de diferentes magnitudes, en interacción con PCs, routers, hubs, proxys, etc.

- SMTP: *Simple Mail Transfer Protocol.* Servicio que permite la transmisión de correo electrónico saliente desde el computador origen hasta el servidor destino.

- SMTP Spoofing: En un nivel superior, concretamente a nivel de aplicación, en el protocolo SMTP (puerto TCP 25) es posible falsear la dirección fuente de un correo o e-mail, enviando por tanto mensajes en nombre de otra persona. Es así porque el protocolo no lleva a cabo ningún mecanismo de autenticación cuando se realiza la conexión TCP al puerto asociado.

- Smurf Attack: Son inundaciones absolutas de datos que envía un atacante para abrumar la capacidad finita de la conexión, y todos lo que están conectados se desconectan de los mismos. El ataque puede durar mucho tiempo incluso hasta días.

- SNMP: *Simple Network Managment Protocol*: Estándar de bajo nivel utilizado para el monitoreo de nodos sobre una red.

- Sniffers: Un sniffer suele ser una combinación de hardware y software que captura información que viaja en una red.

- SNMP: *Simple Network Management Protocol.* Protocolo Simple de Manejo de Redes.

- Spamming: Consiste en el envío masivo de un mensaje de correo a muchos usuarios destino, pudiendo llegar a saturarse los servidores de correo. Suele emplearse para el envío no deseado de publicidad o información.

- Spoofing: En castellano se traduce como engaño. Consiste en el procedimiento mediante el cual se cambia la fuente de origen de un conjunto de datos en una red. Por ejemplo, se puede adoptar otra identidad de remitente con el objetivo de engañar a un cortafuegos. Consisten en la suplantación por parte del atacante de una persona autorizada. Se suele realizar de dos formas: obteniendo el nombre y contraseña del atacado o suplantando a la víctima una vez ésta ya ha iniciado una sesión en su sistema.

- SSL: *Secure Socket Layer*: Método de encriptación o cifrado de la información, para evitar fraudes en las transacciones comerciales a través de Internet (ejemplo, con tarjetas de créditos).

- Syn Flood: Dentro de los ataques DoS, existe uno asociado directamente al protocolo TCP. Consiste en el envío masivo de paquetes de establecimiento de conexión (SYN) contra un sistema. La recepción de estas solicitudes provoca que el sistema destino, objetivo del ataque, reserve cierta cantidad de memoria (buffers) para almacenar las estructuras de datos asociadas a cada una de las nuevas conexiones en curso.

T

- TCP/IP: *Transmission Control Protocol / Internet Protocol*. Es el protocolo de control de transmisión de Internet, protocolo ideado por el Departamento de Defensa de los E.U.A. en 1970. TCP/IP es un conjunto de protocolos diseñados específicamente en una tecnología InterRed; el TCP define el esquema de direccionamiento de Internet, y este esquema es uniforme (es decir, no existen dos direcciones de Internet que sean iguales).

- TCP: *Transport Control Protocol.* Es el protocolo empleado en la mayoría de los servicios que componen Internet actualmente. Es un protocolo fiable, es decir, se asegura de que los paquetes da datos llegan al otro extremo mediante el uso de números de secuencia y de confirmaciones de recepción (ACKs), y

es orientado a conexión, es preciso que las dos partes que van a comunicarse conozcan a la otra y establezcan una conexión formal. Asimismo, está debería terminarse de forma adecuada. Por último se trata de un servicio de stream, ya que las partes intercambian flujos de datos de 8 bits (1 byte), por lo que no existen marcadores en los datos, sólo información.

- Teardrop: El ataque teardrop se basa en el envío de fragmentos de paquetes en lugar de paquetes completos. Se comprobó que algunas implementaciones de la pila TCP/IP no eran capaces de reconstruir paquetes con fragmentos cuyos bytes se superponen. El resultado es de nuevo que el sistema destino puede llegar a bloquearse; apareció en Linux inicialmente. Para llevarlo a cabo bastaría con 2 paquetes, A y B, dónde el offset del paquete B indica que comienza dentro del paquete A.

- TFTP: El protocolo trivial de transferencia de archivos, (TFTP), es un protocolo simple que proporciona una función básica de transferencia de archivos sin autenticación de usuario. TFTP está destinado a las aplicaciones que no necesitan las interacciones sofisticadas que proporciona el protocolo FTP.

- Traceroute: Toda red está caracterizada por una topología o distribución, tanto física como lógica, concreta. Existe una herramienta que ayuda a la obtención de ésta: traceroute, creada originalmente para solucionar problemas en una red. Esta técnica permite saber todos los sistemas existentes en un camino entre dos equipos.

- Troyanos (caballos de Troya): También conocidos como puertas traseras (back doors), son fragmentos de programas no autorizados que se introducen en otros para que el programa original ejecute ciertas acciones no deseadas. En el caso de los troyanos que afectan a los servicios TCP/IP más directamente, se trata de programas completos, que normalmente se justifican como herramientas de administración remota o RAT (típicamente de Windows).

- Tunneling: Transporte de paquetes multicast a través de dispositivos y routers unicast. Los paquetes multicast se encuentran encapsulados como paquetes normales de esta manera pueden viajar por Internet a través de dispositivos que solo soportan protocolos unicast.

U

- UDP: *User Datagram Protocol:* Es un protocolo muy sencillo, no orientado a conexión y no fiable, por lo que son los protocolos de nivel superior los que deben asegurarse de la recepción de los datos. Cada operación de envío genera

un único datagrama UDP. Es empleado principalmente en aplicaciones multimedia, para el envío de flujos de información sin un coste de conexión asociado.

- URL: *Uniform Resorce Locator*. Sistema de direccionamiento estándar para archivos y funciones de Internet, especialmente en el Word Wide Web. El url esta conformado por el servicio (ejemplo: http://) más el nombre de la computadora (ejemplo: www.google.com) más el directorio y el archivo referido.

V

- VPN: *Virtual Private Network*. Red Privada Virtual.

W

- WAN: *Wide Area Network*. Redes de Area Amplia. Es una red de computadoras de gran tamaño, dispersa por un país o incluso por todo el planeta.

- WAV: Extensión típica de los archivos de sonidos, creada por Microsoft.

- Web: Ver WWW.

- Web Site: Sitio de Internet o página de una persona, o de una empresa o institución, donde los navegantes van en búsqueda de información. Se identifican por su dirección en la red o URL.

- WWW: *World Wide Web*. Conjunto de recursos que pueden accederse utilizando un Navegador, mediante el protocolo HTTP.

REFERENCIAS BIBLIOGRÁFICAS

- Canavan John E., **Fundamentals of Network Security**, Artech House, 2001.

- Cheswick William R., Bellovin Steven M., Rubin Aviel D., **Firewalls and Internet Security: Repelling the Wily Hacker, Second Edition,** Published by Addison Wesley Professional, 2003.

- Cocho Julian Marcelo, **Riesgo y Seguridad de los Sistemas Informáticos**, Universidad Politécnica de Valencia, 2003.

- Goncalves Marcus, **Manual de Firewalls**, McGraw-Hill, 2002

- Hernández S., Fernández C. y Baptista L., **Metodología de la Investigación**, Segunda Edición, México, Editorial McGraw-Hill, 1998.

- Kaufman Charles, Perlman Radia and Speciner Mike, **Network Security: Private Communication in a Public World**, Pearson Education, 2002.

- Mansfield Richard, **Defensa contra hackers: Protección de Información Privada,** Anaya Multimedia, 2001.

- McClure Stuart, Scambray Joel and Kurtz George, **Hacking Exposed: Network Security Secrets and Solutions**, McGraw-Hill , 2003.

- McClure Stuart, **Hackers: Secretos y Soluciones para la Seguridad deRedes**, McGraw-Hill, 2000.

- Mendillo, V., **Seguridad Informática y Comunicaciones,** UCV, 2003.

- Merike de Kaeo, **Diseño de Seguridad en Redes**, Editorial Alhambra – Longman, 2002.

- Northcutt Stephen, Zeltser Lenny, Winters Scott, Fredrick Karen, Ritchey Ronald W., **Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems,** Published by New Riders Publishing, 2002.

- Olaf Adam, **Seguridad en Internet**, Editorial Marombo, 2001.

- Oppliger Rolf, **Internet and Intranet Security**, Artech House, 2002.

- Pfleeger Charles P. and Pfleeger Shari Lawrence, **Security in Computing**, Prentice Hall Professional, 2002.

- Rodao Jesus De Marcelo, **Piratas Ciberneticos: Cyberwars, Seguridad Informática e Internet**, Editorial RAMA, 2001.

- Siechert Bott, **Seguridad en Microsoft Windows XP y Windows 2000**, McGraw-Hill, 2003.

- Stallings William, **Network Security Essentials**, Pearson Education, November 2002.

- Strassberg Keith, Rollie Gary and Gondek Richard, **Firewalls: The Complete Reference,** Published by McGraw-Hill/Osborne, 2002.

- Universidad Pedagógica Experimental Libertador, **Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales,** Caracas, FEDUPEL, 1998.

- Zwicky Elizabeth D., Cooper Simon D. and Chapman Brent, **Building Internet Firewalls, Second Edition,** Published by O'Reilly & Associates, 2000.

FUENTES ELECTRÓNICAS

- http://www.3com.com
- http://www.cisco.com/
- http://www.checkpoint.com/
- http://www.sonicwall.com/
- http://www.symantec.com/
- http://www.securitydocs.com/firewalls
- http://www.microsoft.com/security/protect/firewall.asp
- http://www.infosyssec.org/
- http://www.securityfocus.com/
- http://www.firewall.com/
- http://netsecurity.about.com/
- http://www.secinf.net/
- http://www.cert.org
- http://www.ciac.org

ANEXOS

Anexo A: Resultados y configuración de una conexión VPN de un cliente remoto

Cliente VPN
Log L2TP/IPSec

A continuación archivo log que muestra una conexión exitosa L2TP/IPSec con algunos comentarios.

RECEIVED<<< ISAKMP OAK MM (MsgID: 0x0) (SA, VID)
El firewall recibe el requerimiento del cliente VPN.
IKE Responder: Begin Main Mode Phase 1
SENDING>>>> ISAKMP OAK MM (MsgID: 0x0) (SA)
RECEIVED<<< ISAKMP OAK MM (MsgID: 0x0) (KE, NON)
NAT Discovery : Peer IPSec Security Gateway doesn't support VPN NAT Traversal
Algunos clientes VPN como el Windows XP no soportan el NAT traversal (la habilidad de trabajar con dispositivos NAT). Este aviso se puede ignorar si no existen dispositivos NAT entre el cliente VPN y el firewall SuperStack 3.
SENDING>>>> ISAKMP OAK MM (MsgID: 0x0) (KE, NON, VID, VID, VID)
RECEIVED<<< ISAKMP OAK MM (MsgID: 0x0) *(ID, HASH)
IKE Responder: Main Mode Phase 1 Done
SENDING>>>> ISAKMP OAK MM (MsgID: 0x0) *(ID, HASH)
IKE Responder: Begin Phase 2
RECEIVED<<< ISAKMP OAK QM (MsgID: 0x1A14E711) *(HASH, SA, NON, ID, ID)
IKE Responder: Accepting IPSec proposal
SENDING>>>> ISAKMP OAK QM (MsgID: 0x11E7141A) *(HASH, SA, NON, ID, ID)
Loading IPSec SA (Message ID = 0x1a14e711, Local SPI = 0xe98d3fed, Remote SPI = 0xdf1a63f7)
RECEIVED<<< ISAKMP OAK QM (MsgID: 0x1A14E711) *(HASH)
IKE negotiation complete. Adding IPSec SA. Phase 2 Done
IKE se ha completado exitosamente. Inicio de la negociación de L2TP sobre IPSec.
LifeSeconds=3600 remote range: (xxx.xxx.xx.xx - xxx.xxx.xx.xx) -
L2TP Server : L2TP Tunnel Established. - Source:xxx.xxx.xx.xx, 1701 - Destination:xxx.xxx.xxx.xx, 1701 - LocalTunnelID=0xe0c5, RemoteTunnelId=0x2, RemoteHostName= RichLaptop.com –
L2TP Server : L2TP Session Established. - Source:xxx.xxx.xx.xx, 1701 - Destination:xxx.xxx.xxx.xx, 1701 - LocalSessionID=0xd9cf, RemoteSessionId=0x1
L2TP Server: Local Authentication Success. - Source:xxx.xxx.xx.xx, 1701 - Destination:xxx.xxx.xxx.xx, 1701 - Host Name :RichLaptop.com, User Name :Rich, Auth Algorithm :MD5 CHAP -
L2TP se ha completado exitosamente.

Las siguientes entradas de log indican problemas comunes:

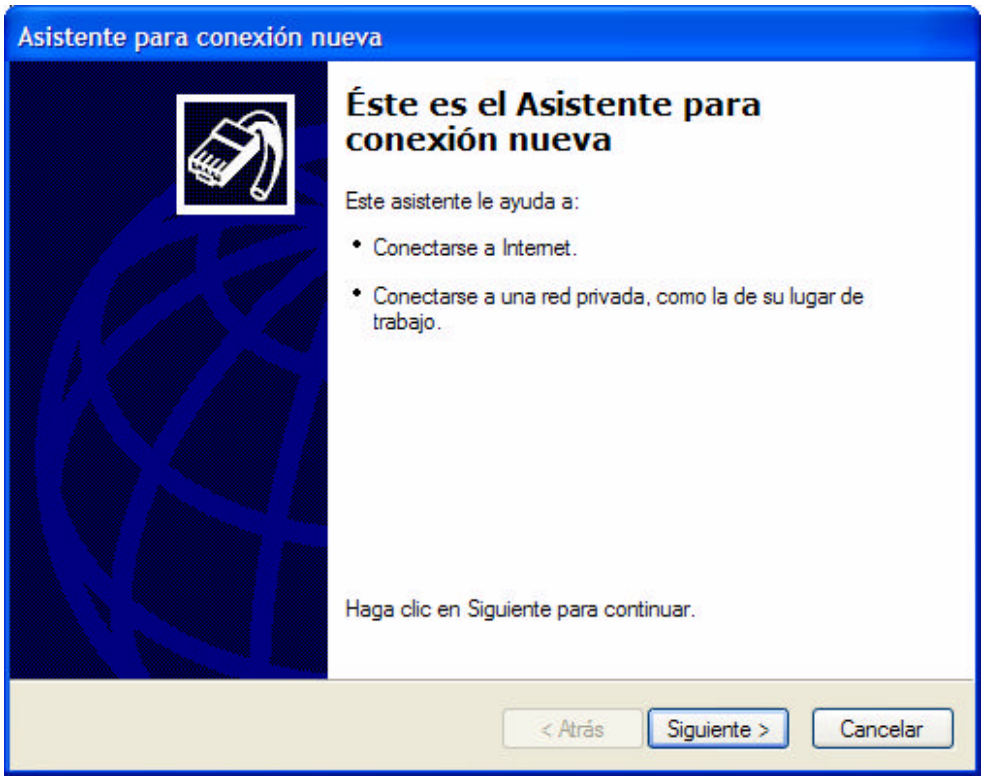
SENDING>>>> ISAKMP OAK INFO (MsgID: 0x4F68AE7F) *(HASH,

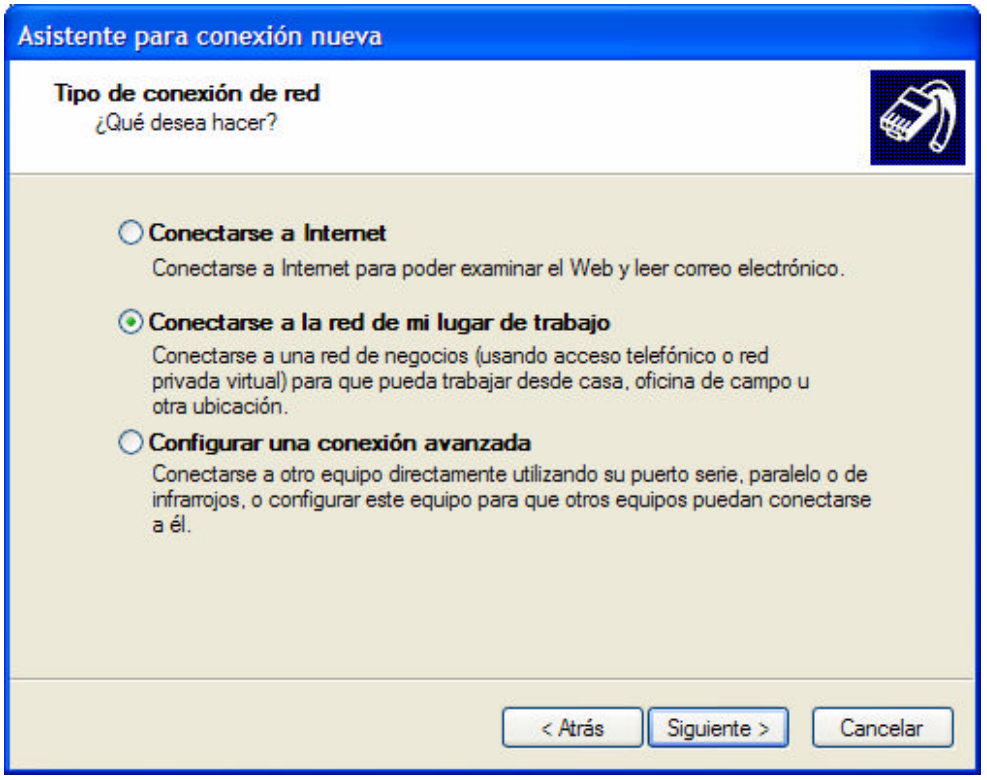
NOTIFY:PAYLOAD_MALFORMED)
El "shared secret" no coincidió..

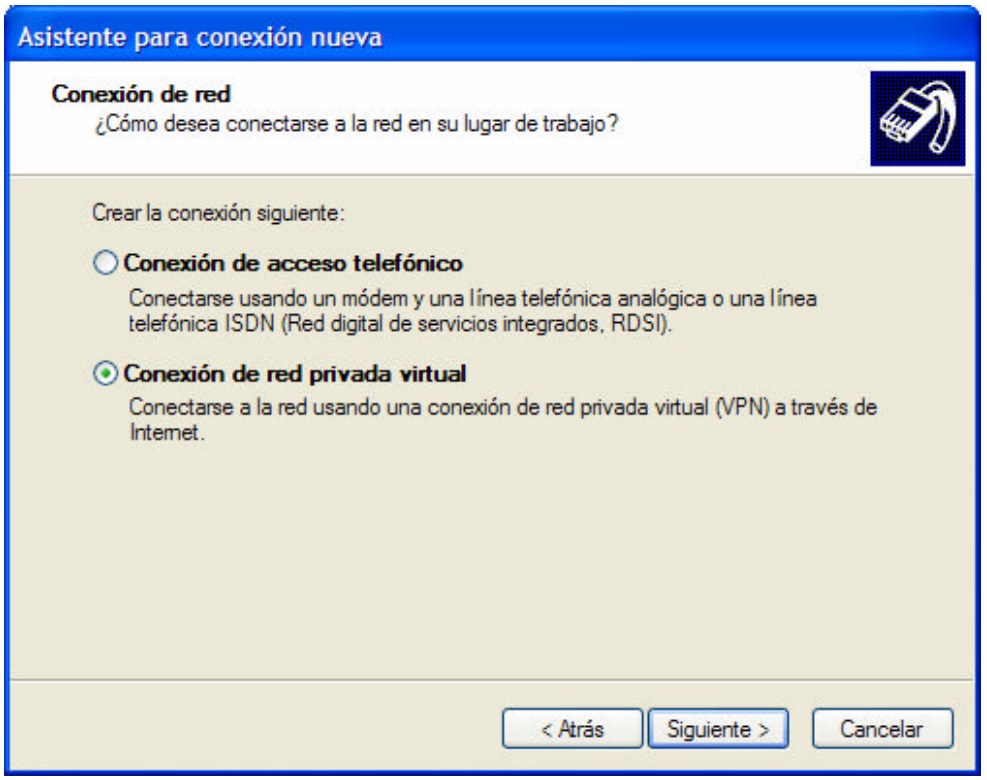
L2TP Server: Local Authentication Failure
El username ó password del L2TP es inválido.

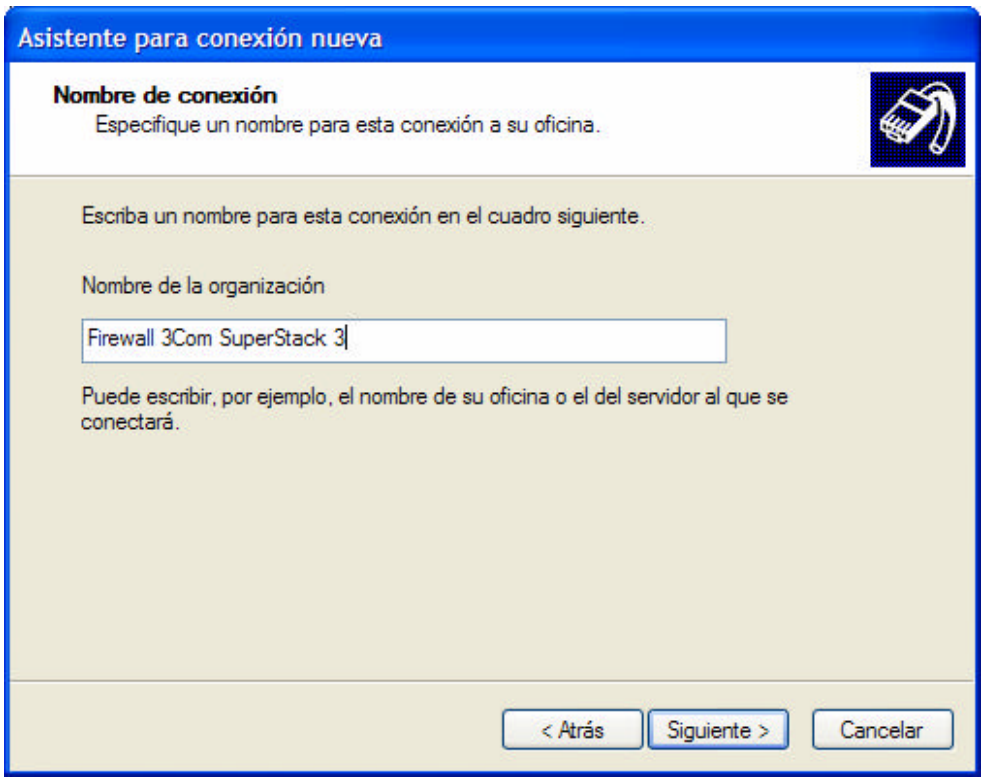
Cliente VPN Windows XP

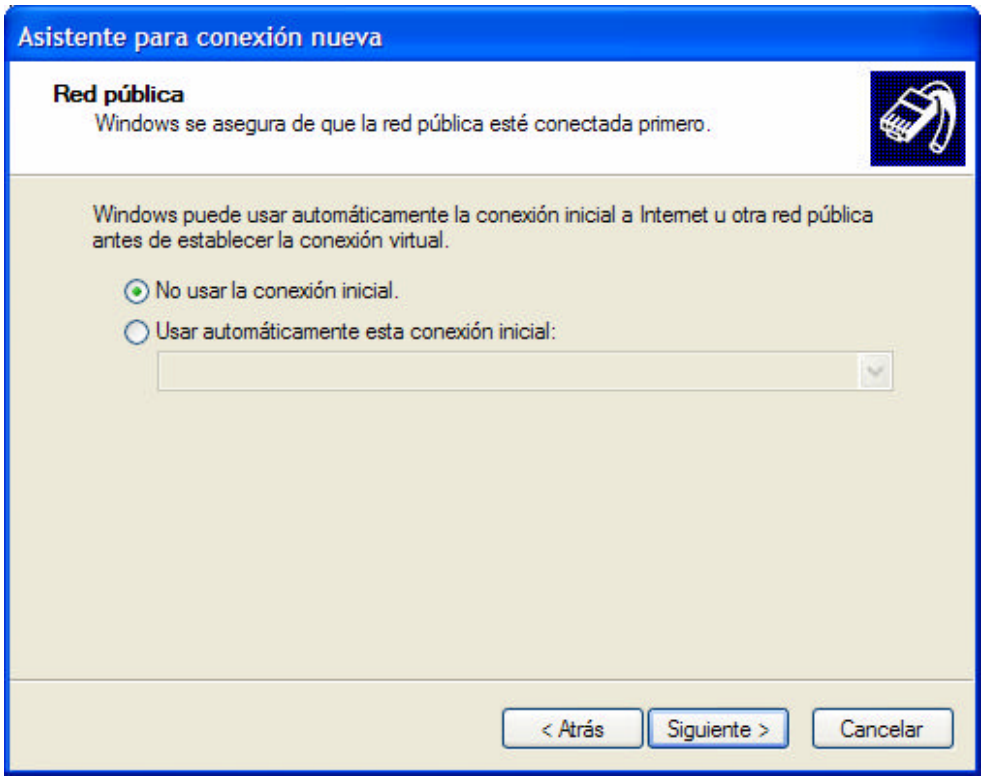
3Com recomienda usar el cliente VPN nativo Windows XP L2TP/IPSec. Las siguiente pantallas describen el procedimiento para dicha configuración.

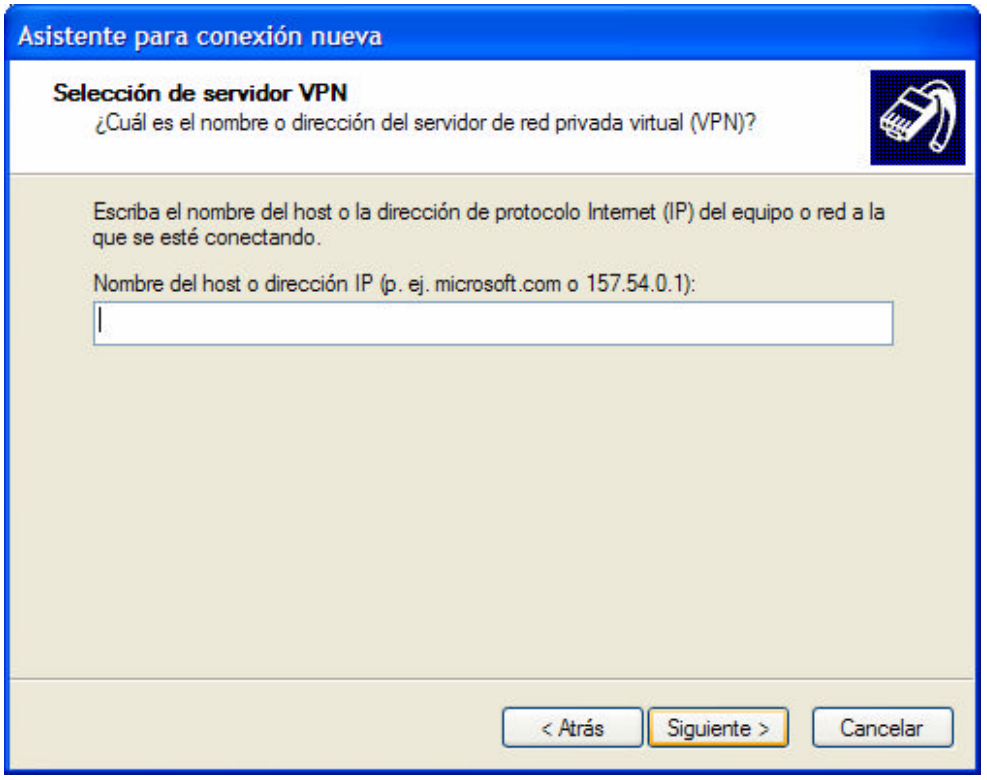


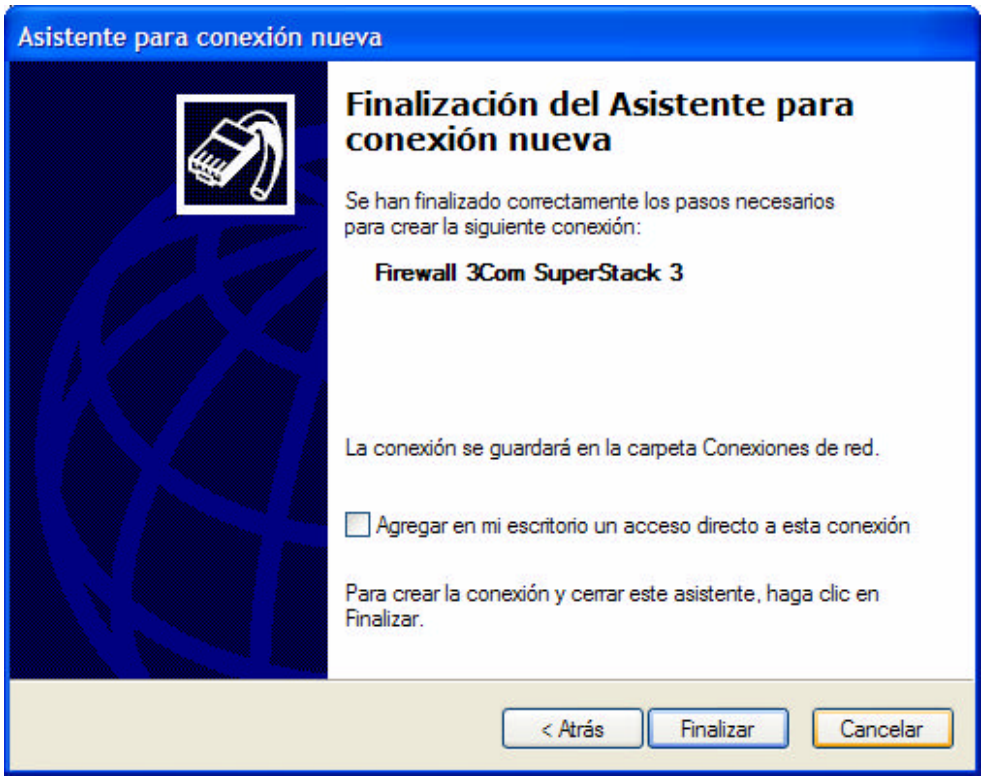

Asistente para conexión nueva
Tipo de conexión de red
¿Qué desea hacer?
Conectarse a Internet
Conectarse a Internet para poder examinar el Web y leer correo electrónico.
Conectarse a la red de mi lugar de trabajo
Conectarse a una red de negocios (usando acceso telefónico o red privada virtual) para que pueda trabajar desde casa, oficina de campo u otra ubicación.
Configurar una conexión avanzada
Conectarse a otro equipo directamente utilizando su puerto serie, paralelo o de infrarrojos, o configurar este equipo para que otros equipos puedan conectarse a él.
< Atrás
Siguiente >
Cancelar


Asistente para conexión nueva
Conexión de red
¿Cómo desea conectarse a la red en su lugar de trabajo?
Crear la conexión siguiente:
Conexión de acceso telefónico
Conectarse usando un módem y una línea telefónica analógica o una línea telefónica ISDN (Red digital de servicios integrados, RDSI).
Conexión de red privada virtual
Conectarse a la red usando una conexión de red privada virtual (VPN) a través de Internet.
< Atrás
Siguiente >
Cancelar

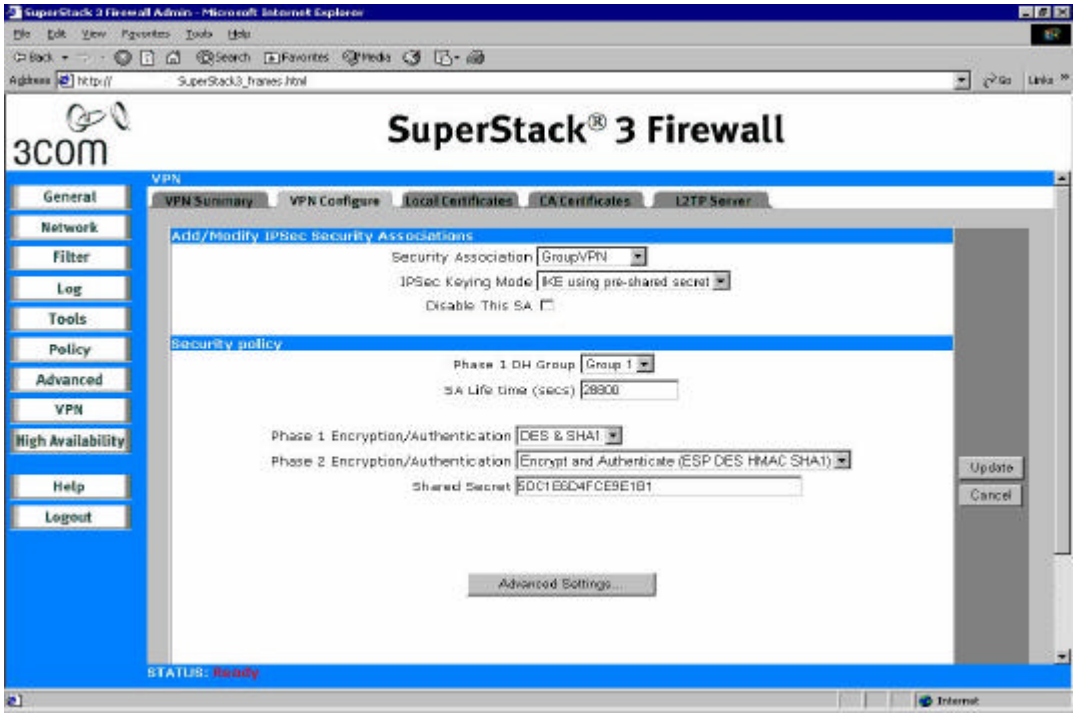

Asistente para conexión nueva
Nombre de conexión
Especifique un nombre para esta conexión a su oficina.
Escriba un nombre para esta conexión en el cuadro siguiente.
Nombre de la organización
Firewall 3Com SuperStack 3
Puede escribir, por ejemplo, el nombre de su oficina o el del servidor al que se conectará.
< Atrás
Siguiente >
Cancelar

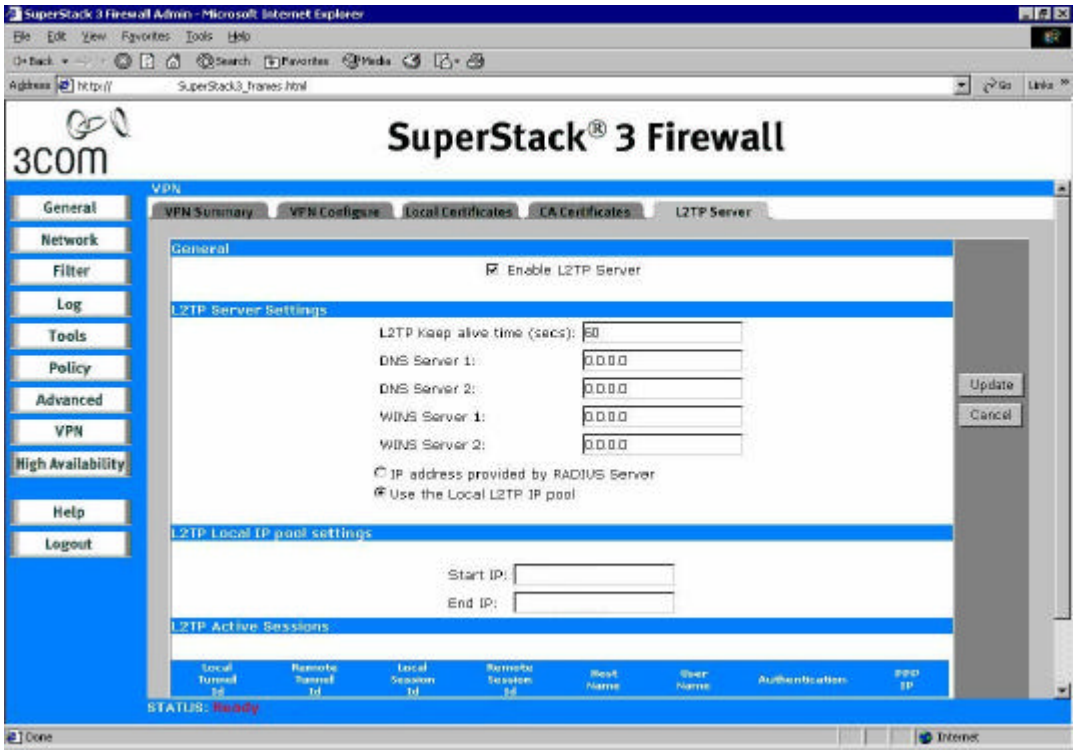

Asistente para conexión nueva
Red pública
Windows se asegura de que la red pública esté conectada primero.
Windows puede usar automáticamente la conexión inicial a Internet u otra red pública antes de establecer la conexión virtual.
No usar la conexión inicial.
Usar automáticamente esta conexión inicial:
< Atrás
Siguiente >
Cancelar


Asistente para conexión nueva
Selección de servidor VPN
¿Cuál es el nombre o dirección del servidor de red privada virtual (VPN)?
Escriba el nombre del host o la dirección de protocolo Internet (IP) del equipo o red a la que se esté conectando.
Nombre del host o dirección IP (p. ej. microsoft.com o 157.54.0.1):
< Atrás
Siguiente >
Cancelar


Asistente para conexión nueva
Finalización del Asistente para conexión nueva
Se han finalizado correctamente los pasos necesarios para crear la siguiente conexión:
Firewall 3Com SuperStack 3
La conexión se guardará en la carpeta Conexiones de red.
Agregar en mi escritorio un acceso directo a esta conexión
Para crear la conexión y cerrar este asistente, haga clic en Finalizar.
< Atrás
Finalizar
Cancelar

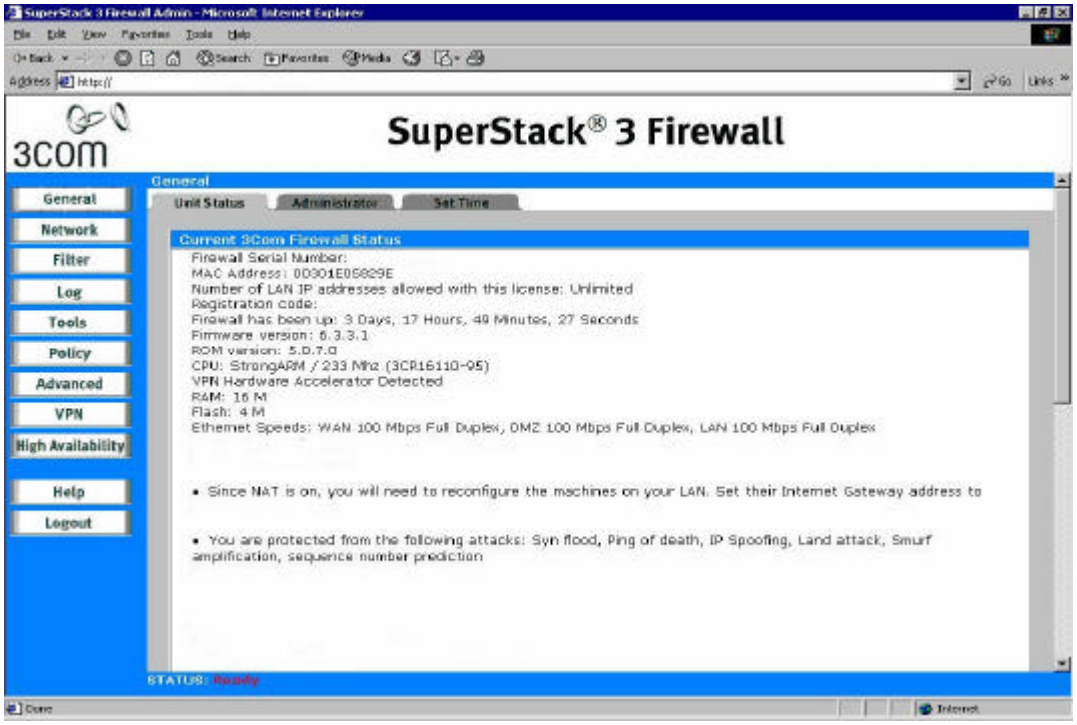
Configuración en el Firewall 3Com SuperStack 3

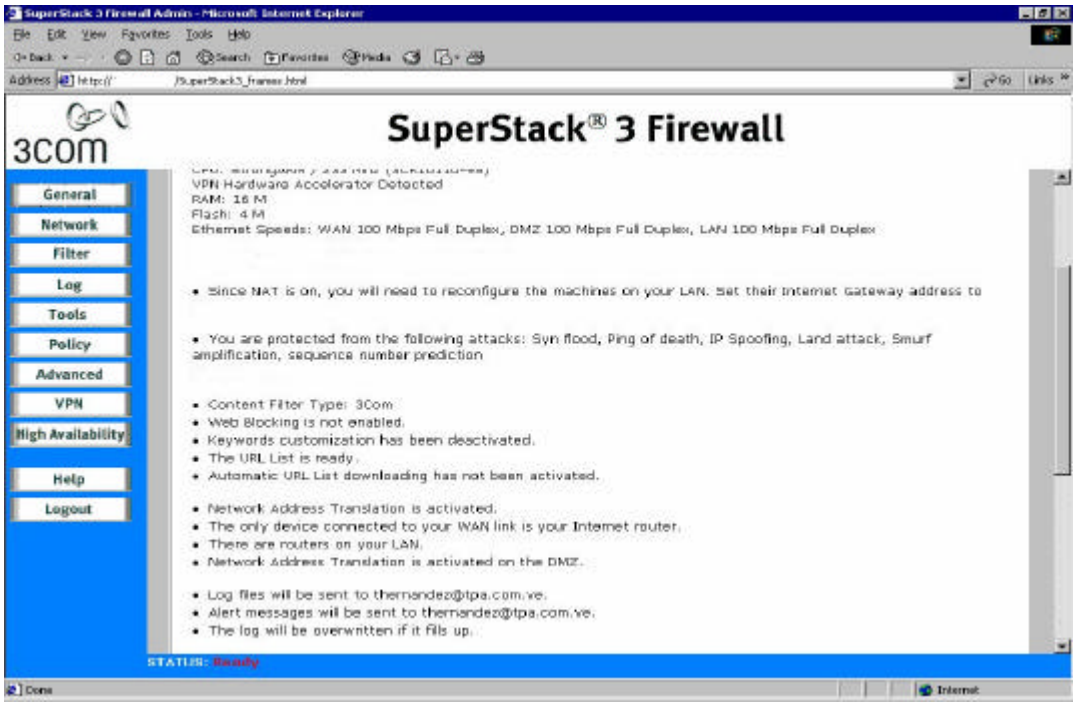


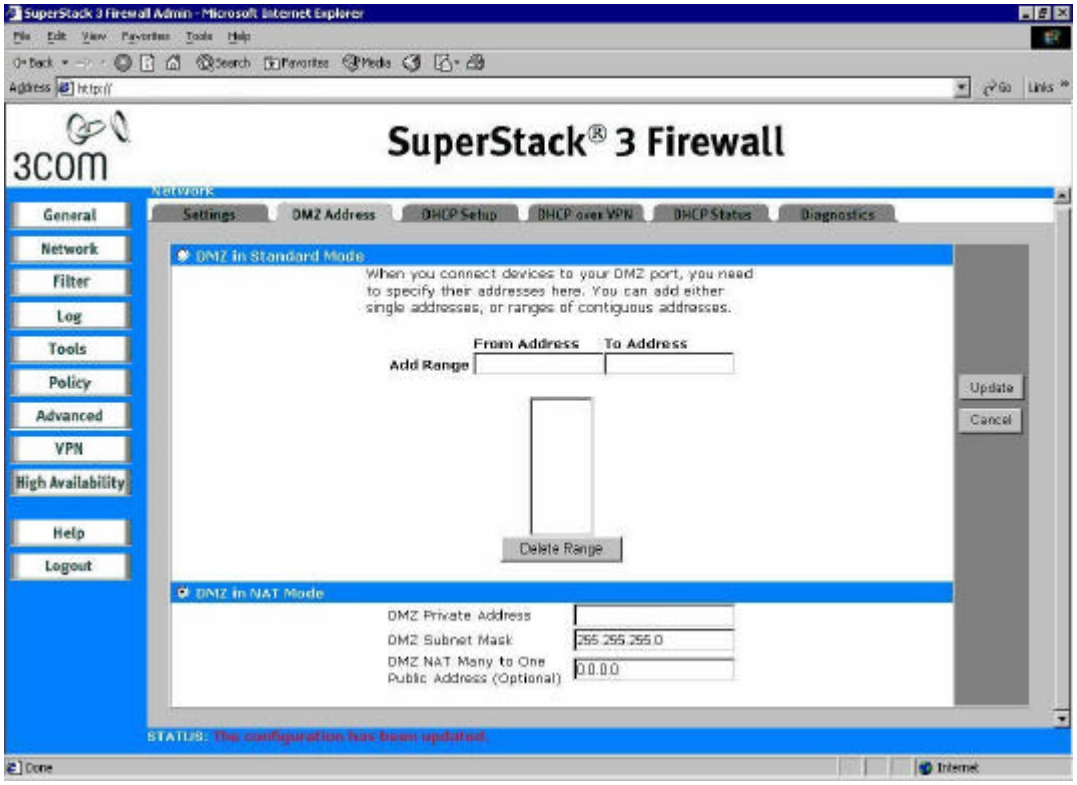


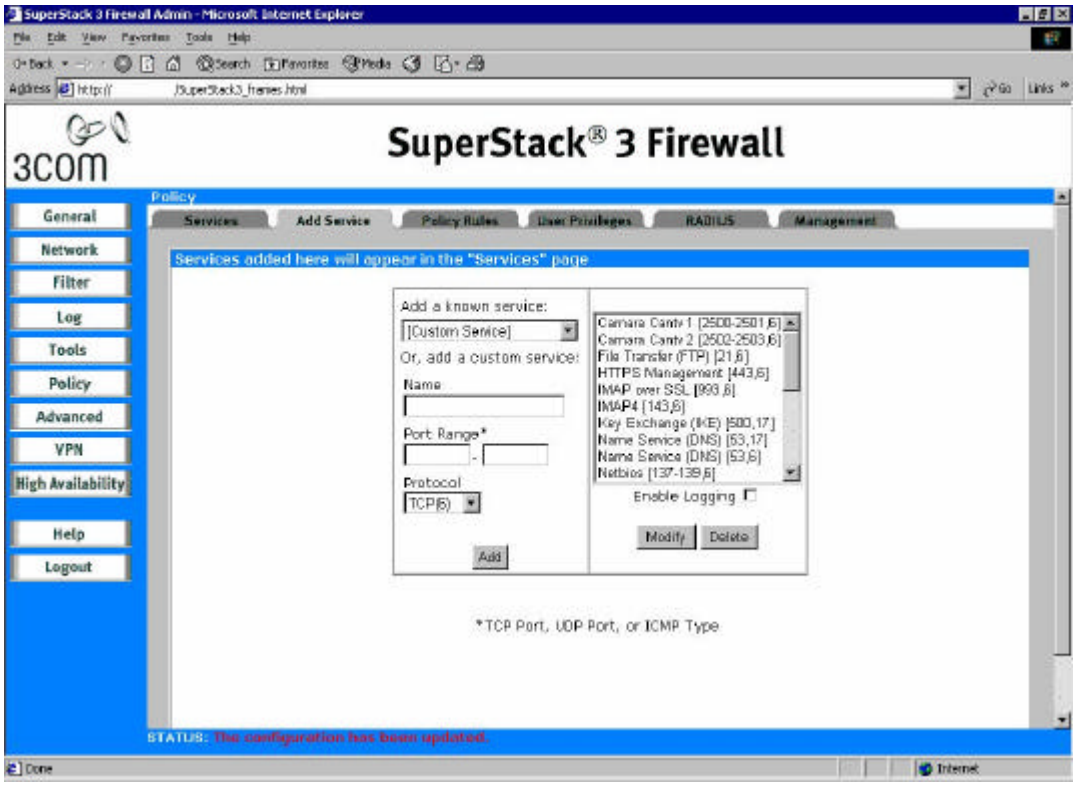
Anexo B: Muestra de configuraciones del Firewall 3Com SuperStack 3

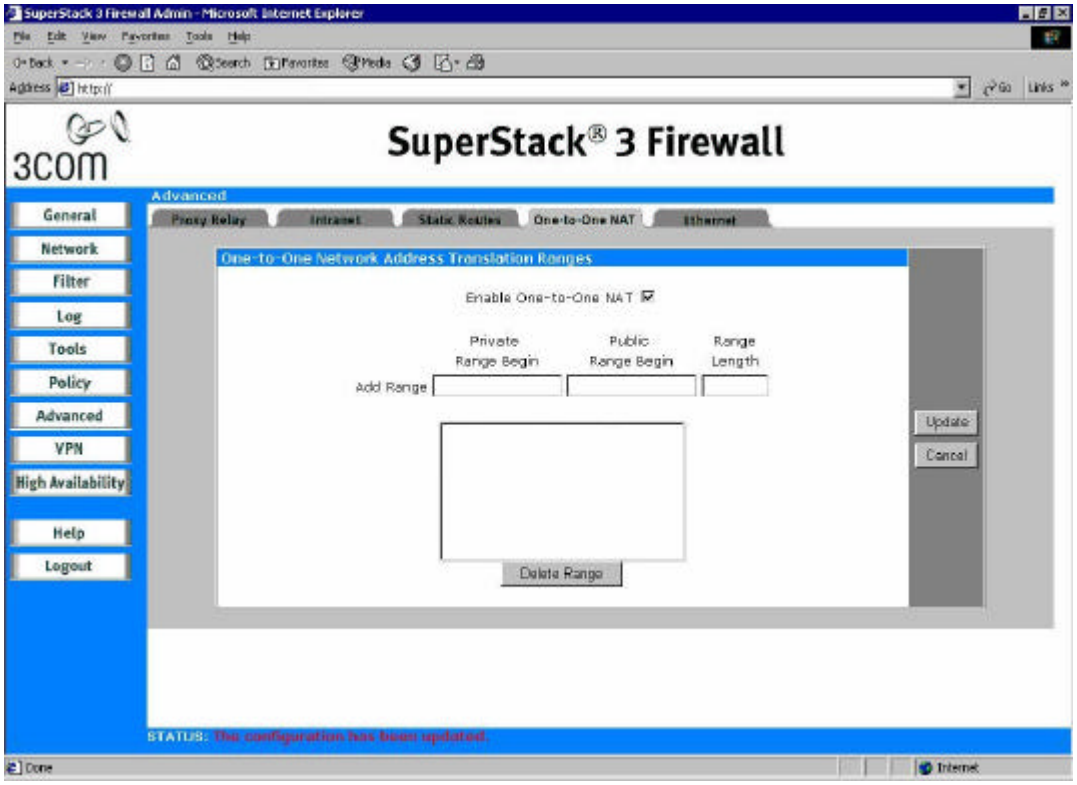
Muestra de algunas pantallas principales de la configuración del Firewall 3Com SuperStack 3

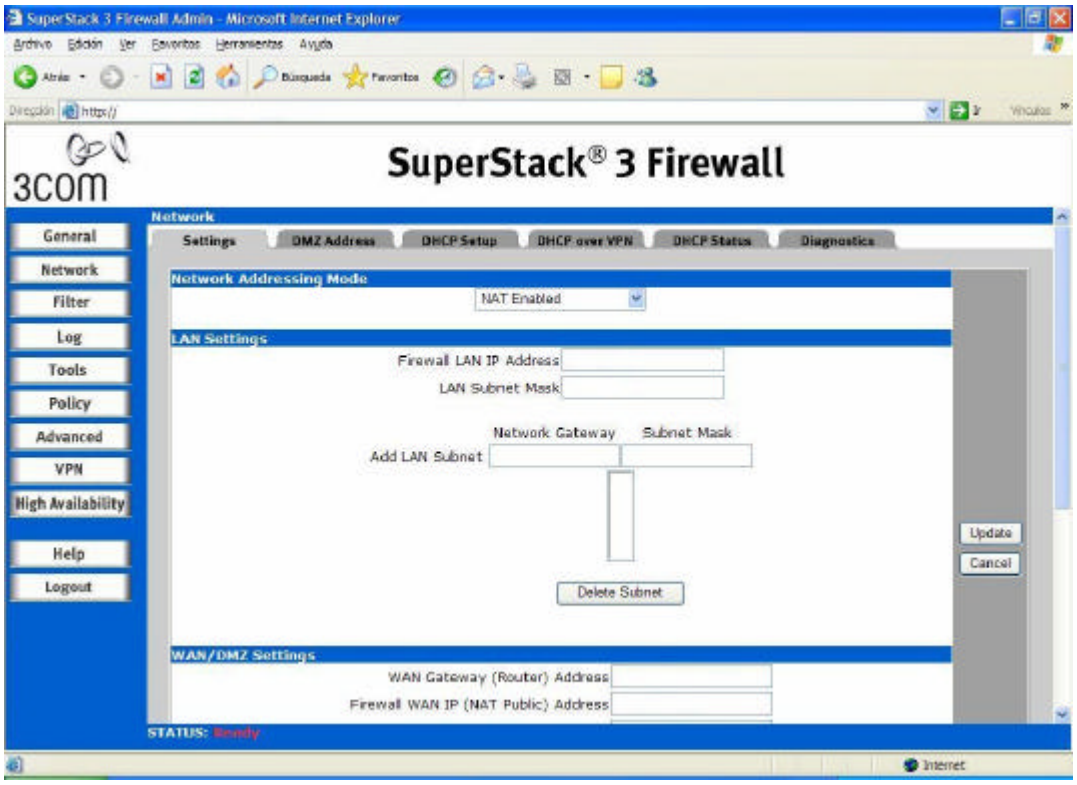


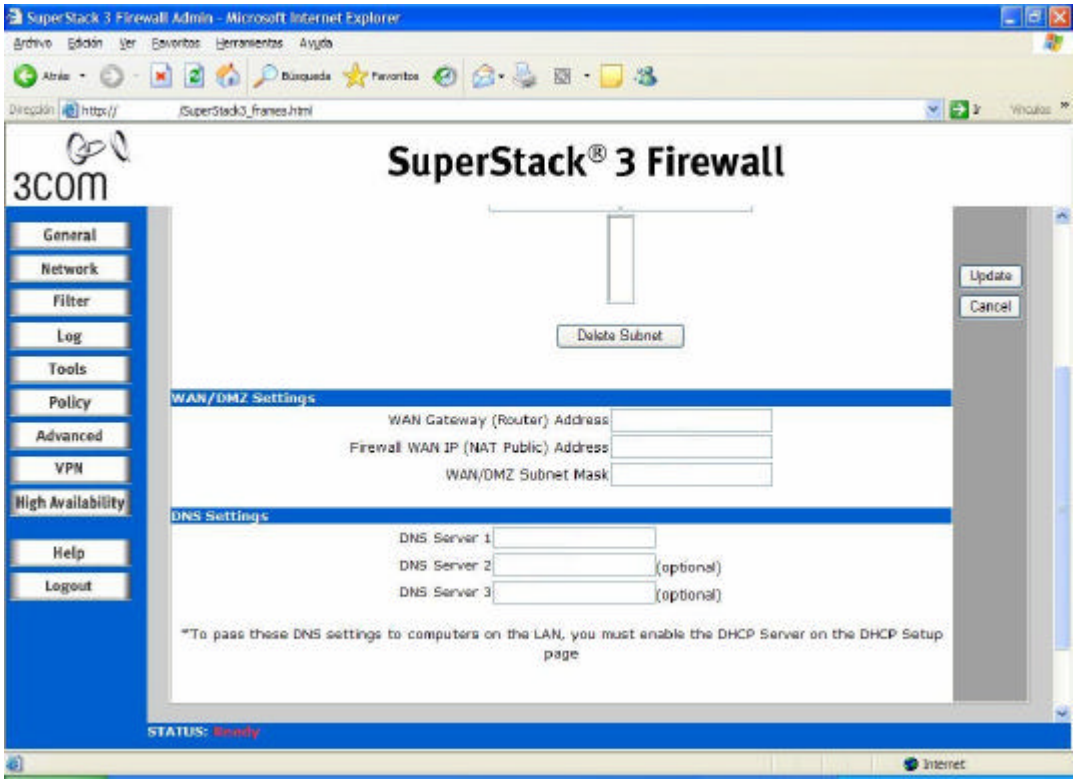


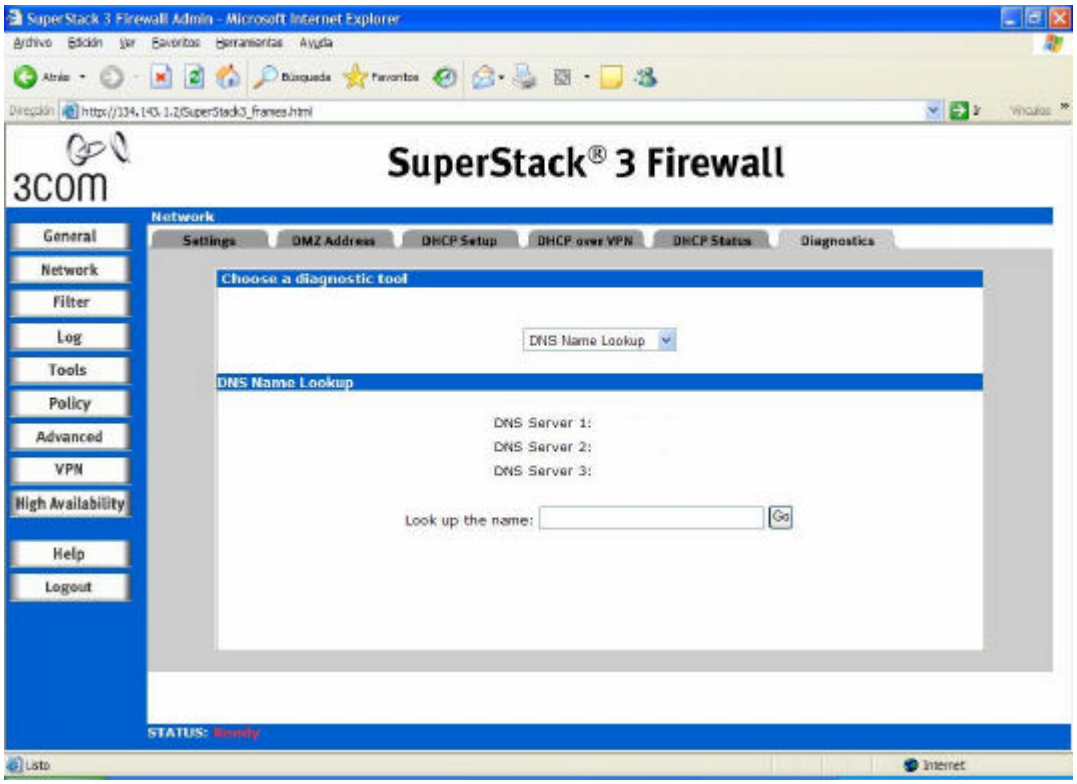

SuperStack 3 Firewall Admin - Microsoft Internet Explorer
SuperStack® 3 Firewall
3com
Network
General
Network
Filter
Log
Tools
Policy
Advanced
VPN
High Availability
Help
Logout
Settings
DMZ Address
DHCP Setup
DHCP over VPN
DHCP Status
Diagnostics
DMZ in Standard Mode
When you connect devices to your DMZ port, you need to specify their addresses here. You can add either single addresses, or ranges of contiguous addresses.
From Address
To Address
Add Range
Update
Cancel
Delete Range
DMZ in NAT Mode
DMZ Private Address
DMZ Subnet Mask
255.255.255.0
DMZ NAT Many to One Public Address (Optional)
0.0.0.0
STATUS: The configuration has been updated.
Done
Internet

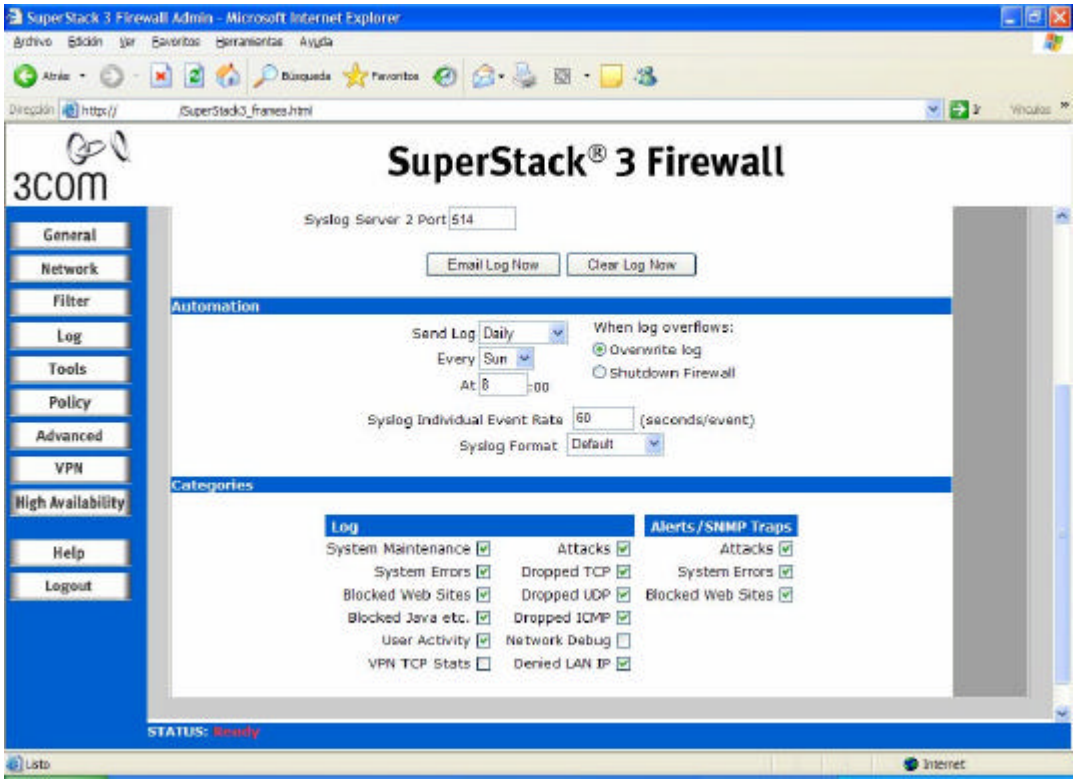

SuperStack 3 Firewall Admin - Microsoft Internet Explorer
SuperStack® 3 Firewall
3com
Policy
General
Network
Filter
Log
Tools
Policy
Advanced
VPN
High Availability
Help
Logout
Services
Add Service
Policy Rules
User Privileges
RADIUS
Management
Services added here will appear in the "Services" page
Add a known service:
[Custom Service]
Or, add a custom service:
Name
Port Range*
Protocol
TCP(6)
Add
Camara Cantv 1 [2500-2501,6]
Camara Cantv 2 [2502-2503,6]
File Transfer (FTP) [21,6]
HTTPS Management [443,6]
IMAP over SSL [993,6]
IMAP4 [143,6]
Key Exchange (IKE) [500,17]
Name Service (DNS) [53,17]
Name Service (DNS) [53,6]
Netbios [137-139,6]
Enable Logging
Modify
Delete
*TCP Port, UDP Port, or ICMP Type
STATUS: The configuration has been updated.
Done
Internet

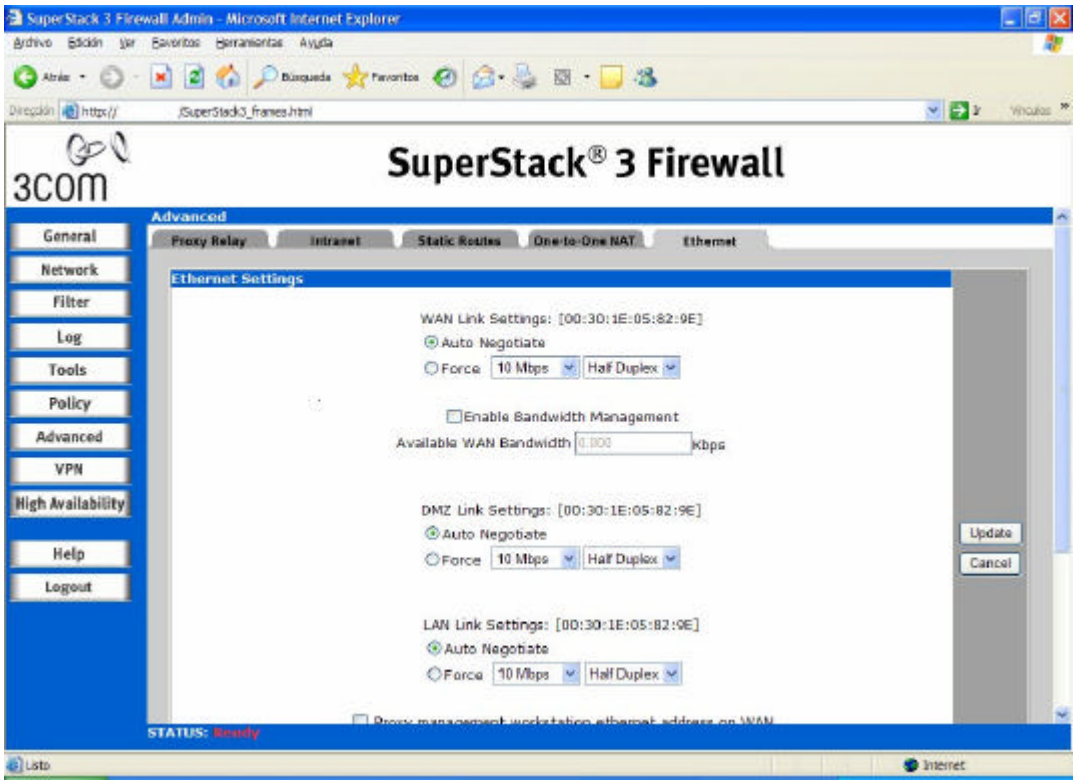

SuperStack 3 Firewall Admin - Microsoft Internet Explorer
SuperStack® 3 Firewall
3com
Advanced
General
Network
Filter
Log
Tools
Policy
Advanced
VPN
High Availability
Help
Logout
Proxy Relay
Intranet
Static Routes
One-to-One NAT
Ethernet
One-to-One Network Address Translation Ranges
Enable One-to-One NAT
Private Range Begin
Public Range Begin
Range Length
Add Range
Update
Cancel
Delete Range
STATUS: The configuration has been updated.
Done
Internet


SuperStack 3 Firewall Admin - Microsoft Internet Explorer
SuperStack® 3 Firewall
3com
Network
General
Network
Filter
Log
Tools
Policy
Advanced
VPN
High Availability
Help
Logout
Settings
DMZ Address
DHCP Setup
DHCP over VPN
DHCP Status
Diagnostics
Network Addressing Mode
NAT Enabled
LAN Settings
Firewall LAN IP Address
LAN Subnet Mask
Network Gateway
Subnet Mask
Add LAN Subnet
Update
Cancel
Delete Subnet
WAN/DMZ Settings
WAN Gateway (Router) Address
Firewall WAN IP (NAT Public) Address
STATUS: Ready
Internet


SuperStack 3 Firewall Admin - Microsoft Internet Explorer
SuperStack® 3 Firewall
General
Network
Filter
Log
Tools
Policy
Advanced
VPN
High Availability
Help
Logout
Update
Cancel
Delete Subnet
WAN/DMZ Settings
WAN Gateway (Router) Address
Firewall WAN IP (NAT Public) Address
WAN/DMZ Subnet Mask
DNS Settings
DNS Server 1
DNS Server 2 (optional)
DNS Server 3 (optional)
*To pass these DNS settings to computers on the LAN, you must enable the DHCP Server on the DHCP Setup page
STATUS: Ready


SuperStack 3 Firewall Admin - Microsoft Internet Explorer
SuperStack® 3 Firewall
Network
Settings
DMZ Address
DHCP Setup
DHCP over VPN
DHCP Status
Diagnostics
General
Network
Filter
Log
Tools
Policy
Advanced
VPN
High Availability
Help
Logout
Choose a diagnostic tool
DNS Name Lookup
DNS Name Lookup
DNS Server 1:
DNS Server 2:
DNS Server 3:
Look up the name:
Go
STATUS: Ready


SuperStack 3 Firewall Admin - Microsoft Internet Explorer
SuperStack® 3 Firewall
General
Network
Filter
Log
Tools
Policy
Advanced
VPN
High Availability
Help
Logout
Syslog Server 2 Port 514
Email Log Now
Clear Log Now
Automation
Send Log Daily
Every Sun
At 8 :00
When log overflows:
Overwrite log
Shutdown Firewall
Syslog Individual Event Rate 60 (seconds/event)
Syslog Format Default
Categories
Log
System Maintenance
System Errors
Blocked Web Sites
Blocked Java etc.
User Activity
VPN TCP Stats
Attacks
Dropped TCP
Dropped UDP
Dropped ICMP
Network Debug
Denied LAN IP
Alerts/SNMP Traps
Attacks
System Errors
Blocked Web Sites
STATUS: Ready


SuperStack 3 Firewall Admin - Microsoft Internet Explorer
SuperStack® 3 Firewall
Advanced
Proxy Relay
Intranet
Static Routes
One-to-One NAT
Ethernet
General
Network
Filter
Log
Tools
Policy
Advanced
VPN
High Availability
Help
Logout
Ethernet Settings
WAN Link Settings: [00:30:1E:05:82:9E]
Auto Negotiate
Force 10 Mbps Half Duplex
Enable Bandwidth Management
Available WAN Bandwidth kbps
DMZ Link Settings: [00:30:1E:05:82:9E]
Auto Negotiate
Force 10 Mbps Half Duplex
LAN Link Settings: [00:30:1E:05:82:9E]
Auto Negotiate
Force 10 Mbps Half Duplex
Update
Cancel
STATUS: Ready