PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE UNA ARQUITECTURA DE SEGURIDAD PERIMETRAL DE UNA RED DE COMPUTADORAS PARA UNA EMPRESA PEQUEÑA

Tesis para optar el Título de Ingeniero Electrónico, que presenta el bachiller:

JORGE LUIS VALENZUELA GONZALES

ASESOR: ING. LUIS ANGELO VELARDE

Lima, junio del 2012

Resumen

En el trabajo realizado se presenta una solución de seguridad perimétrica que cubra los requerimientos de una red de computadoras de una empresa pequeña. Se muestra además una simulación del diseño propuesto en un ambiente de pruebas controlado.

En el primer capítulo se presenta el estado actual y riesgos de la información, y la importancia de la misma. Se presenta además la seguridad perimetral de la red de datos como parte de una problemática mayor. La seguridad de la información.

En el segundo capítulo se muestra en detalle y de manera técnica, los riesgos, amenazas contra la integridad de una red de computadoras de una empresa pequeña y las contramedidas que pueden ser adoptadas.

En el tercer capítulo se explica el escenario de trabajo, sus requerimientos y sus necesidades sin especificar aun producto alguno, sea software o hardware.

En el cuarto capítulo se presentan los criterios que fueron tomados en consideración para la selección de la solución más idónea para el escenario planteado en el tercer capítulo.

En el quinto capítulo, se desarrollan la política de seguridad que debe ser aplicada en la solución seleccionada en el cuarto capítulo, se plasma en los componentes que la conforman y se evalúa su desempeño en un ambiente de pruebas.

Finalmente se presenta las conclusiones que se desprenden del análisis del escenario planteado, así como las recomendaciones para mantener un nivel de seguridad adecuado.

Dedicatoria

A mi madre, quien no ha dejado
de apoyarme en ningún momento
y constantemente me exhortó a culminar esta tesis.

Agradecimientos

A mi madre, quien siempre me apoyó y exhortó a culminar esta tesis. A mis compañeros de estudios con quienes conservo una estrecha amistad hasta la fecha. Al Ing. Angelo Velarde por su tiempo y dedicación como asesor para la presente tesis. Al Ing. Eduardo Ismodes por darme la confianza necesaria para culminar mis estudios, y a todos los demás profesores de la especialidad, que me motivaron a desarrollarla y culminarla. A Paulo Cesar Cisneros y Leslie Puelles, quienes me permitieron iniciar mi carrera en seguridad de la información al darme la oportunidad de trabajar en Trendcorp, y a todas las personas que conocí y que contribuyeron de manera directa o indirecta al desarrollo de este proyecto.

Índice

Lista de Figuras

Lista de Tablas

INTRODUCCION

Sin tomar en cuenta el tipo de negocio, acceder a Internet y promocionarse en él, ha dejado de ser una opción para convertirse en una necesidad. Una empresa que no se anuncia en una página Web o no cuenta con correo electrónico ya esta perdiendo una gran cantidad de negocios.

Sin embargo, en estas épocas ya no es suficiente con anunciarse en Internet sino proporcionar un servicio con el menor número de fallos posible (disponibilidad), asegurar a los visitantes que su información no será divulgada ni será expuesta a terceros (confidencialidad) y certificar que la información proporcionada no ha sido alterada en forma maliciosa (integridad).

Ante la necesidad de garantizar estos tres requerimientos, las empresas se han visto en la necesidad de proteger sus servicios valiéndose de una gran diversidad de productos.

No obstante, la seguridad de la información no debe tratarse como un producto sino como un proceso largo y continuo que debe adaptarse ante las nuevas particularidades del entorno tecnológico.

Capítulo 1

El problema de la seguridad de la información en Internet

1.1 El Internet y sus riesgos

Actualmente el Internet es una red abierta, gratuita y cualquier red u ordenador puede conectarse sin mayor costo que la conexión. El Internet está formado por un conglomerado de nodos de conexión e información viajando de un lugar a otro del mundo.

La inexistencia de restricciones en el Internet ha provocado que los virus, troyanos y otros códigos maliciosos se propaguen entre los ordenadores, principalmente a través del correo electrónico y páginas Web, permitiendo a personas inescrupulosas obtener información u tomar control de ellos, o utilizarlos para realizar algún ataque contra otro sitio. Estos ataques se pueden agrupar en las siguientes categorías.

- Entrada no autorizada

  Este es uno de los ataques más frecuentes y de mayor impacto. Algunos ejemplos son la modificación de sitios Web y modificar transacciones.

- Negación de servicio

  Una caída de servicio puede ser provocada por un ataque desde algún lugar en la red. Muchos no lo saben, pero desde sus pc's pueden estar siendo lanzados ataques hacia ciertos sitios de Internet. A estos equipos se les conoce como zombis o redes zombis en general.

- Sustitución y suplantación del servicio

  Consiste en hacerse pasar por un servidor o servicio para obtener información vital de los usuarios. Uno de los mejores ejemplos es el *phishing*.

1.2 El valor de la información

Definir o establecer el valor de la información o datos es absolutamente relativo pues, a diferencia de los equipos, la documentación o las aplicaciones, es un recurso intangible. Sin embargo, debido al incremento en el uso del Internet como herramienta de negocio, las páginas Web, los servidores de correo electrónico, entre otros, se convierten en piezas fundamentales dentro del negocio de la empresa.

Por ejemplo, tener el sitio Web de compra de pasajes de una aerolínea por 20min puede significar miles en perdidas.

Adicionalmente, el acceso no autorizado a los servidores de base de datos de clientes de una empresa de comercio puede significar grandes pérdidas.

Se debe considerar además, el tema de la reputación de la empresa. Ser víctima de un ataque efectivo, puede verse desde el punto de vista de los clientes o futuros clientes como una clara muestra de falta de seguridad y de confiabilidad.

1.3 Seguridad de la información

Antiguamente se pensaba que la seguridad de la información era un asunto meramente técnico que debía ser resuelto mediante la utilización de un componente tecnológico. Se creía incluso que el costo de este componente podía ser incluido dentro del presupuesto de otros departamentos, como por ejemplo, TI (Tecnología de la Información).

Hoy en día no es solo un aspecto tecnológico, muy por el contrario, es una solución integrada que combina estrategias, procesos y tecnología. Si no se cuenta con reglas, responsabilidades y procedimientos definidos, y con personal capacitado para la gestión de los procesos, la inversión en tecnología no es más que una pérdida de dinero.

La seguridad de la información debe lograr el equilibrio adecuado entre la protección y la habilitación de acceso a los activos de información. Debe enfocarse en proteger la información de la organización contra pérdidas o uso indebido de la misma.

1.4 Variables que influyen en la seguridad perimetral de una red

La tecnología de seguridad perimetral existente se basa en un firewall cuya función es proteger la red interna contra conexiones provenientes desde el internet así como la de publicar los servicios de la empresa; un proxy de navegación a Internet que permite controlar de manera bastante rudimentaria los accesos a la navegación a Internet y un servidor *antispam* ubicado en la red interna y al cual todos equipos de red (incluyendo computadoras) tienen acceso y pueden enviar correos a través de él. Este y otros accesos indebidos, son parte de los nuevos requerimientos de seguridad perimetral de la empresa. Requerimientos que fueron extraídos de la normativa que los regula.

En la actualidad existe una gran variedad de productos y soluciones de seguridad, firewalls, preventores de intrusos, sistemas de control de acceso, autenticación fuerte, filtro de contenidos, entre otros, que ofrecen un alto grado de seguridad. Es en este punto donde las empresas consultoras se posicionan

en una ubicación estratégica al cumplir la tarea de seleccionar, no la mejor solución (que no necesariamente es la más cara) sino la solución que mejor se adapte a la red corporativa. Afortunadamente las empresas vienen tomando conciencia de la importancia y necesidad de proteger su información, lo que ha facilitado la tarea de estos consultores e integradores.

Sin embargo, es importante recalcar que ni la mejor solución de seguridad es efectiva si el personal que lo administra no cuenta con la cultura, conocimiento y habilidad para plasmar los intereses de la empresa en estos dispositivos. La continua capacitación de este personal es aun más importante que la misma solución implementada.

1.5 Declaración del Marco Problemático

La seguridad de la información fue hasta hace algunos años un tema que solo se escuchaba en las grandes empresas, mayormente debido a su alto costo de adquisición Sin embargo, éste ya no es un tema exclusivo de las grandes empresas.

Existen actualmente una gran cantidad de soluciones al alcance de todos, pero esto ha conllevado a otro problema aun mayor. La falta de información o desconocimiento pueden llevar a adquirir e implementar soluciones de seguridad que no cubran las necesidades reales de la red o que den una falsa sensación de seguridad.

Es importante por esto conocer primero el estado de la red que se quiere proteger y luego buscar la solución más adecuada, no solo evaluando las diferentes soluciones existentes en el mercado sino también enterarse de las tendencias de la seguridad de la información ya que para cuando una solución sea implementada y puesta en marcha, puede ya haber quedado obsoleta.

Capitulo 2

Solución de Seguridad Perimetral para una red de computadoras

2.1 Estado del Arte

2.1.1 Presentación del Asunto de Estudio

En el mundo actual la interconexión de millones de dispositivos: computadoras personales, notebooks, servidores, teléfonos celulares, pda's, etc., es el centro de la actividad comercial moderna. Gracias a estas redes, personas y empresas pueden intercambiar información, y extender sus relaciones y negocios rompiendo las barreras del idioma, distancia y tiempo. La interconexión que hace posible esta comunicación, es también la causa de su vulnerabilidad, pues una entrada que permite el acceso a alguien autorizado también puede convertirse en el punto de ingreso de indeseables, ladrones o maliciosos.

Es por este motivo que tan importante como el delimitar las puertas de acceso, es saber quien ingresa, desde donde ingresa, como lo hace y que es lo que hace una vez que haya ingresado.

A continuación se presentan las tecnologías actuales utilizadas para elevar el nivel de seguridad perimetral, protegiéndola contra intrusiones, accesos no autorizados y otras amenazas para asegurar la continuidad del negocio

2.1.2 El Estado de la Investigación

Antes de buscar la mejor solución de seguridad, debemos primero estar conscientes de qué es lo que queremos proteger, para que lo queremos proteger, y aun mas importante, de que lo queremos proteger.

Si queremos proteger nuestra casa contra robos, lo primero que hacemos es buscar las posibles rutas de acceso a los ladrones, como lo son las puertas, ventanas, tragaluces (vulnerabilidades). El siguiente paso es averiguar como podrían los ladrones ingresar: forzando la cerradura de la puerta o rompiendo la ventana con una piedra (amenazas). Una vez que tenemos esta bien claro, recién podemos pensar en cambiar la cerradura a la puerta o ponerle una cerradura adicional, y/o colocar rejas en nuestras ventanas (contramedidas).

2.1.2.1 Amenazas y Ataques

Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como puede ser un servidor de archivos o de correo, a un destino, como por ejemplo un usuario o un cliente Web. Una amenaza se convierte en ataque cuando ésta es ejecutada.

De acuerdo a su comportamiento, Stamp diferencia las amenazas en pasivas y activos, los cuales a su vez pueden ser agrupadas en cuatro categorías principales: interrupción, intercepción, modificación y fabricación.

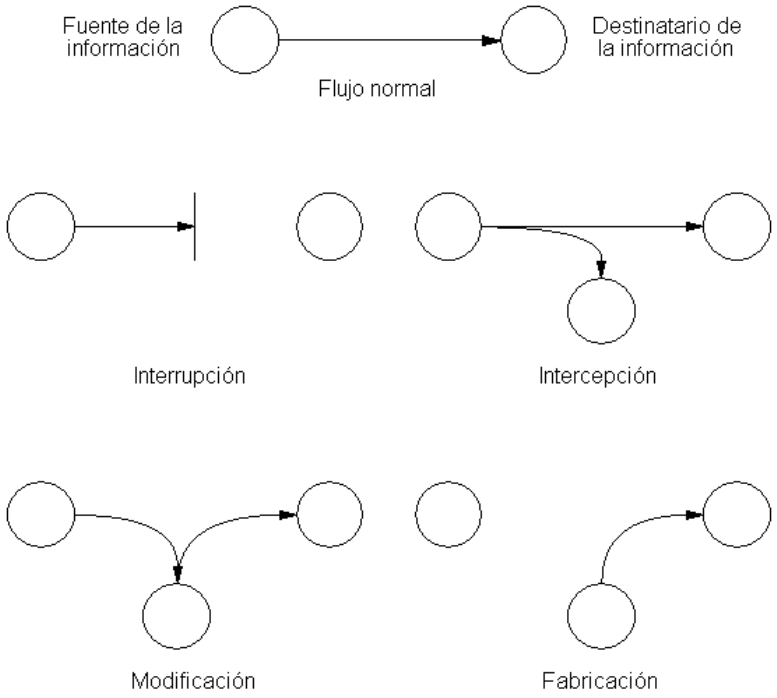

FIGURA 2.1 CLASIFICACION DE ATAQUES DE RED

Fuente: “Stamp” [STA2005]

- **Interrupción**

  Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque directo contra la disponibilidad. Como ejemplo de ataque tenemos el Ataque de Denegación de Servicios, bombas lógicas y a los *Worms* o gusanos.

- **Intercepción**

  Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser

una persona, un programa o un equipo. Por ejemplo un spyware o Caballos de Troya.

- **Modificación**

  Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo, modificar sus funciones y la información que maneja. Ejemplo: Virus, Hackers.

- **Fabricación**

  Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Por ejemplo: *Phishing* y *Farming*.

2.1.2.2 Contramedidas

Dentro de las soluciones tecnológicas que actualmente están disponibles para reforzar la seguridad de una red, los Cortafuegos son muy populares.

Adicionalmente existen en el mercado una buena cantidad de productos conocidos como Sistemas de Detección de Intrusos - IDS (Intrusión Detection System). Estos sistemas basan su funcionamiento en la recolección y análisis de información de diferentes fuentes, que luego utilizan para determinar la posible existencia de un ataque o penetración de intrusos y cuentan con la capacidad para identificar falsos positivos..

Existen también soluciones como los *Web Application Firewall, Proxies reversos* y otras soluciones que son soluciones de aplicación muy específica.

a. Cortafuegos (Firewall)

Los Firewall son utilizados para restringir el acceso desde una red hacia otra. La mayoría de las empresas utiliza los firewalls para restringir el acceso a usuarios de Internet hacia su red. Un firewall soporta y refuerza las políticas de seguridad de red de una empresa. Estas políticas pueden ser definidas en forma muy granular, estableciendo los servicios que pueden ser accedidos, las direcciones ip's o rangos que deben ser restringidos y que puertos pueden ser utilizados.

Actualmente los firewall son pasarelas que pueden ser ruteadores, servidores de autenticación o equipos de aplicación especifica. Monitorean los paquetes que entran y salen desde la red que protegen. Filtran los paquetes que no cumplen con los requerimientos de la política

de seguridad. Pueden descartar estos paquetes, re-empaquetarlos o re-direccionarlos dependiendo de la configuración del firewall y de las políticas de seguridad. Estos paquetes son filtrados de acuerdo a la dirección fuente o destino, puerto o servicio, tipo de paquete, protocolo, entre otros.

Existen diferentes tipos de firewalls disponibles actualmente ya que cada escenario puede tener requerimientos únicos así como metas de seguridad específicas. A continuación se presentan las diferentes tecnologías de Firewalls.

- **Filtro de Paquetes (Packet Filtering)**

  Este tipo de filtro está basado en la información de la capa de red. El firewall puede tomar decisiones basado en la información de la cabecera solamente, la cual es limitada. Este tipo de firewall es considerado de primera generación debido a que fueron los primeros en ser creados y usados.

- **Inspección de Estado (Stateful Inspection)**

  La inspección de estado requiere que el firewall conserve una tabla de estado (state table), la cual es como una ficha donde guarda quien dijo que a quien. Cuando un equipo con filtro de paquetes con inspección de estado recibe un paquete, éste primero mira en su tabla de estado para ver si existe una conexión establecida y si esta información fue requerida. Si no existe una conexión previa y la tabla de estado no tiene información sobre el paquete, el paquete es comparado con la ACLs. Si la ACL permite este tipo de tráfico, el paquete puede ingresar a la red. Si no esta permitido, el paquete es desechado.

  Si bien esto provee un nivel extra de protección, también agrega más complejidad ya que el equipo debe ahora mantener una tabla de estados dinámica y recordar las conexiones.

- **Proxy Firewalls**

  El concepto de proxy es el de re-direccionar un requerimiento a una entidad separada. Un proxy se coloca entre redes confiables y no confiables, y realiza la conexión en ambos sentidos, en nombre de la fuente. De esta manera, si un usuario en Internet requiere enviar información a una computadora dentro de la red protegida, el proxy tomará este requerimiento y lo analizará en búsqueda de información sospechosa. El requerimiento no va directamente al equipo destino.

- **Proxies de Aplicaciones**

  Los proxies de aplicación inspeccionan el paquete entero y toman la decisión de dejarlo pasar o no basándose en el contenido del paquete. Son capaces de entender diferentes servicios y protocolos y los comandos utilizados en los mismos. Un proxy de aplicaciones puede distinguir entre un comando FTP GET y un FTP PUT, por ejemplo, y puede tomar una decisión dependiendo del nivel de granularidad establecido en las políticas.

- **Filtro de paquetes dinámico**

  Cuando un sistema necesita comunicarse con un equipo fuera de la red de confianza, éste tiene que escoger un puerto fuente de manera que el sistema sabe a donde responder. El puerto que puede escoger debe estar por encima del puerto 1024, ya que puertos con numeración inferior a este valor corresponden a servicios específicos o ya definidos, o son puertos reservados. Una vez definido el puerto de comunicación, el firewall crea una ACL que permita al equipo que esta fuera de su red a comunicarse con el equipo interno vía este puerto. Cuando la conexión termina o es cortada por algún motivo, la ACL es limpiada.

  El beneficio del firewall con filtro de paquetes dinámico, también conocido como firewall de cuarta generación es que tiene la opción de permitir cualquier tipo de tráfico de salida y sólo el tráfico de entrada como respuesta.

- **Proxy Kernel.**

  Los Kernel Proxy son considerados firewalls de quinta generación. Se diferencian de todos los demás firewalls en que puede crear su propia pila TCP/IP personalizada cuando los paquetes tienen que ser evaluados.

  Cuando un paquete llega al firewall, una nueva pila de protocolos es creada y con solo los protocolos o proxies que son necesarios para analizar estos paquetes. Si es un paquete FTP, solo el proxy FTP es llevado a esta pila. El paquete es analizado en cada nivel de la pila, es decir, el data link header va a ser evaluado, tanto como el network header, transport header, entre otros.

  Los Proxy de Kernel son más rápidos que los firewall de aplicaciones debido a que el análisis y el procesamiento son hechos en el kernel y no necesita pasar por un software de nivel más alto que el del sistema operativo.

- **Otras características**

  Adicionalmente a las ya mencionadas tecnologías, existen otras características que algunos fabricantes ofrecen en sus productos y que pueden causar que un cliente opte por uno u otro producto. Entre estas características están: Web cache, Administración centralizada, filtro anti-spam, alta disponibilidad, manejo de VPNs, filtro de páginas Web.

b. Sistemas Detectores de Intrusos (IDS)

Los Sistemas Detectores de intrusos (IDS) son utilizados para monitorear una red o un grupo especifico de computadoras. Los IDS pueden ser configurados para buscar ataques, analizar logs de auditoría, alertar al administrador cuando los ataques suceden, proteger sistemas de archivos, exponer técnicas de hackeo, mostrar que vulnerabilidades necesitan ser trabajadas, entre otros.

- **Detección de Intrusos basada en firmas**

  Las firmas son modelos de cómo los ataques son realizados y como pueden ser identificados o detenidos. Cada ataque identificado tiene una firma, la cual es utilizada para detectar un ataque en progreso o determinar si ha ocurrido alguno en la red. Cualquier acción que no es reconocida como un ataque es considerado aceptable. La efectividad del tipo de protección depende de la periodicidad con que el software es actualizado con nuevas firmas o ataques conocidos. Este tipo de IDS es débil contra posibles nuevos ataques ya que solo puede reconocer los ataques que tiene previamente identificados.

- **Detección de Intrusos basado en comportamiento**

  Este tipo de software observa y detecta variaciones del comportamiento esperado de los usuarios y los sistemas. Una referencia del comportamiento habitual de los usuarios es compilado y todos las futuras actividades son comparadas con estas.

  A este tipo de IDS también se les conoce como estadísticos y pueden detectar nuevos y desconocidas vulnerabilidades, pero también pueden causar muchas falsas alarmas.

  Cuando un ataque es detectado, pueden suceder muchas cosas, y esto depende de la capacidad del IDS y de las políticas que le han sido asignadas.

c. Otras soluciones

Existen otras soluciones como gateways de correo electrónico y proxies reversos, que no se consideran elementos de seguridad perimetral ya que su función es proteger un servicio específico.

2.1.3 Síntesis del asunto de estudio

Cada día, las empresas se vuelven más dependientes de sus redes informáticas, al punto aplicaciones como el Intranet, el Extranet y el correo electrónico se hay convertido en aplicaciones críticas para el negocio y que cualquier problema que las afecte, por mas mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.

Por otro lado, cada vez es mayor el número de atacantes y cada vez están más organizados. Van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Es en este punto en que las tecnologías de seguridad adquieren una importancia vital. Previniendo la corrupción de datos, robo de información, el acceso no autorizado y para eliminar las vulnerabilidades de los sistemas.

Para otorgarle un alto nivel de seguridad a las comunicaciones, cada institución debe revisar sus procesos, conocimientos y estructura organizacional, así como sus dispositivos hardware y herramientas software de seguridad. Es importante aclarar en este punto lo siguiente:

La seguridad se define a nivel de proceso, no a nivel de producto.

Las tecnologías por sí mismas sirven de poco. Es lo que la gente hace con ellas lo que marca la diferencia.

Siempre hay que tener en cuenta que la seguridad comienza y termina con personas.

2.2 Modelo Teórico

Es importante tener en cuenta la relación entre seguridad, grado de utilización y costo. Es posible tener una seguridad y capacidad de utilización pero con un alto costo en términos de dinero, tiempo y de personal. Se puede lograr que sea menos costoso y más utilizable. No es difícil tampoco conseguir que algo sea eficaz en cuanto a costos, sin embargo, conseguir que algo sea seguro y utilizable implica un gran esfuerzo. De ahí que la seguridad requiera planificación y recursos.

Claro está que para los administradores de red, el costo de la solución no es lo primero en su lista de prioridades al seleccionar el mejor producto. Lo que busca es la solución que realice el trabajo en forma más eficiente y efectiva, y sea más fácil de utilizar y desplegar por su personal. Lamentablemente la decisión final no está en las manos del administrador de red, y si en el gerente financiero, o el mismo dueño en el caso de empresas pequeñas, para el cual el costo si es un factor predominante y busca siempre el precio más bajo para algo que el piensa que no es “muy” necesario para él.

Es en este punto donde un análisis de riesgo cobra importancia pues permite dar una visión de los costos de la solución de seguridad y contrastarlo con lo que costaría para la empresa la perdida de alguna de sus funcionalidades debido a la falta de seguridad.

Finalmente, los administradores de seguridad se enfrentan a variables interesantes. Básicamente, la opción que debe realizarse es entre un sistema que sea seguro y utilizable, un sistema que sea seguro y barato, o un sistema que sea barato y utilizable. No es posible tenerlo todo.

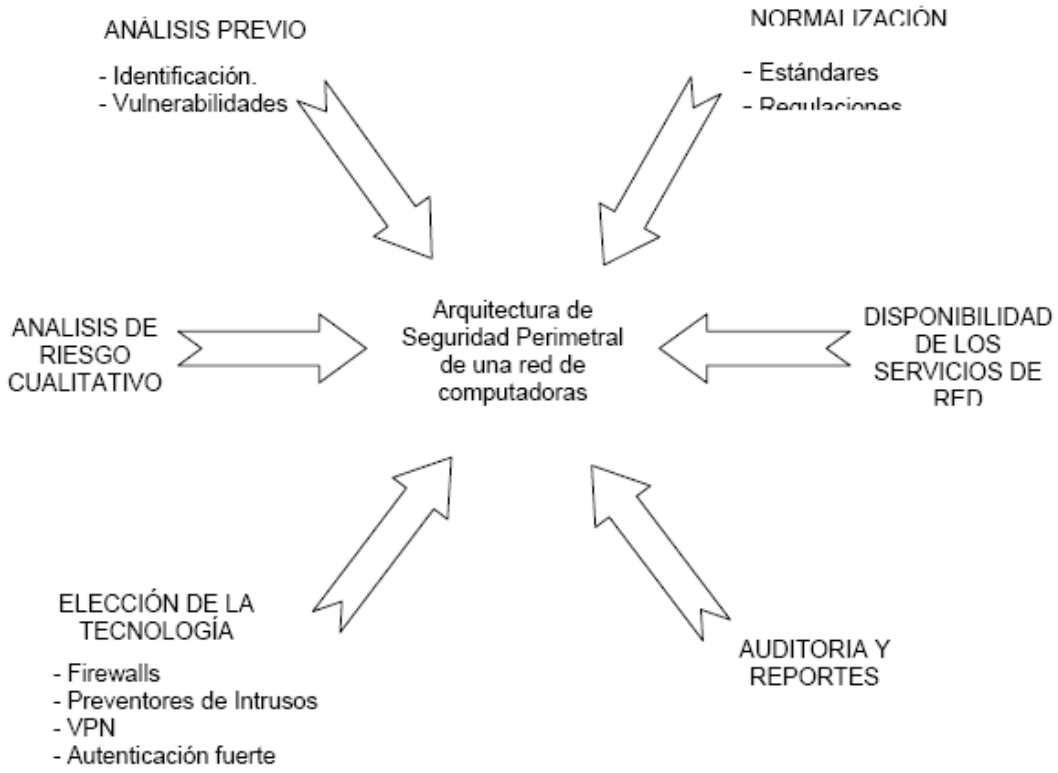

FIGURA 2.2 MODELO TEORICO

La figura 2.2 muestra la representación grafica del modelo teórico expuesto, además de la información y recursos necesarios para poder diseñar una arquitectura de seguridad para una red de datos.

2.3 Definiciones operativas

2.3.1 Indicadores Cualitativos

Permiten conocer la calidad, los grados de mejora de ciertas características clave en el manejo de la seguridad de una red.

- **Calidad del Servicio de Acceso a los servicios de red**

  Medido en función a la velocidad de acceso a los servicios de la empresa y a Internet. Estos factores influirán en gran manera en la percepción que los usuarios tengan del servicio y productos proporcionados.

- **Satisfacción del Cliente**

  Se puede percibir mediante la evaluación de las quejas y/o sugerencias que tengan los usuarios acerca de la disposición de los servicios de red. Depende de la adecuada estructuración y configuración de políticas en los elementos de seguridad de red agregados a la misma.

- **Capacidad del Personal de Gestión de Seguridad**

  Relativo al personal técnico encargado del monitoreo de la red y de los elementos de seguridad implementados. Su capacidad ayudará a resolver los potenciales problemas que pudiesen presentarse, de una manera rápida y eficiente.

- **Facilidad de aplicación de nuevas políticas de seguridad**

  Se refiere a cuán fácil es aplicar un cambio en la configuración de los elementos de seguridad de la red tanto cuando la red funciona correctamente como en situación de crisis.

2.3.2 Indicadores Cuantitativos

Indica numéricamente los logros o degradaciones de ciertas características del servicio de acceso a Internet residencial.

- **Disponibilidad del servicio**

  Es el tiempo, en porcentaje, que un servicio específico se mantiene operativo en forma continua.

- **Tiempo de respuesta para la solución de problemas**

  Implica el tiempo en el cual la empresa responde ante cualquier consulta por parte del cliente, así como el tiempo que le toma a éste solucionar el problema en cuestión. Incluye el tiempo que demora la empresa volver a poner en línea el servicio afectado.

- **Tiempo de Respuesta ante problemas**

  Este indicador está relacionado con la capacidad y habilidad del personal para detectar e identificar un problema en un servicio publicado hacia Internet.

- **Costos en Adquisición y Mantenimiento de la solución**

  Se refiere a los costos que tendrá la empresa para poder brindar el nivel de seguridad deseado a la red. Incluye también el costo la capacitación de su personal de seguridad y del servicio de soporte técnico.

Capitulo 3

Diseño de la arquitectura de la solución de seguridad perimetral

3.1 Presentación del escenario de trabajo

3.1.1 La empresa

La empresa para la cual se hizo el diseño se dedica a la elaboración y comercialización de materiales de construcción. Cuenta con una única sede ubicada en Lima. El número aproximado de trabajadores es de 120 personas, de las cuales aproximadamente 60 personas realizan trabajo de oficina, 10 trabajo de campo y el resto realizan trabajos en planta. El índice de crecimiento en personal de la empresa es de aproximadamente un 10% por año.

La necesidad de renovar, tecnológicamente hablando, el equipamiento de seguridad de redes es el resultado de un incidente de seguridad reportado semanas antes de realizado el análisis contenido en la presente tesis.

El incidente consistió en un alto deterioro del desempeño de la red, el cual no pudo ser resuelto de manera rápida debido a que los equipos con los que se contaba no permitieron analizar la situación debido a sus limitaciones técnicas y a la falta de acceso administrativo. Luego de ser atendido el incidente, la gerencia aceptó la necesidad de actualizar la plataforma actual.

3.1.2 La red

La red de computadoras a protegerse al momento de iniciar los trabajos se encuentra montada según se presenta en la figura 3.1.

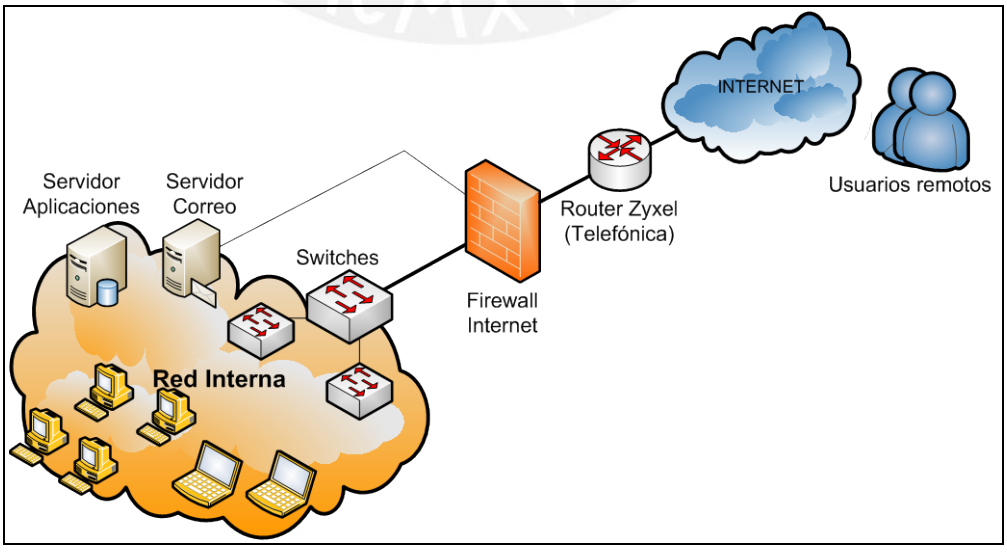

FIGURA 3.1 DIAGRAMA DE RED INICIAL

La figura 3.1 fue obtenida luego de entrevistar al personal encargado del area de sistemas y corroborarlo mediante una visita a su centro de cómputo.

La red está conformada principalmente por los siguientes elementos:

- **Router de Internet**

  Entregado y configurado por el proveedor de internet para interconectar la red de la empresa con su red WAN y permitirle el acceso a Internet.

- **Firewall de Internet (o de perímetro)**

  El firewall de acceso a Internet es un equipo Firewall Dlink con una antigüedad mayor a 6 años al cual se le hizo las siguientes observaciones:

  - No es posible administrarlo vía web o línea de comandos a través de la red.
  - El único medio de acceso para su administración es a través del puerto serial.
  - Nadie en la empresa conoce los comandos para administrar el firewall.
  - No es posible visualizar la configuración que se ejecuta en el dispositivo.

  De acuerdo al análisis realizado y la información entregada por la empresa el firewall cumple con las siguientes funciones:

  - Publicación del servidor de correo para envío y recepción de correos desde internet.
  - Publicación de la pagina web y correo web corporativos.
  - Publicación mediante escritorio remoto del servidor de aplicaciones para el acceso de usuarios externos.
  - Permitir la navegación a internet de los usuarios de la red interna.

- **Switches**

  La empresa cuenta con 6 switches que permiten interconectar todos los equipos de la red interna: pc's, laptops, servidores y firewall de internet.

  Todos los switches encontrados son "no administrables", es decir, su configuración no puede ser modificada y funcionan únicamente en el

nivel 2 de OSI y no cuentan con otras funcionalidades a las de interconexión de equipos.

- **Servidor de Correo**

  El servidor de correo es un servidor con 02 procesadores Intel Xeon de 1.6Ghz, 4GB de Memoria RAM, capacidad de almacenamiento de 68GB y 02 interfaces de red, con el siguiente software instalado:

  - Microsoft Windows Server 2003 R2 en español, como sistema operativo del servidor.
  - Microsoft Windows Domain Controller 2003, como Controlador de Dominio de la red de la empresa.
  - Microsoft Exchange Server 2003 en español, como Servidor de Correo Electrónico.
  - Microsoft OWA Web Access, como interface web para el acceso de los usuarios para visualizar sus casillas de correo electrónico.
  - Microsoft ISA Server, como servidor proxy para el control del acceso de los usuarios hacia internet.
  - Microsoft SQL Server, como motor de base de datos para las aplicaciones de la empresa.
  - McAfee GroupShield for Exchange, como solución antispam instalada e integrada con el servidor Microsoft Exchange Server 2003.
  - McAfee Antivirus Client, como solución antivirus para el servidor.
  - Symantec Backup Exec Solution, como solución de copia de respaldo de servidores.

- **Servidor de Aplicaciones**

  El servidor de aplicaciones es un servidor con 02 procesadores Intel Xeon de 1.6Ghz, 4GB de Memoria RAM, capacidad de almacenamiento de 68GB y 02 interfaces de red, con el siguiente software instalado:

  - Microsoft SQL Server 2000, como motor de base de datos de las aplicaciones de la empresa.
  - Microsoft Terminal Server, para permitir el acceso de los usuarios que se conectan desde internet vía escritorio remoto.
  - McAfee Virus Scan Enterprise, como solución corporativa de antivirus para equipos de computo y servidores.

- McAfee Antivirus Client, como solución antivirus para el servidor.
- McAfee ePolicy Orchestor, como consola de administración de la solución antivirus corporativa.

- **Red Interna**

  Conformada por aproximadamente 60 equipos de computo, impresoras y Access Points.

3.2 Requerimientos de la solución

La implementación de una solución de seguridad perimetral es solo una parte de los requerimientos de la empresa en cuanto a renovación tecnológica. Durante la etapa de levantamiento de información se detectó falencias en cuanto a las condiciones de operación de sus equipos de cómputo y mantenimiento de los mismos, sin embargo, ese tema se encuentra fuera del alcance de la presente tesis.

A continuación se presentan todos los requerimientos de la solución manifestados por el cliente. En el punto 4 del capítulo 4 se verificará el cumplimiento de estos requerimientos que correspondan al diseño de la solución de seguridad perimetral, motivo de la presente tesis.

- Una solución de les permita proteger la red de ataques provenientes desde internet.
- Aprovechar de manera efectiva el servicio de internet, permitiendo tener visibilidad y control en todo momento del tráfico saliente y entrante.
- Control granular de acceso a Internet de direcciones URL y protocolos.
- Seguridad y granularidad en el acceso a los usuarios que se conectan de manera remota desde internet, pudiendo llevar un registro de sus accesos.
- Mínimo impacto sobre los demás elementos de red y usuarios. Es decir, que la implementación de la nueva solución de seguridad no afecte de manera negativa en la manera en que los usuarios desempeñan sus funciones.
- Reutilizar en la medida de lo posible los productos de seguridad con los que actualmente cuenta la empresa.

3.2.1 Requerimientos de administración y gestión

De acuerdo a las exigencias presentadas por el cliente, los requerimientos para la implementación de la solución de seguridad son:

a. Gestión de la solución.

Como regla principal para la gestión de los distintos componentes de la solución de seguridad, se deben definir grupos, roles y responsabilidades para la administración lógica de los distintos componentes de la solución, de manera que sea posible identificar cada cambio realizado: sea creación o modificación de nuevas reglas en la política de seguridad.

b. Reglas generales para el control de acceso.

- No permitir la conexión de direcciones de red internas desde el Internet hacia la DMZ (antispoofing).
- Bloquear todo tráfico entrante/saliente no declarado como permitido.
- Implementar una DMZ que filtre y analice cualquier tráfico, para prohibir el acceso directo desde y hacia el Internet, desde la red de usuarios.
- Utilizar NAT para enmascarar todo el tráfico saliente hacia Internet.
- Todo acceso requerido desde internet debe realizarse a través de un medio seguro y encriptado.

c. Reglas de asignación de un único ID por usuario

- Identificar a todos los usuarios con un único usuario antes de brindarle acceso a los sistemas desde internet.
- Implementar al menos uno de los siguientes métodos de autenticación para todos los usuarios
  - Contraseña.
  - Token
  - Biometría
- Implementar autenticación de dos factores para el acceso remoto de los empleados, administradores y terceros.

- Habilitar el acceso remoto al proveedor solo durante el tiempo necesario para la tarea requerida.
- Requerir una longitud mínima de las contraseñas a un mínimo de 9 caracteres.
- Forzar que las contraseñas de los usuarios cuenten con caracteres numéricos y alfanuméricos.
- Prohibir el re-uso de contraseñas con una antigüedad menor a cinco cambios.
- Bloquear una cuenta de usuario luego de seis intentos fallidos de acceso.

d. Política de evaluación constantemente la seguridad de los sistemas y procesos

- Realizar escaneos de vulnerabilidades externos e internos constantemente y cada vez que se implemente un nuevo sistema, componente de red, o se realice algún cambio en la topología de la red o a nivel del firewall.
- Realizar pruebas de penetración al menos una vez al año y cada vez que se realice una modificación en la red.
- Utilizar sistemas de detección de intrusos para monitorear todo el tráfico de la red y alertar sobre eventos sospechosos.
- Mantener los detectores de intrusos actualizados

3.2.2 Requerimientos técnicos

Los requerimientos técnicos de la solución son los siguientes.

- Capacidad de alta disponibilidad en modo activo-pasivo en ambos firewalls.
- Capacidad de configuración de enlace de respaldo en el firewall perimetral.
- Aplicación de filtro de paquetes dinámico en los firewalls.
- Bloqueo de ataques de negación de servicio.
- Capacidad de bloqueo de ataques o intentos de intrusión.

Adicionalmente existen requerimientos específicos para cada elemento de seguridad, los cuales serán utilizados como primer criterio para la selección de los equipos a utilizarse para construir la solución.

a. Firewall Perimetral e Interno

- Capacidad para configurar túneles VPN
- Soporte de IPv6
- Soporte de traslación de direcciones de red (NAT, NAPT, PAT)
- Soporte de VoIP
- Control de flujo y ancho de banda
- Capacidad de prevención de intrusos, filtro de contenido y antivirus embebido
- Capacidad de manejar más de un enlace hacia internet

b. Control de Acceso Remoto (VPN SSL)

- Acceso basado en políticas
- Capacidad de otorgar los accesos por dirección destino y puerto o aplicación, por usuario o grupo de usuarios, y por horarios (granularidad)
- Control de acceso de acuerdo a regulaciones de seguridad.
- Comunicación encriptado entre el cliente y el dispositivo VPN.
- No necesidad de cliente instalado.
- Soporte para equipos Mac de Apple.

c. Control de acceso a Internet

- Capacidad de aplicar políticas por usuarios y grupos de usuarios definidos en el directorio activo de la empresa.
- Filtro de protocolos de Internet
- Capacidad para filtrar direcciones en internet por su dirección y/o su dirección IP.

3.2.3 Requerimientos adicionales

Debido al alto grado de lentitud detectado en el servidor de correo, se realizó un análisis detallado del uso de los recursos del mismo, lo cual se realizó de acuerdo a la siguiente metodología:

a. Consumo total de memoria RAM del equipo y distribución por servicio o aplicación.

b. Consumo total de CPU del equipo y distribución por servicio o aplicación.

c. Accesos totales de I/O (lectura/escritura) en disco duro por servicio o aplicación.

d. Identificación de aplicaciones y/o servicios que provocan la degradación del desempeño del servidor

Las graficas 3.2 y 3.3 muestran el detalle de los recursos utilizados por los diferentes servicios y aplicaciones en el servidor de correo.

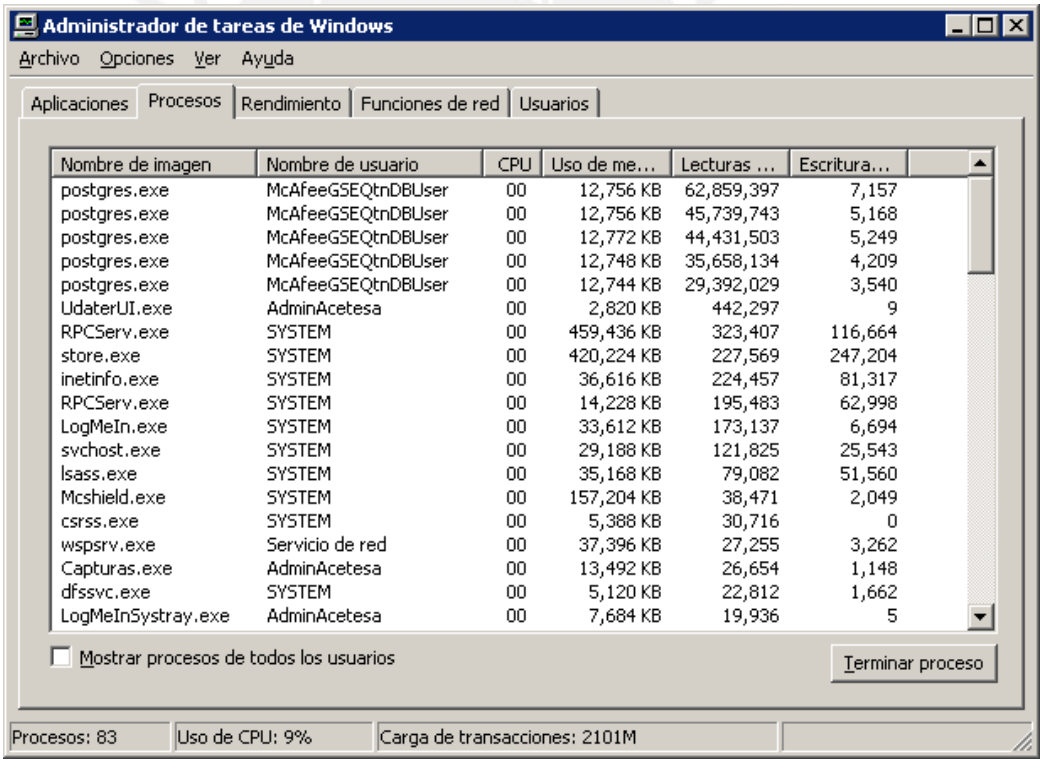

FIGURA 3.2 PRIMERA GRAFICA DE RECURSOS DE SERVIDOR DE CORREO

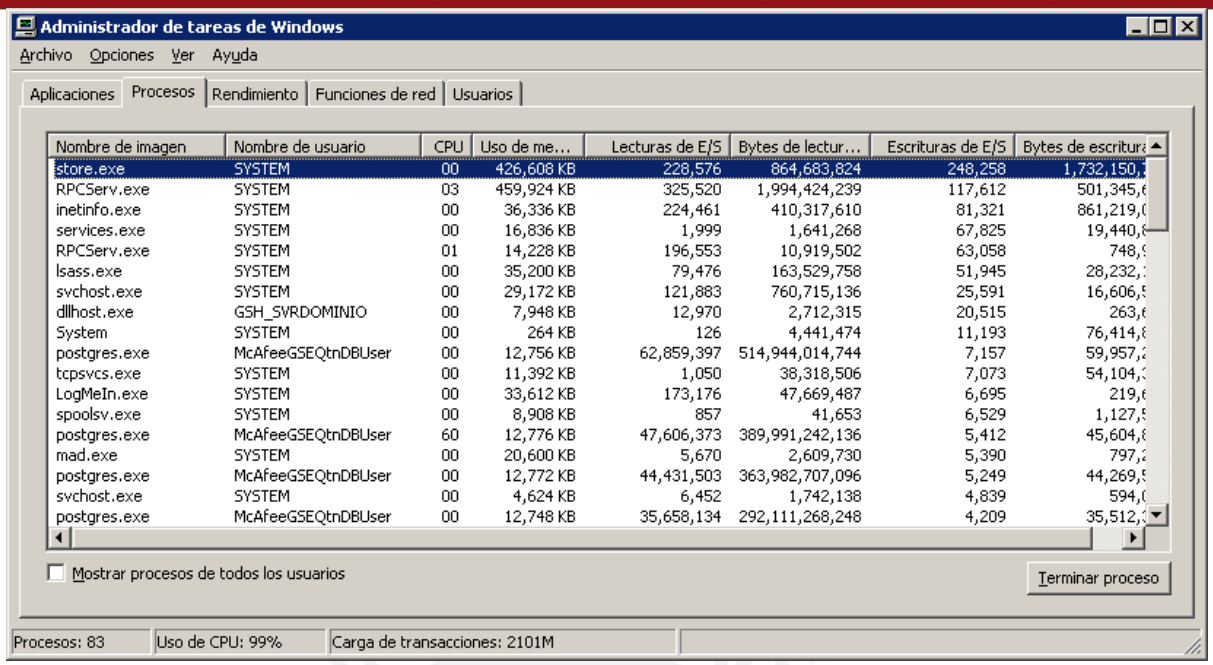

FIGURA 3.3 SEGUNDA GRAFICA DE RECURSOS DE SERVIDOR DE CORREO

La información mostrada en las figuras 3.2 y 3.3, obtenidas mediante las herramientas provistas por el mismo sistema operativo, fue trasladada a una tabla resumen, la cual se muestra a continuación.

TABLA 3.1 RESUMEN DE USO DE RECURSOS EN SERVIDOR DE CORREO

Software	Memoria utilizada (MB)	% CPU Utilizado	Lectura/Escritura en disco (kbytes)
McAfee Groupshield	522.90	42	18000
McAfee AV	157.00	10.5	50
MS Exchange 2003	406.72	9.8	227
OS/ otras aplicaciones	1,027.30	7.7	500
Total	2,113.92	70	

La tabla 3.1 muestra un resumen de los servicios y aplicaciones que consumen la mayor cantidad de recursos en el equipo. A partir de esta tabla se obtuvieron las graficas 3.4, 3.5, 3.6, presentadas en los puntos siguientes

a. Memoria utilizada. Distribución de la memoria RAM utilizada por las distintas aplicaciones, software y programas instalados en el servidor.

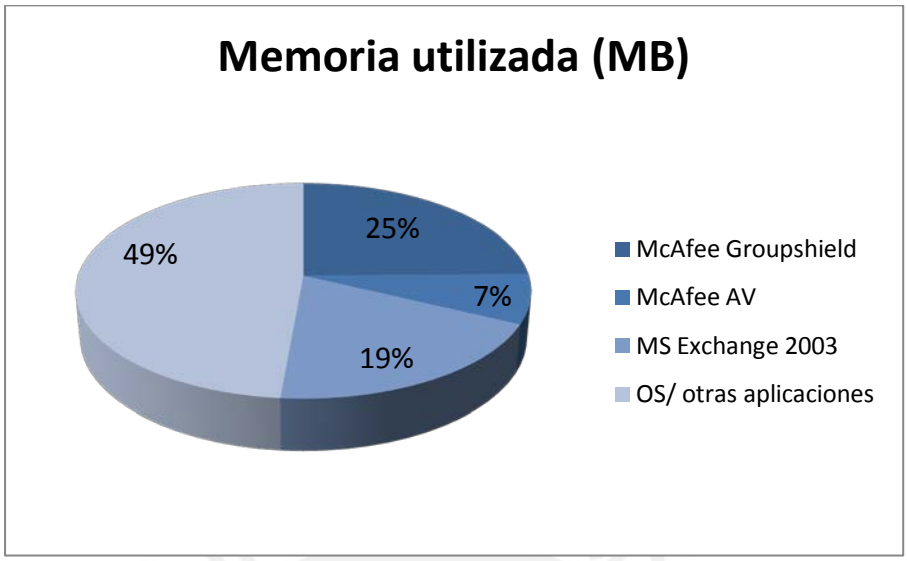

FIGURA 3.4 DISTRIBUCION DE LA MEMORIA UTILIZADA EN EL SERVIDOR DE CORREO

No se encontró ningún comportamiento anómalo en el uso de la memoria en el servidor.

b. %CPU Utilizado. Corresponde a la distribución del uso de los recursos de procesamiento del servidor por las distintas aplicaciones, software y programas que se encuentran ejecutándose en el equipo, considerando que el uso promedio total de CPU es de 70%.

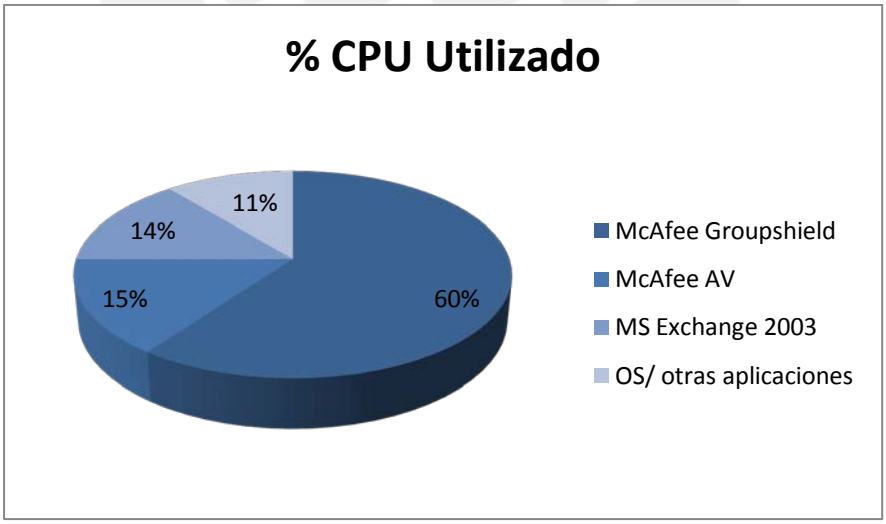

FIGURA 3.5 DISTRIBUCION DEL USO DEL PROCESADOR EN EL SERVIDOR DE CORREO

De acuerdo a la figura 3,5, las aplicaciones de McAfee utilizan casi el 50% del CPU, lo cual no es un comportamiento normal y puede ser un indicio de que un comportamiento anómalo.

c. Lectura/Escritura en disco. Corresponde a la cantidad de información que ha sido accedida/escrita en el disco duro por las diferentes aplicaciones, software y programas que se encuentran ejecutándose en el equipo.

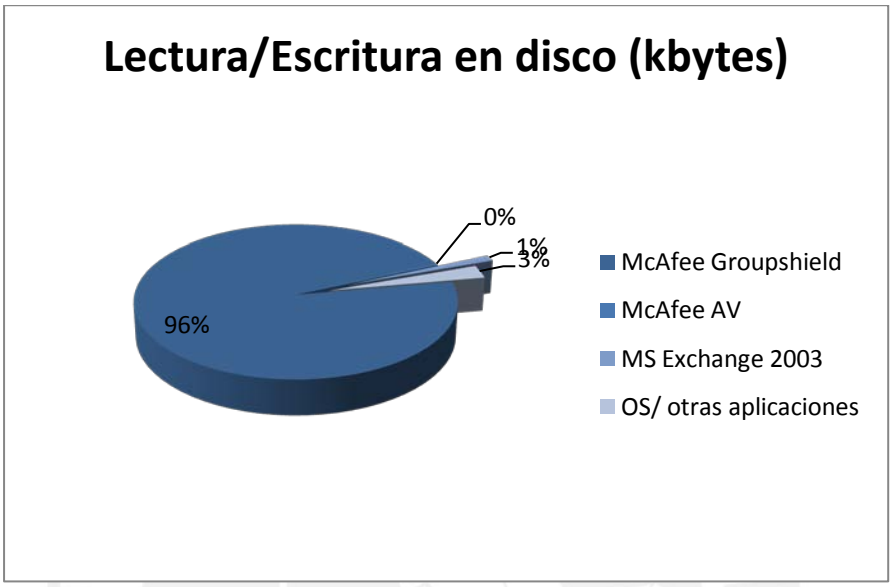

FIGURA 3.6 DISTRIBUCION DE LA CANTIDAD DE ACCESOS AL DISCO DURO EN EL SERVIDOR DE CORREO

La figura 3.6 muestra que el servicio GroupShield de McAfee realiza demasiados accesos al disco duro. Un número muy alto de accesos de lectura/escritura en el disco duro puede causar que el servidor muestre lentitud y mantenga el CPU en continuo funcionamiento debido a que tiene que esperar que la información sea transferida desde/hacia el disco duro a la memoria del equipo para trabajarla.

El análisis arrojó que el servidor se encontraba sobrecargado debido a la existencia de aplicaciones que consumen recursos del equipo. Se sugirió remover el McAfee Groupshield ya que al realizar un gran número de consultas y tareas de escritura en el disco duro provoca que el servicio de correo electrónico sea lento.

Debido al carácter concluyente de la información recopilada mediante el uso de las herramientas propias del equipo, y basada en la experiencia del personal a cargo del análisis, no se consideró necesario el uso de herramientas de terceros ni un análisis exhaustivo del tráfico de red.

De acuerdo a la información provista por el McAfee, esto se debe a que cada correo que ingrese al servidor, sea entrante o saliente, es escrito tres veces en disco: en la cola de ingreso, en la cola de procesamiento, en la cola de envíos; antes de ser enviado al servidor de correo, el cual, también lo

almacena en disco. Esto significa que cada correo procesado por el servidor es escrito y accedido del disco cuatro veces.

Es recomendación del fabricante además, que el antispam se ubique fuera del servidor de correo.

Es imperativo remover esta aplicación del servidor no solo para mejorar el rendimiento del mismo sino para evitar el deterioro de los componentes físicos debido a la alta carga de trabajo.

De esta manera se logrará reducir la cantidad de accesos I/O al disco duro del servidor de correo, el cual, como ya se mencionó antes, cumple también la función de controlador de dominio, lo cual lo convierte en un servidor de misión critica para la empresa al ser el único que servidor de autenticación.

El *antispam* será colocado en una zona desmilitarizada (DMZ) por temas de diseño tal y como se menciona en el siguiente punto.

3.3 Diseño de la nueva arquitectura de seguridad perimetral

3.3.1 Recomendaciones y buenas prácticas

Matt Curtin se refiere a la DMZ, abreviación de “zona desmilitarizada”, como parte de la red que no pertenece directamente ni a la red interna ni a Internet. Recomienda también colocar en esta zona todos los equipos que se publican en Internet o tienen un acceso directo al mismo. Por ejemplo el servidor Web, la pasarela de correo electrónico, entre otros.

Es por este motivo que se sugiere colocar los siguientes equipos en la DMZ:

- Servidor Web
- Servidor antispam o “gateway de correo electrónico”
- Concentrador VPN SSL
- Servidor Proxy de navegación a Internet

Se sugiere además colocar el IPS de Internet o Externo protegiendo directamente la DMZ y no el segmento que va a Internet, para poder detectar cualquier ataque o tráfico anómalo proveniente de las redes internas hacia estos servidores, además del tráfico proveniente desde Internet.

3.3.2 Nueva arquitectura

De acuerdo a los requerimientos presentados y a las recomendaciones realizadas, la arquitectura de red propuesta es la mostrada en la figura 3.7.

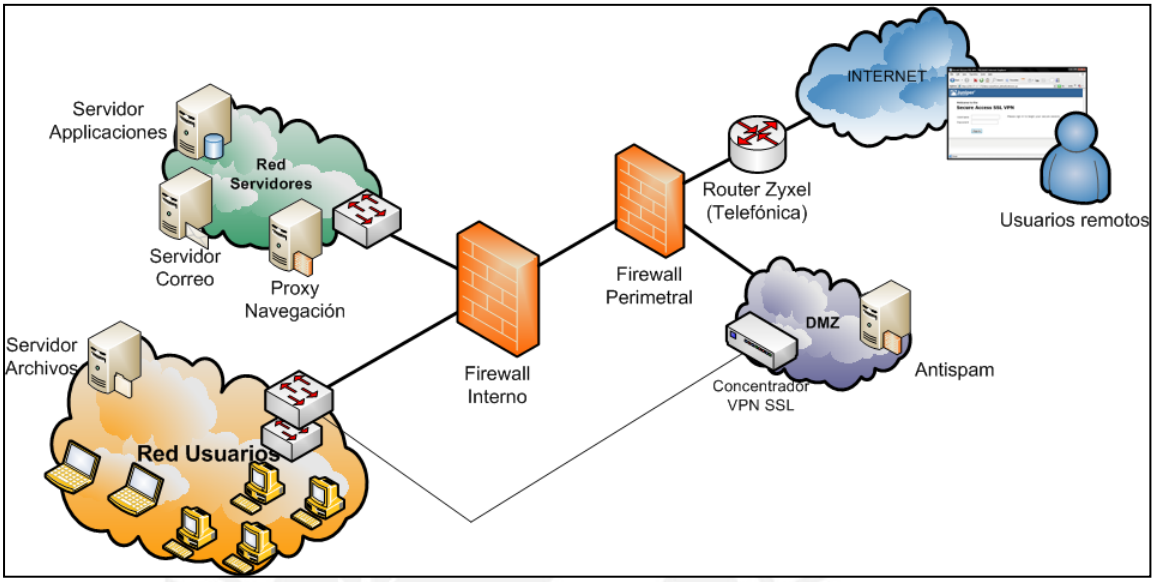

FIGURA 3.7 DIAGRAMA DE RED PROPUESTO

Si bien el diagrama propuesto contempla la arquitectura propuesta para toda la red de datos de la empresa, para efectos de la presente tesis, se describe únicamente la arquitectura propuesta para la seguridad perimetral,

La arquitectura de seguridad perimetral contempla:

a. La implementación de un firewall perimetral que cumpla las funciones de control de acceso hacia/desde internet; y cumpla con los requerimientos técnicos expuestos en el punto 3.2.2. Contará con tres zonas de seguridad:

   - Zona Internet. En esta zona se conecta el firewall al router de internet y manejará las direcciones IP públicas.
   - Zona DMZ. En esta zona se ubicará el servidor antispam y el concentrador VPN SSL.
   - Zona Interna. En la cual se conecta la red de datos de la empresa, considerando como tal, los servidores internos, equipos de red y computadoras de los usuarios.

b. Implementación de un concentrador VPN-SSL. El cual tendrá la función de proveer el acceso a usuarios remotos de manera granular y garantizando la seguridad en la conexión, de acuerdo a las condiciones que se exponen más adelante.

El detalle de los componentes que conforman el nuevo diseño se presenta a continuación.

Es importante recordar que en éste punto se presenta únicamente cómo estarán interconectados los componentes propuestos. La configuración y política que se les aplicará será vista mas adelante.

3.3.3 Componentes de la nueva arquitectura.

La red de datos de la empresa estará conformada por los equipos mencionados a continuación y cumpliendo sus respectivas funciones señaladas para cada uno de ellos, definidas en respuesta a los requerimientos establecidos anteriormente:

a. Router de Internet.

Entregado y configurado por el proveedor de internet para interconectar la red de la empresa con su red WAN y permitirle el acceso a Internet.

b. Firewall Perimetral.

Cumplirá con los requerimientos técnicos mencionados en el punto *"3.2.2.1 Firewall Perimetral e Interno"* y tendrá la función de controlar la comunicación entre la red interna e internet mediante reglas y políticas de control de acceso y prevención de intrusos.

El firewall perimetral contará con la siguiente configuración:

a. Tres zonas de seguridad: *Internet, DMZ* y *RedInterna*, comunicadas entre si solo a través de los protocolos de comunicación establecidos como permitidos en la política de seguridad del firewall. En la zona *Internet* se encontrará conectado el router de internet que permite la interconexión con la red WAN del ISP y el acceso a Internet. La DMZ estará conformada por el antispam y el concentrador VPN. La Red Interna corresponde a la red de usuarios y servidores que, vistos desde la perspectiva del firewall perimetral, son una única red.

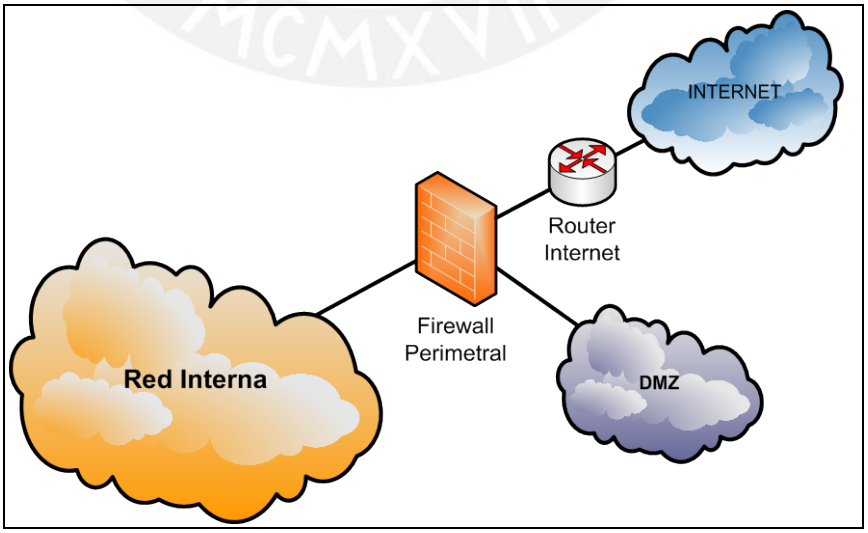

FIGURA 3.8 ZONAS DE SEGURIDAD EN EL FIREWALL PERIMETRAL

La figura 3.8 muestra la topología sugerida para la empresa. Se puede notar la existencia de la zona DMZ, sugerida en el punto 3.3.1.

b. Políticas o reglas de control de acceso: que establecerán que dispositivos podrán conectarse hacia y desde la zona "Red Interna" con la DMZ, y controlar la comunicación entre la DMZ e Internet.

c. Reglas de prevención de intrusos: que considera el análisis y verificación de la sanidad del tráfico que está atravesando el firewall o cortafuegos en sus diferentes direcciones.

c. Concentrador VPN SSL.

Cumplirá la función de crear un canal de comunicación seguro que le permita a un usuario ubicado en internet a acceder a los recursos de la red interna que el perfil de acceso asociado a su cuenta de usuario le permita.

El canal seguro estará conformado por un túnel VPN cifrado con un certificado SSLv2 de 128 bits entre el concentrador VPN y la computadora del usuario.

Para que el usuario pueda conectarse via VPN, es necesario que ingrese al sitio web publicado en HTTPS por el concentrador VPN SSL, ingresar su cuenta de usuario y contraseña. Una vez que éstos datos son validados, se crea automáticamente el canal seguro entre el equipo y la computadora del usuario.

d. Antispam.

Cumplirá la función de retener todo correo considerado como no deseado o "correo basura" mediante diferentes técnicas que incluyen: método heurístico de detección de spam, políticas de control de contenido, consultas de reputación de direcciones IP y listas negras, entre otros.

Los únicos canales de comunicación necesarios para el funcionamiento del antispam son: comunicación mediante el protocolo SMTP con el servidor de correo de manera bidireccional, al igual que hacia Internet; y acceso a Internet via DNS para realizar sus consultas con los servidores de listas negras y de reputación, y HTTPS para actualizar su motor antispam.

e. Proxy de navegación.

Cumplirá la función de controlar el acceso de los usuarios hacia internet. Limitará su acceso a los protocolos HTTP y HTTPS y restringirá las direcciones IP y sitios webs que de acuerdo a la política de seguridad de la empresa no deban ser accedidos por los usuarios.

f. Firewall Interno.

Cumplirá la función de controlar el acceso de los usuarios a los servidores para que éstos solo accedan a los programas y aplicaciones necesarios para la realización de sus funciones dentro de la empresa. Uno de los accesos que tendrán los usuarios hacia la red de servidores será el que les permita utilizar su cliente de correo electrónico corporativo.

Este componente si bien no es parte de esta tesis, es un elemento que formó parte del proyecto y por lo tanto debe ser mencionado.

3.3.4 Dimensionamiento de los dispositivos de seguridad

Luego de presentada la nueva arquitectura es necesario seleccionar los dispositivos que van a conformar la solución. Establecer los requerimientos mínimos de capacidad de los equipos será nuestro segundo criterio de selección.

a. Criterios para el dimensionamiento del Firewall Perimetral

Los criterios a tener en cuenta para el dimensionamiento de este elemento son, entre otros:

- numero de interfaces de red y su velocidad
- capacidad de procesamiento de paquetes por segundo (*throughput*)
- número máximo de sesiones concurrentes soportadas
- capacidad de crear/abrir nuevas sesiones o conexiones por segundo.

Es importante notar que no se debe seleccionar un equipo que cumpla estrictamente con los requerimientos actuales pues los equipos pueden quedar obsoletos ante el crecimiento de la empresa y de la red de datos. Es por este motivo, y teniendo en cuenta el crecimiento de la empresa se considerarán equipos que ofrezcan por lo menos un 30% más de los recursos requeridos obtenidos a través de las mediciones.

a. Throughput del firewall. Considerando que manejará tráfico entre la red interna y la DMZ, y DMZ e Internet, se hizo una evaluación de la tasa de transferencia de paquetes en la LAN y se obtuvo que el valor máximo es de 60Mbps.

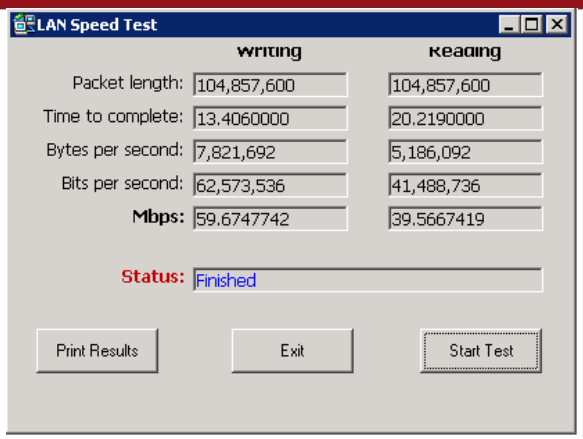

FIGURA 3.9 TASA DE TRANSFERENCIA MAXIMA EN LA RED INTERNA

La figura 3.9 muestra los resultados obtenidos con la herramienta *Lan Speed Test,* utilizada para medir la velocidad de transferencia dentro de la red. Dicha medición se realizó entre el servidor de correo actual y un equipo conectado al mismo switch al que se encuentra conectado dicho servidor. Cabe mencionar que la velocidad establecida en las interfaces de red de los servidores es de 100Mbps debido a que ésta es la capacidad de los switches.

De esta manera, el *throughput* requerido en el firewall es de:

Throughtput. = 60Mbps + 2Mbps = 62Mbps

El valor de 60Mbps proviene de las mediciones realizadas. El valor de 2Mbps proviene del ancho de banda provisto por el servicio de internet.

b. Número máximo de sesiones concurrentes soportadas. Dado que no fue posible obtener este valor dada las limitaciones del equipamiento e infraestructura de red de la empresa, se utilizó una aproximación utilizada por distintas empresas nacionales como Trendcorp, ITCorp, Eplus Soluciones, Sidif, entre otras - todas ellas con larga trayectoria en el dimensionamiento de soluciones de seguridad de redes – para obtener un valor útil aproximado. La fórmula utilizada es,:

Sesiones de los usuarios = 20 * #usuarios

Donde 20 es una aproximación utilizada de manera empírica y obtenida de la cantidad de ventanas del navegador de internet que un usuario puede tener abierta y en uso (4), más la cantidad de consultas de DNS requeridas para resolver las direcciones IP de las páginas web que está visitando.

Sesiones del servidor de correo = 120

Donde se considera que el servidor antispam mantiene abierto no más de 40 sesiones para recibir nuevos correos e igual número para el envío de éstos hacia internet. Las cuarenta sesiones restantes corresponden a

las consultas DNS realizadas por cada sesión abierta para enviar/recibir correos.

De esta manera, el valor mínimo del máximo de sesiones concurrentes que debe soportar el firewall es de:

Max. Sesiones = 20*60 + 120 = 1320 sesiones

Considerando un crecimiento de la red en un 50%, y redondeando el valor se obtiene:

Max. Sesiones = 3000 sesiones concurrentes

c. Nuevas sesiones/segundo. Considerando que un usuario no puede abrir más de una ventana del navegador de internet por segundo, y que el servidor de correo no abre más de 40 sesiones por segundo (que es en realidad el valor máximo de sesiones que va a manejar),

Nuevas sesiones/seg = 5*60 + 120 = 420 nuevas sesiones/segundo

Cabe mencionar que éstos cálculos entregan un valor máximo posible considerando que todos los usuarios están accediendo a internet de manera simultánea y en el mismo momento, lo cual es sólo un caso hipotético.

d. Numero de interfaces de red. De acuerdo al diseño propuesto, el equipo debe contar con al menos tres interfaces de red. Es recomendable considerar una o dos interfaces adicionales en caso de falla o para futuros crecimientos.

e. Zonas de seguridad. De acuerdo al diseño, es necesario que el equipo soporte 3 zonas de seguridad. Se considera necesario que el equipo soporte al menos una zona de seguridad mas para futuros crecimientos.

De acuerdo a los datos obtenidos en los cálculos de los puntos a, b, c, d y e; los requerimientos del firewall perimetral son:

TABLA 3.2 DIMENSIONAMIENTO DEL FIREWALL PERIMETRAL

	Firewall		
Requerimiento	**Actual**	**Requerido**	**Recomendado**
Throughput de Firewall	desconocido	62Mbps	80Mbps
Max. numero de sesiones	desconocido	3000	6000
Nuevas sesiones/segundo	desconocido	420	1000
# Interfaces de red FE10/100	5	5	6
# Zonas de seguridad	desconocido	4	6

La tabla 3.2 muestra los requerimientos mínimos y recomendados para el dimensionamiento del firewall. Para la obtención de los valores

recomendados se consideró un 25% de recursos por encima de los mínimos, puesto que estos se obtuvieron de manera teórica.

Las formulas utilizadas en los puntos 3.3.4.1.b y 3.3.4.1.c no se encuentran documentadas en ningún documento o libro de referencia. Fue recogida de profesionales con remarcada experiencia en el campo de la seguridad informática y que actualmente continúan utilizándola en sus respectivas empresas como Trendcorp, ITCorp, Sidif, Eplus Soluciones, entre otras.

b. Dimensionamiento del Concentrador VPN SSL

Para el dimensionamiento de este equipo se utilizó los valores entregados por el cliente y que se utilizaron para obtener el licenciamiento necesario.

#de usuarios conectados por vpn en forma concurrente = menos de 5 usuarios.

c. Dimensionamiento del antispam y del proxy de navegación

Dado que ambas son soluciones en software con las que la empresa ya cuenta actualmente, los requerimientos de hardware son definidos por los fabricantes o marcas. A continuación se presentan los requerimientos de hardware de ambos productos.

a. Servidor antispam
   - Procesador : Xeon de 2.0Ghz / superior recomendado
   - Memoria RAM : 2GB RAM / 4GB RAM recomendado
   - Disco duro : 80GB / 120GB recomendado
   - Sist.Operativo : cuenta con sistema operativo propietario

b. Servidor proxy de navegación
   - Procesador : Xeon de 2.0Ghz
   - Memoria RAM : 1GB RAM / 2GB RAM recomendado
   - Disco duro : 80GB / 120GB recomendado
   - Sist.Operativo : MS Windows 2003 Server Standard

Capitulo 4

Selección de los componentes de la solución de seguridad perimetral

4.1 Evaluación de las soluciones

Existen dos criterios que deben ser tomados en cuenta para la elección de la solución a adquirir:

- **Evaluación tecnológica**

  Que contempla cuán bien cumple cada fabricante con los requerimientos de la empresa

- **Evaluación económica**

  Nos muestra que tan atractiva económicamente hablando es la propuesta.

El peso de cada criterio para la elección de la solución puede variar dependiendo del escenario de acción.

4.2 Selección de los fabricantes

En el mercado existen un gran número de fabricantes cuyos productos pueden cumplir con nuestros requerimientos, sin embargo, es importante conocer el posicionamiento en el mercado internacional y local de cada uno de ellos. Tener conocimiento de qué marcas son líderes en sus respectivos rubros y más aun, su comportamiento en los últimos tiempos. Es decir, si se mantuvieron como líderes, o si su ubicación privilegiada es tan solo momentánea, es un dato muy útil para elegir la mejor solución.

Existen empresas que se dedican a analizar las diferentes tecnologías en el aspecto técnico como en el comercial. Una de ellas, y la más reconocida a nivel mundial es Gartner.

Gartner es una empresa lider en investigación de empresas de tecnología, que tiene por finalidad comparar estas empresas en función de su historia, participación y crecimiento en el mercado, productos y servicios que ofrece, y su capacidad de mantenerse a la vanguardia tecnológica, proveyendo nuevas tecnologías y productos. El detalle de los criterios y metodología utilizados por Gartner para evaluar a las empresas se encuentra en su página web (www.gartner.com)

4.2.1 El cuadrante mágico de Gartner

Gartner utiliza diferentes criterios para evaluar las diferentes tecnologías y fabricantes. Esta información está disponible en la URL de Gartner, sin embargo explicaremos las cuatro categorías en las cuales se pueden ubicar los diferentes fabricantes.

- **Lideres (Leaders)**

  Los lideres son aquellos que se ubican en el mercado de empresas medianas y grandes, teniendo en cuenta que todos sus productos están desarrollados para empresas grandes. Adicionalmente han mostrado un gran y progresivo progreso en sus tecnologías a través del tiempo, haciendo que la valla tecnológica sea más alta para todos los competidores y tienen la capacidad, incluso cambiar el curso de la industria.

- **Competidores (Challengers)**

  El cuadrante de competidores contiene vendedores que tienen una buena ubicación en el mercado pero no son líderes en términos tecnológicos. Cuentan con una fuerza de ventas agresiva y son muy buenos para cerrar contratos, sin embargo sus productos cuentan con un limitado número de funciones avanzadas.

- **Visionarios (Visionaries)**

  Son aquellos que tienen buenos diseños y funcionalidades para el mercado, muchos de ellos pueden considerarse como productos de “siguiente generación”, pero no cuentan con una buena base comercial, estratégica o económica para competir con los líderes y competidores; o influenciar en el curso de la industria.

- **Jugadores de base (Niche Players)**

  Usualmente son fabricantes que se adecuan rápidamente a los cambios en el mercado pero no pueden definir su curso. La mayoría son pequeños vendedores con soluciones para empresas pequeñas.

En los estudios publicados por Gartner a inicios del 2010, presenta el siguiente cuadro comparativo con relación a los fabricantes de firewalls.

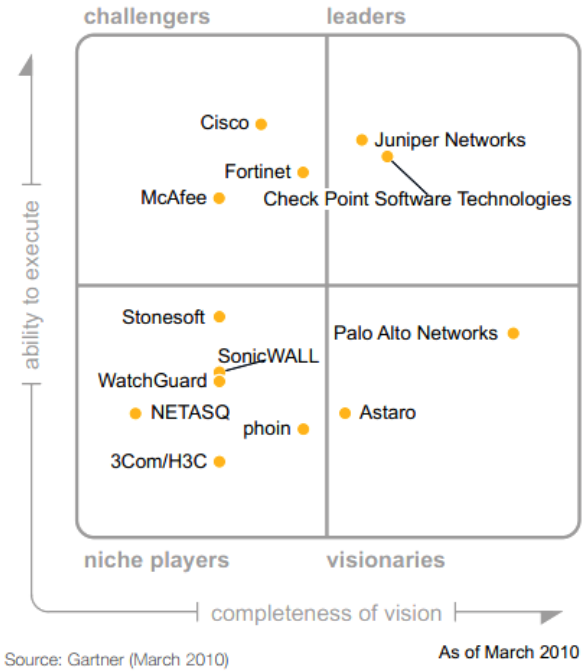

FIGURA 4.1 CUADRANTE MAGICO DE GARTNER PARA FIREWALLS – 1Q2010

Fuente: "Gartner" [GAR2010]

El grafico anterior muestra el resultado de la evaluación de Gartner respecto a firewalls, en el cual se muestra claramente el posicionamiento de Juniper Networks y Checkpoint como líderes en ese mercado.

El siguiente cuadro muestra el resultado de la evaluación de Gartner para el mercado de VPN sobre SSL.

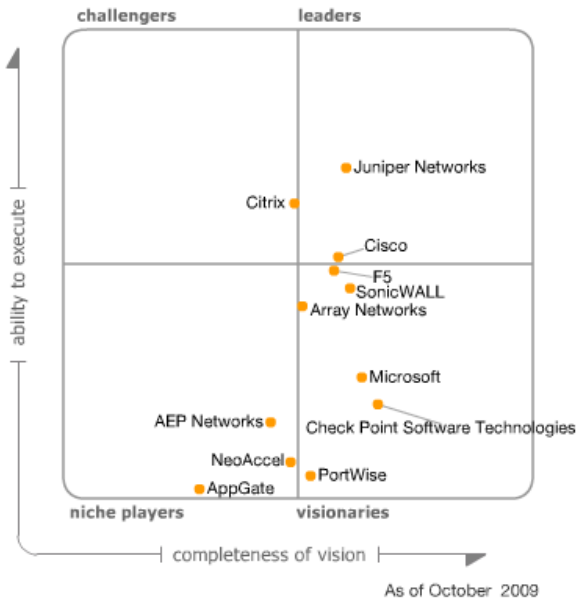

FIGURA 4.2 CUADRANTE MAGICO DE GARTNER PARA SSL-VPN – 3Q2009

Fuente: "Gartner" [GAR2010]

El cuadro anterior muestra el resultado del análisis de Gartner respecto a soluciones de VPN-SSL, mostrando la marcada ventaja de Juniper Networks frente a sus demás competidores, siendo los más cercanos Citrix y Cisco.

Utilizando como referencia los estudios presentados por Gartner, la selección de las tecnologías a utilizar las limitaremos a aquellos fabricantes que se encuentren en el cuadrante superior derecho de Gartner. Aquellos que son considerados lideres en el mercado.

Se ha utilizado para la presente tesis la información provista por Gartner correspondiente a los años 2009 y 2010 debido a que el proyecto se desarrolló en dicho periodo de tiempo.

4.3 Evaluación técnica

Luego de haber presentado un primer criterio de selección de los fabricantes o productos, se procede a realizar una comparación de funcionalidades y capacidades de los equipos que cumplen con los requisitos técnicos presentados en el punto 3.3.4.

4.3.1 Comparación técnica de los firewall

Los fabricantes competidores en este rubro son Checkpoint y Juniper Networks.

Es importante explicar que Checkpoint cuenta con soluciones basadas en software y en hardware (appliance). Para el caso de Checkpoint se considerará un equipo de la familia UTM-1 que es el *appliance* de Checkpoint. Con esta salvedad, a continuación se muestra el resultado de la evaluación técnica de entre los equipos Checkpoint UTM-1 136 y Juniper Networks SSG5.

TABLA 4.1 EVALUACION TECNICA DEL FIREWALL

Característica / Funcionalidad	Checkpoint UTM-1 136	Juniper Networks SSG5
Throughput ≥ 62Mbps	1.5Gbps	90Mbps
Soporte de VLAN con 802.1q	Si	Si
Interfaces Ethernet	5x10/100/1000	7x10/100
Max. Sesiones concurrentes	600mil	8mil
Nuevas sesiones/segundo	>20,000	2,800
Throughput de VPN	120Mbps	40Mbps
Zonas de seguridad	no maneja	8
Max. Políticas de seguridad	999	200
Gestión Centralizada	Si	Si
Soporte de traslación de direcciones de red (NAT)	Si	Si
Soporte de VoIP	Si	Si
Control de flujo y ancho de banda	Si	Si
Capacidad de filtro de contenido y antivirus embebido	Si	Si
Soporte de IPv6	Si	Si
Soporte de alta disponibilidad activo-pasivo	Si	Si
Soporte de VPN client/site, site/site	Si	Si
Nat trasversal para H323	Si	Si
Nat trasversal para IPSec	Si	Si
Soporte de protocolos SIP, H323 y MGCP	Si	Si

Es necesario mencionar que las características y funcionalidades mostradas son solo las principales de una lista más extensa, donde se detallan funcionalidades que ambas soluciones cumplen. El detalle de las funcionalidades de estos equipos se encuentra en sus hojas de datos, en la sección de anexos.

Dado que el manejo de zonas de seguridad no es un término estándar sino más bien utilizado por algunos fabricantes de firewalls, no se consideró relevante. De esta manera, ambas opciones pasan a la evaluación económica.

4.3.2 Comparación técnica de los equipos VPN SSL

Las marcas que compiten en este producto son Citrix con su Access Gateway y el FirePass de F5. No se considera a Cisco debido a que no cuenta con una solución de VPN SSL dedicada.

TABLA 4.2 EVALUACION TECNICA DEL SSL-VPN

Característica/Funcionalidad	Citrix Access Gateway	F5 FirePass	Juniper SecureAccess
Sistema operativo especifico	Si	Si	Si
Toda la comunicación debe ser sobre SSL	Si	Si	Si
Es de propósito especifico	Si	Si	Si
Soporte de alta disponibilidad	Si	Si	Si
Soporte de VPN L3	Si	Si	Si
Soporte de SSL v2 y v3	No	Si	Si
Facilidad de personalizar el portal de acceso	No	Si	Si
Soporte para plataformas Microsoft, Mac OS, Solaris y RHL	No	No	Si
Soporte para dispositivos móviles (PDA, Palm)	No	No	Si
Soporte de conexión a través de un proxy	Si	Si	Si
Integración con directorio activo de Microsoft para la autenticación de usuarios	Si	Si	Si
Integración con servidor de tokens de RSA en forma nativa	Si	No	Si
Integración con servidor Radius para la autenticación de usuarios	Si	Si	Si
Granularidad y escalabilidad de niveles de acceso	Si	Si	Si
Revisión de las condiciones de seguridad del cliente antes de la conexión	No	Si	Si
Capacidad de detección y protección de clientes contra keyloggers, troyanos, etc.	No	No	Si
No requiere la instalación manual de un cliente	Si	Si	Si

De igual manera que en el caso de los firewalls, el cuadro muestra el comparativo entre las distintas opciones, y en aquellas características y funcionalidades en las que pueden ser comparadas, debido a que cada una cuenta con funcionalidades muy particulares y que no han sido evaluadas debido a que no se encuentran dentro de los requerimientos del cliente.

En el cuadro mostrado se puede observar que el único equipo que tiene capacidad para soportar clientes VPN-SSL en plataformas no basadas en Microsoft es el equipo SecureAccess de Juniper, por lo que es el único equipo que pasa a la evaluación económica.

Es necesario mencionar que las características y funcionalidades mostradas son solo las principales de una lista más extensa, donde se detallan funcionalidades que ambas soluciones cumplen.

Es importante mencionar que los criterios de evaluación pueden variar dependiendo de escenario y de los requerimientos puntuales de cada empresa. Para efectos de la presente tesis, se procuró considerar aquellos que a criterio del autor de la tesis y basada en su experiencia, son los más comunes para redes pequeñas.

Como ejemplo que permita graficar cómo estos criterios pueden variar, se puede considerar una empresa que ya cuente con una solución de Citrix XenApp, el cual es el producto de virtualización (o webificación) de aplicaciones de tipo cliente servidor, y que, al integrarse con el equipo Access Gateway, presenta grandes ventajas debido a la comunicación nativa de ambos productos por proceder del mismo fabricante.

4.4 Evaluación económica

4.4.1 Evaluación económica del firewall externo

A continuación se presenta el comparativo de costos de los equipos preseleccionados:

TABLA 4.3 EVALUACION ECONOMICA DEL FIREWALL EXTERNO

Item	Checkpoint UTM-1 136	Juniper SSG5
Costo de los equipos	$ 3,000.00	$ 1,500.00
Licenciamiento del producto	-	-
Consola administración	$ 2,000.00	$ 2,000.00
Licenciamiento de Consola administración*	$ 8,000.00	$ 5,000.00
Soporte	$ 2,000.00	$ 1,500.00
Total	**$ 15,000.00**	**$ 10,000.00**

El cuadro 4.3 contiene el comparativo del costo de ambas soluciones de firewall: Checkpoint UTM 1136 y Juniper Networks SSG5.

Dado que la consola de administración de los firewalls es compartida por el firewall interno y perimetral, se coloca en esta tabla solo la mitad de su costo para ambos fabricantes.

4.4.2 Evaluación económica del SSL VPN

Si bien el único fabricante que calificó técnicamente es Juniper Networks, se presenta el comparativo de precios para el equipo SecureAccess700 y el Access Gateway de Citrix.

TABLA 4.4 EVALUACION ECONOMICA DEL CONCENTRADOR VPN SSL

Item	Citrix Access Gateway	Juniper SA700
Costo de los equipos	$ 2,500.00	$ 1,500.00
Licenciamiento para 8 usuarios concurrentes	$ 1,200.00	$ 1,000.00
Soporte	$ 740.00	$ 500.00
Total	**$ 4,440.00**	**$ 4,000.00**

El cuadro 4.4 contiene el comparativo del costo de ambas soluciones de acceso VPN-SSL: Citrix Access Gateway y Juniper Networks SA700.

4.4.3 Consideraciones adicionales

Algunas consideraciones a tener en cuenta al analizar la propuesta:

- No se presenta una propuesta económica para el proxy de navegación y antispam debido a que el cliente cuenta y/o adquirió estas soluciones de manera separada, y se asume que cumplen con los requerimientos de la empresa.
- La solución completa propuesta se considera también un firewall interno. cuya evaluación no se muestra debido a que no es parte de la presente tesis.
- Si bien no es mandatorio utilizar como referencia a Gartner para la selección de los fabricantes, es indudable que ofrece una referencia muy objetiva, y es una de las herramientas y criterios de selección más utilizada en el mercado peruano.
- Existen otros criterios de selección como la presencia de la marca en el mercado local. En el caso de los fabricantes mencionados, todos cuentan con presencia en el mercado peruano y cuentan con un alto nivel de soporte local, brindado por sus representantes; por lo que estos criterios no fueron considerados de manera cuantitativa.
- Tal y como se mencionó al final del punto 4.3, es posible que para una empresa pueda justificarse el costo adicional del equipo de Citrix si esto significa que se obtendrá un valor agregado al integrarlo con la solución de XenApp mencionada.
- La valorización de los equipos utilizada en la presente tesis están basados en precios referenciales otorgados para la presente tesis y no deben ser utilizados para otros fines.

4.5 Presentación de la solución propuesta

La elección de los distintos componentes de la solución de seguridad perimetral se decidió basándose en:

Su posicionamiento en el mercado actual de tecnología de la información, el cual fue provisto por Gartner en el punto *4.2.1. El cuadrante mágico de Gartner.*

Las características técnicas y funcionalidades provistas, la cual fue provisto a través de los cuadros comparativos contenidos en el punto *4.3 Evaluación técnica*, y las hojas de datos ubicadas en el Anexo 3.

Es importante mencionar que los criterios de evaluación pueden variar dependiendo de escenario y de los requerimientos puntuales de cada empresa. Para efectos de la presente tesis, se procuró considerar aquellos que a criterio del autor de la tesis y basada en su experiencia, son los más comunes para redes pequeñas, y las exigencias de la empresa que participó en el presente estudio.

4.5.1 Propuesta técnica

La solución propuesta es la siguiente:

a. Firewall Perimetral. Se escogió el equipo Juniper SSG5 debido a que cumple con los requerimientos del cliente y tiene un costo bastante menor que la alternativa propuesta por Checkpoint.

b. Concentrador VPN-SSL con Autenticación Fuerte. Se escogió el equipo Juniper SA700 con licenciamiento para 10 usuarios concurrentes. Se optó por esta alternativa debido a su capacidad para evaluar el nivel de seguridad de los equipos remotos que deseen conectarse a la red del cliente, además de su capacidad para enviar sus registros de eventos a la consola de administración de los firewalls.

c. Autenticación fuerte. Se ofreció un pack de 10 Tokens físicos de RSA para complementar la solución de acceso remoto seguro con autenticación fuerte.

d. Proxy de navegación. La empresa cuenta con una licencia de Microsoft ISA Server 2004, la cual se utilizara como proxy de navegación.

e. Antispam. La empresa adquirió un software antispam que cumplía con sus requerimientos.

Dado que la solución completa involucraba la seguridad perimetral así como el control de accesos interno se presenta los componentes adicionales que la conforman:

f. Firewall Interno. Se escogió el equipo Juniper SRX220 por cumplir con los requerimientos técnicos del cliente y porque, al tener un sistema operativo (JunOS) diferente al SSG5 (ScreenOS) provee un mayor nivel de seguridad por ser dos firewalls con diferentes arquitecturas.

g. Consola de administración centralizada de control de accesos. Se estableció que la consola seria el Network and Security Manager de Juniper pues permite gestionar los firewalls y el concentrador vpn ssl.

4.5.2 Propuesta económica

De acuerdo a la propuesta técnica, el costo de la solución es el siguiente.

Descripción	Cant.	Precio Total en US$
Juniper Firewall SSG5-H Incluye: • un año de mantenimiento de nuevas versiones del sistema operativo y actualizaciones del IPS	1	1,500.00
Juniper Firewall SRX220 Incluye: • un año de mantenimiento de nuevas versiones del sistema operativo • un año de licenciamiento de antivirus, IPS y antivirus.	1	4,000.00
Juniper Secure Access VPN SSL Incluye: • licenciamiento para 10 usuarios concurentes • un año de mantenimiento de nuevas versiones del sistema operativo	1	4,000.00
Tokens RSA SID 700. Incluye: • 3 años de duración de la pila. • Licencia para la consola de administración	10	0.00
Juniper Network and Security Manager Incluye: • un año de mantenimiento de nuevas versiones del producto.	1	8,000.00
Servicio de Instalación	1	1,750.00
Servicio de Soporte Técnico del proveedor, modalidad 24X7 por un año	1	3,500.00
TOTAL EN US$		**22,750.00**

Condiciones de Venta:

- El precio está expresado en dólares americanos y no incluye IGV.
- Los valores mostrados son referenciales y no deben ser utilizados para otros fines que la presente tesis.
- Los valores reales no pueden ser mostrados por el contrato de confidencialidad con el cliente, proveedor y fabricante.

Capitulo 5

Definición de políticas de seguridad

5.1 Etapas del proceso de Implementación

La definición de las políticas de seguridad que serán aplicadas sobre los componentes que conforman la solución de seguridad perimetral: firewall externo, concentrador VPN SSL y proxy de navegación, son etapas de todo el proceso de implementación de la solución de seguridad completa. Por este motivo se presenta, mas no se detalla, todo el proceso de implementación.

La implementación de la solución se realizó siguiendo las recomendaciones del PMI para la gestión de proyectos. El proyecto se desarrolló en cuatro (04) etapas:

- **Inicio**

  En la cual se presentó el proyecto, sus alcances, objetivos y etapas principales.

- **Planificación**

  En la cual se desarrolló las fases o etapas en actividades y tareas, su duración y fechas de entrega. Se estableció responsabilidades y recursos para cada tarea.

- **Desarrollo**

  Donde se realizaron las tareas y actividades que conforman el proyecto.

- **Cierre**

  Corresponde a las tareas de análisis del desarrollo, validación del cumplimiento de los alcances y presentación del informe de cierre.

Para efectos de la presente tesis, solo se presentará el alcance del proyecto y la etapa de desarrollo.

5.2 Alcance del proyecto

Del documento de descripción del proyecto se extrajo la siguiente información.

Los alcances para el presente proyecto fueron los siguientes:

- Definición de las políticas de control de acceso que serán aplicadas en los firewalls y concentrador vpn ssl.

- Configuración de los equipos que conforman la solución según la arquitectura de red aprobada por el cliente.
- Configuración de los equipos de manera que se cumplan todos los requisitos de seguridad del cliente y de la normativa PCI.
- Inducción y capacitación sobre la solución implementada, a los miembros del personal de la entidad financiera que el cliente indique con un máximo de 4 participantes.
- La empresa es la encargada de proporcionar el acceso físico a los ambientes en donde se realizaron las configuraciones e instalaciones.
- La empresa estaba comprometida a brindar los datos necesarios y a tiempo para la implementación dentro de los tiempos previstos.
- El proveedor está obligado a resolver cualquier duda o consultar con respecto al funcionamiento y la configuración de la solución al personal de la empresa cliente.
- Cualquier punto que no esté incluido en los alcances del proyecto deberá ser discutido por ambas partes hasta llegar a un acuerdo.

Como el alcance de la presente tesis es el diseño de la solución de seguridad perimetral, el único ítem que será documentado es el siguiente:

- Definición de las políticas de control de acceso que serán aplicadas en los firewalls y concentrador vpn ssl.

5.2.1 Plan de Trabajo

Para la implementación de la solución se elaboró un plan de trabajo detallado que fue aprobado por el cliente.

El plan de trabajo se presenta a continuación:

TABLA 5.1 PLAN DE IMPLEMENTACION DE LA SOLUCION DE SEGURIDAD

Item	Tarea	Descripcion	Tiempo (dias)	Dia 1	Dia 2	Dia 3	Dia 4	Dia 5	Dia 6	Dia 7	Dia 8	Dia 9	Dia 10
1	**Definición de políticas de seguridad**		**1**										
1.1	Para el firewall perimetral		1	x									
1.2	Para el firewall interno		1	x									
1.3	Para el acceso remoto vpn		1	x									
1.4	Para el proxy de navegación		1	x									
2	**Implementación de firewall perimetral**		**1**		**X**								
2.1	Configuración del firewall perimetral		1		x								
2.2	Puesta en producción y prueba de servicios y accesos	Puesta en línea y prueba de servicios	1		x								
3	**Segmentación de red**		**3**			**X**	**X**	**X**					
3.1	Implementación del firewall interno		1			x							
3.2	Prueba de servicios desde nuevo segmento de usuarios	Prueba de conexión a servidor de correo y aplicaciones	1			x							
3.3	Migración de usuarios a nuevo segmento	Cambio de direccionamiento IP de los usuarios	2			x	x	x					
4	**Implementación de solución de acceso remoto seguro**	**Instalación del SecureAccess de Juniper y consola de tokens**	**2**						**X**	**X**			
4.1	Instalación de consola para los tokens		1						x				
4.2	Configuración del SA2500		1						x				
4.3	Puesta en producción del SA2500		1							x			
5	**Implementación de políticas en proxy de navegación**		**2**						**X**	**X**			
6	**Afinamiento de políticas de seguridad**		**3**								**X**	**X**	**X**

5.3 Desarrollo de las políticas de seguridad

Para efectos de la presente tesis, solo se documentará las etapas 1.1, 1.3 y 1.4 del Plan de Implementación presentado en el punto anterior.

5.3.1 Políticas de seguridad para el firewall perimetral

5.3.1.1 Componentes de una política de seguridad

Una política de seguridad está conformada por un grupo de reglas que establecen de donde y hacia donde se realizarán las comunicaciones, el protocolo o servicio que utilizarán para comunicarse y si es necesaria la aplicación de traducción de direcciones IP de red (Network Address Translation – NAT).

Los elementos básicos que conforman una regla son:

- Dirección Origen
- Dirección Destino
- Nat Origen
- Nat Destino
- Servicio o Protocolo
- Acción

A continuación se presenta un ejemplo de una política de seguridad. Esta política permite que el equipo A ubicado en una zona Privada, con dirección IP 10.1.10.5 pueda acceder al equipo D, ubicado en internet, con dirección IP 200.5.5.5. Se puede apreciar que la dirección IP del equipo A es enmascarada (mediante NAT) en la IP 1.1.8.1 para poder alcanzar al equipo D ubicado en Internet.

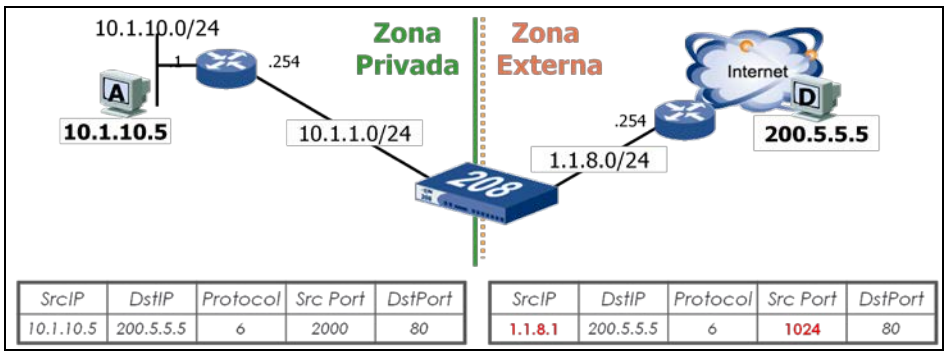

FIGURA 5.1 EJEMPLO DE REGLA DE ACCESO

5.3.1.2 Accesos requeridos hacia y desde internet de la empresa

El cliente requiere los siguientes accesos hacia y desde internet hacia su red interna.

TABLA 5.2 REGLAS PARA EL FIREWALL EXTERNO O PERIMETRAL

Acceso requerido	Traducción Técnica	Política requerida
Comunicación por correo electrónico con Internet	• Acceso vía protocolo SMTP desde internet hacia el servidor Antispam. • Acceso vía protocolo SMTP desde servidor antispam hacia Internet.	• NAT de entrada de "IP Publica Correo" a servidor Antispam. • NAT de salida de servidor Antispam a "IP Publica Correo" • Acceso vía DNS para el servidor antispam hacia internet. • Comunicación ida y vuelta vía protocolos SMTP entre servidor Antispam y servidor de correo.
Acceso a Internet para los usuarios vía HTTP y HTTPS	• Acceso vía protocolos HTTP y HTTPS para el proxy de navegación hacia internet.	• NAT de salida para el servidor proxy de navegación. • Acceso a internet para el proxy de navegación por los protocolos HTTP, HTTPS y DNS.
Publicación de la interface Web de correo electrónico	• Acceso vía HTTPS desde internet al servidor de correo.	• NAT de entrada de "IP Publica OWA" a servidor de correo. • Acceso vía HTTPS desde internet hacia el servidor de correo.
Acceso de los usuarios remotos vía VPN SSL	• Acceso vía HTTPS desde internet al concentrador VPN SSL	• NAT de entrada de "IP VPN SSL" a concentrador VPN SSL. • Acceso vía HTTPS desde internet hacia el concentrador VPN SSL.

La tabla 5.2 contiene las reglas de acceso hacia y desde internet, que deben ser implementadas en el firewall de perímetro.

5.3.1.3 Reglas adicionales requeridas

Adicionalmente a las reglas solicitadas por la empresa, es necesario agregar las siguientes reglas:

TABLA 5.3 REGLAS ADICIONALES PARA EL FIREWALL PERIMETRAL

Acceso requerido	Política requerida
Acceso para administración del concentrador VPN SSL y antispam en la DMZ	• Acceso vía protocolo HTTP, HTTPS, SMTP y SSH al antispam desde la pc del administrador de red. • Acceso vía protocolo HTTPS y SSH al antispam desde la pc del administrador de red.
Comunicación entre concentrador VPN SSL y consola de tokens	• Acceso desde el concentrador VPN SSL a la consola de tokens vía grupo de protocolos RSA_SecureID.
Registro de todos los intentos fallidos de conexión	• Reglas de CleanUp.

La tabla 5.3 contiene aquellas reglas que son necesarias para el funcionamiento de la red y que no están relacionadas directamente con la publicación de servicios y acceso a internet.

5.3.1.4 Política de seguridad a ser aplicada en el firewall perimetral

Basándonos en los requerimientos de los puntos 3.1.2 y 3.1.3, la política de seguridad a ser aplicada en el firewall perimetral es la que se muestra a continuación.

Los nombres “Srv_Antispam”, “Srv_Correo”, “Srv_Proxy”, “Srv_Tokens”, “SA2500”, IP_Pub_Correo”, “IP_Pub01”, y otros nombres utilizados en la política mostrada representan a las direcciones IP reales del cliente, los cuales no son mostrados por el acuerdo de confidencialidad existente.

TABLA 5.4 POLITICA DE SEGURIDAD PARA EL FIREWALL PERIMETRAL

ID Regla	Originales				Traducidos (NATEADOS)				Servicio	Acción	NAT
	Zona Origen	Objeto Origen	Zona Destino	Objeto Destino	Zona Origen	Objeto Origen	Zona Destino	Objeto Destino			
Trafico de correo electrónico entre servidor antispam e internet											
1	DMZ	Srv_Antispam	Internet	Any	DMZ	IP_Pub_Correo	Internet	Any	SMTP	Permitir	Estático 1:1
2	DMZ	Srv_Antispam	Internet	Any	DMZ	IP_Pub_Correo	Internet	Any	DNS HTTP	Permitir	Estático 1:1
3	Internet	Any	DMZ	IP_Pub_Correo	Internet	Any	DMZ	Srv_Antispam	SMTP	Permitir	Estático 1:1
Trafico de correo electrónico entre servidor antispam y servidor de correo											
4	DMZ	Srv_Antispam	Red Interna	Srv_Correo	DMZ	Srv_Antispam	Red Interna	Srv_Correo	SMTP	Permitir	No NAT
5	Red Interna	Srv_Correo	DMZ	Srv_Antispam	Red Interna	Srv_Correo	DMZ	Srv_Antispam	SMTP	Permitir	No NAT
Salida de los usuarios a internet											
6	Red Interna	Srv_Proxy	Internet	Any	Red Interna	IP_Pub_01	Internet	Any	HTTP HTTPS DNS	Permitir	Dinámico
Publicación de correo web (OWA)											
7	Internet	Any	Red Interna	IP_Pub_OWA	Internet	Any	Red Interna	Srv_Correo	HTTPS	Permitir	Estático 1:1
Acceso Remoto Seguro											
8	Internet	Any	DMZ	IP_Pub_VPN	Internet	Any	Red Interna	SA2500	HTTPS	Permitir	Estático 1:1
9	DMZ	SA2500	Red Interna	Srv_Tokens	DMZ	SA2500	Red Interna	Srv_Tokens	SecureID	Permitir	
Gestión del Antispam y del SA2500											
10	Red Interna	PC_Admin	DMZ	Srv_Antispam	Red Interna	PC_Admin	DMZ	Srv_Antispam	HTTP HTTPS SMTP SSH	Permitir	
11	Red Interna	PC_Admin	DMZ	SA2500	Red Interna	PC_Admin	DMZ	SA2500	HTTPS	Permitir	
egistro de intentos de acceso no autorizad											
12	Internet	Any	DMZ	Any	Internet	Any	DMZ	Any	Any	Denegar	
13	Internet	Any	Red Interna	Any	Internet	Any	Red Interna	Any	Any	Denegar	
14	DMZ	Any	Internet	Any	DMZ	Any	Internet	Any	Any	Denegar	
15	Red Interna	Any	Internet	Any	Red Interna	Any	Internet	Any	Any	Denegar	
16	Red Interna	Any	DMZ	Any	Red Interna	Any	DMZ	Any	Any	Denegar	
17	DMZ	Any	Red Interna	Any	DMZ	Any	Red Interna	Any	Any	Denegar	

La forma de entender la tabla 5.4 es la siguiente. Bajo la columna "Originales" se muestra los objetos antes de que la comunicación se establezca. Bajo "Originales" se puede apreciar cuatro columnas, las cuales identifican la "Zona Origen" y "Objeto Origen" del tráfico. De igual manera se visualiza la "Zona Destino" y el "Objeto destino". De esta manera, para la regla ID.2, se debe leer de la siguiente manera:

El equipo Srv_Antispam, ubicado en la zona DMZ puede establecer comunicación con el equipo "Any" ubicado en "Internet".

Bajo la columna "Traducción" se muestra como se verán los objetos al pasar por el firewall. La columna "Servicio" y "Acción" definen el protocolo de comunicación y la acción que tomara el firewall respecto a ese tráfico. Así, toda la regla se lee de la siguiente manera:

El equipo Srv_Antispam ubicado en la DMZ tiene permitido establecer conexiones via SMTP hacia cualquier objeto (Any) ubicado en internet, y será visto por éstos con la dirección IP IP_Pub_Correo.

5.3.2 Política de acceso para el concentrador VPN SSL

5.3.2.1 Componentes de una política de acceso remoto

El perfil de acceso es el conjunto de permisos que se le otorgan al usuario remoto cuando este se conecta a través del túnel VPN SSL luego de haber realizado una operación de autenticación satisfactoria.

Los componentes básicos que conforman una política de acceso son:

- Servidor de autenticación. Contiene una lista de cuentas de usuarios y sus respectivas credenciales y contraseñas.
- Cuenta de usuario. Único en un servidor de autenticación y asocia a una persona con un registro en un servidor de autenticación.
- Rol de acceso. Define los permisos y accesos para un usuario y/o grupo de usuarios. Se traduce como direcciones IP a los que el usuario puede acceder y los protocolos mediante los cuales puede acceder a ellos.

5.3.2.2 Política requerida por la empresa

El cliente requiere los siguientes accesos hacia y desde internet hacia su red interna:

TABLA 5.5 REGLAS DE ACCESO REMOTO

Requerimiento	Configuración requerida
Acceso irrestricto a toda la red interna para los gerentes (5 usuarios), a quienes se les entregara un token.	• Asociar una cuenta de usuario y un token a cada uno de los 5 gerentes. • Crear un servidor de autenticación en el SA2500 asociado al servidor de los tokens • Crear un perfil de acceso para el grupo de gerentes.
Acceso irrestricto a la red interna para el personal de sistemas (2), a quienes se le entregara tokens.	• Asociar una cuenta de usuario y un token al administrador de red y asistente de soporte. • Crear un perfil de acceso para el grupo de soporte
Acceso restringido a correo electrónico y aplicación de ventas a los vendedores de campo, quienes se autenticaran con su usuario de directorio activo de Microsoft.	• Crear un servidor de autenticación en el SA2500 asociado al servidor de directorio activo de la empresa • Crear un perfil de acceso limitado para el grupo de ventas.
Acceso a equipos de seguridad para personal de soporte del proveedor.	• Crear una cuenta de usuario en el servidor de autenticación local del SA2500. • Crear un perfil que le permita al proveedor acceder a los dispositivos de seguridad por temas de soporte.

La tabla 5.5 contiene, en un lenguaje coloquial, las reglas de acceso para los usuarios que se conectaran de manera remota a la red cliente.

5.3.2.3 Política de seguridad a ser aplicada en el concentrador VPN SSL

Basándonos en los requerimientos de los puntos 3.2.2, la política de seguridad a ser aplicada en el concentrador VPN SSL es la que se muestra a continuación.

a. Autenticación.

TABLA 5.6 USUARIOS EN EL CONCENTRADOR VPN SSL

Usuarios	Grupo	Servidores de Autenticación
gerente1	G_Gerentes	RSA Auth. Manager
gerente2	G_Gerentes	RSA Auth. Manager
gerente3	G_Gerentes	RSA Auth. Manager
gerente4	G_Gerentes	RSA Auth. Manager
gerente5	G_Gerentes	RSA Auth. Manager
sisadmin01	G_Sistemas	RSA Auth. Manager
sissop01	G_Sistemas	RSA Auth. Manager

Ventas01	G_Ventas	Directorio Activo Corporativo
Ventas02	G_Ventas	Directorio Activo Corporativo
Ventas03	G_Ventas	Directorio Activo Corporativo
Soporte		Servidor Local

La tabla 5.6 contiene el listado de usuarios y grupos que podrán acceder de manera remota a la red corporativa. Cabe mencionar que los nombres mostrados son genéricos.

b. Perfiles de acceso

TABLA 5.7 USUARIOS EN EL CONCENTRADOR VPN SSL

Nombre	Asignado a	Nivel de acceso
Acceso Gerentes	G_Gerentes	Acceso a toda la red interna
Acceso Sistemas	G_Sistemas	Acceso a toda la red interna
Ventas	G_Ventas	Acceso vía SMTP/POP3 a servidor de correo Acceso vía RDP a servidor de aplicaciones
Soporte	Soporte	Acceso a firewalls, consola de firewalls, antispam y proxy

La tabla 5.7 contiene el listado de perfiles de acceso y los grupos de usuarios asociados a cada perfil, considerando el grado o nivel de acceso otorgado.

5.3.2.4 Política de acceso a internet para usuarios en el proxy de navegación

Los requerimientos de la empresa son:

- Únicamente los usuarios autenticados en el directorio activo de la empresa y que salgan a través del proxy de navegación puedan navegar en internet y exclusivamente por los protocolos HTTP y HTTPS.
- Se bloquee el acceso a ciertas paginas agrupadas bajo el nombre “paginas prohibidas” a todos los usuarios.
- Se garantice acceso irrestricto a internet al gerente general de la empresa.

De esta manera la política del proxy de navegación queda como se muestra a continuación.

TABLA 5.8 POLITICA DE SEGURIDAD PARA EL PROXY

ID Regla	Usuarios	Autenticación	Protocolos	Destino	Accion
1	Gerente general	Directorio Activo	HTTP, HTTPS	Any	Permitir
2	Todos	Directorio Activo	HTTP, HTTPS	Paginas Prohibidas	Denegar
3	Todos	Directorio Activo	HTTP, HTTPS	Any	Permitir
4	Todos	None	HTTP, HTTPS	Any	Denegar

La tabla 5.8 muestra las reglas de acceso a internet para los usuarios internos.

5.4 Simulación de la solución propuesta.

Para validar el funcionamiento de la solución propuesta y la completa interoperabilidad de los componentes de la misma, se elaboró un ambiente de laboratorio lo más cercano al escenario de la empresa, sin embargo no fue posible simular la carga del número de equipos con los que cuenta, por lo que para la validación de la capacidad se utilizó información recogida de equipos similares que ya se encuentran en producción en otras empresas.

Por temas de confidencialidad, no es posible revelar el nombre de dichas empresas.

5.4.1 Arquitectura del escenario de pruebas.

Para las pruebas mostradas a continuación se consideró el siguiente escenario de pruebas.

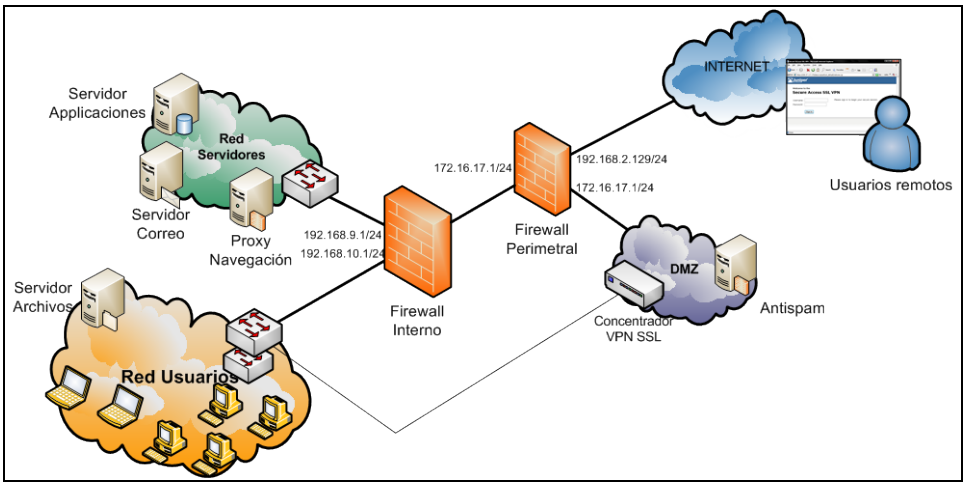

FIGURA 5.2 ARQUITECTURA DEL ESCENARIO DE PRUEBAS

Dado que para el firewall perimetral la Red de Servidores y la Red de Usuarios es la misma red, para las simulaciones mostradas a continuación, la interface con la dirección IP 172.16.17.1/24 tendrá la IP 192.168.9.1/22.

5.4.2 Firewall perimetral.

El firewall perimetral funcionará con la siguiente configuración.

5.4.2.1 Parámetros de red y zonas de seguridad.

El equipo Juniper SSG5 tiene tres interfaces configuradas con la siguiente información.

TABLA 5.9 CONFIGURACION DE RED DEL FIREWALL PERIMETRAL

Interface	Dirección IP	Zona de Seguridad
Ethernet0/0	192.168.9.1/22	Red Interna
Ethernet0/1	172.16.17.1/24	DMZ
Ethernet0/3	192.168.2.129/24	Internet

La tabla 5.9 muestra la configuración de red del equipo Juniper SSG5 utilizado para las simulaciones.

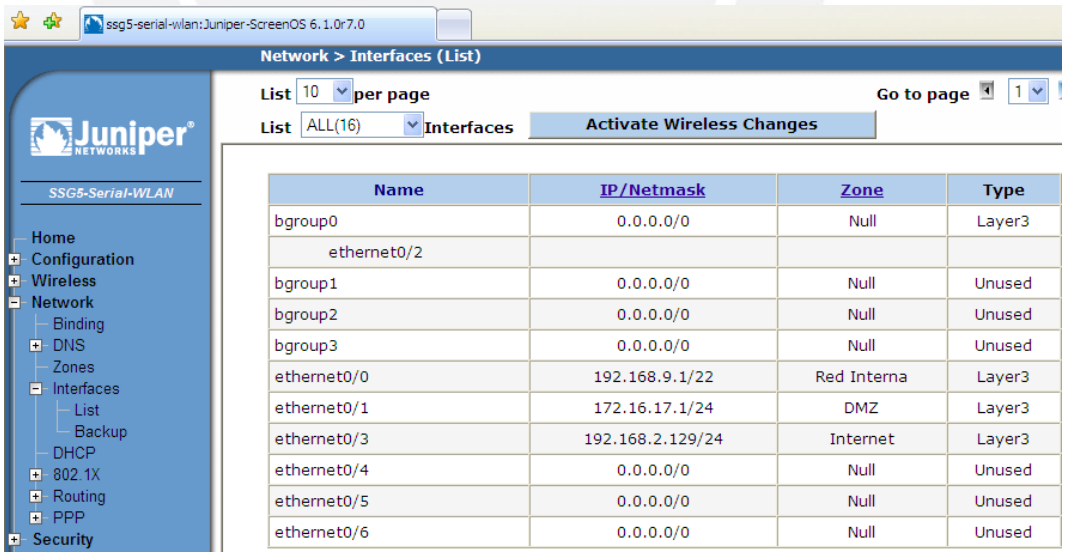

FIGURA 5.3 CAPTURA DE PANTALLA DE DATOS DE RED DEL FIREWALL PERIMETRAL

La figura 5.3 muestra la información contenida en la tabla 5.9 ya ingresada en el equipo Juniper SSG5.

5.4.2.2 Reglas de acceso.

Las reglas de acceso mencionadas en el punto 5.3.1.4 se establecieron de la siguiente manera en el dispositivo.

Policy > Policies (From All zones To All zones)

5-serial-wlan

List 50 per page

From All zones

To All zones

Search

New

From Red Interna To DMZ, total policy: 4

ID	Source	Destination	Service	Action	Option	Enable	Move
11	PC_Admin	Srv_Antispam	HTTP HTTPS SMTP SSH				
6	SRV_Correo	Srv_Antispam	SMTP				
12	PC_Admin	SA2500	HTTPS				
13	Any	Any	ANY				

From DMZ To Red Interna, total policy: 3

ID	Source	Destination	Service	Action	Option	Enable	Move
10	SA2500	SRV_Tokens	SecureID				
5	Srv_Antispam	SRV_Correo	SMTP				
14	Any	Any	ANY				

From Internet To DMZ, total policy: 3

ID	Source	Destination	Service	Action	Option	Enable	Move
9	Any	MIP(192.168.2.132)	HTTPS				
4	Any	MIP(192.168.2.133)	SMTP				
15	Any	Any	ANY				

From DMZ To Internet, total policy: 3

ID	Source	Destination	Service	Action	Option	Enable	Move
2	Srv_Antispam	Any	SMTP				
3	Srv_Antispam	Any	DNS HTTP				
16	Any	Any	ANY				

From Internet To Red Interna, total policy: 2

ID	Source	Destination	Service	Action	Option	Enable	Move
8	Any	MIP(192.168.2.131)	HTTPS				
17	Any	Any	ANY				

From Red Interna To Internet, total policy: 2

ID	Source	Destination	Service	Action	Option	Enable	Move
7	SRV_Proxy	Any	DNS HTTP HTTPS				
18	Any	Any	ANY				

FIGURA 5.4 CAPTURA DE PANTALLA DE REGLAS DE ACCESO EN FIREWALL PERIMETRAL

La figura 5.4 contiene las políticas de seguridad a ser aplicadas en el firewall del cliente, mostradas también en la Tabla 5.4, configuradas en el firewall utilizado para la simulación. Cada entrada representa una regla de acceso, y cuenta con los campos: Source (Origen), Destination (Destino), Service (Servicio), Action (Accion: permitir/denegar).

Para facilitar el entendimiento de la figura, se tomará como ejemplo la regla ID.2, la misma que se utilizó para explicar la tabla 5.4 anteriormente.

Tal y como se puede apreciar, las reglas se encuentran agrupadas de acuerdo a las parejas formadas por “Zona Origen” y “Zona Destino”. De esta manera la regla 2 se encuentra en el grupo “From DMZ to Internet”.

Bajo el campo “Source” se muestra el objeto Srv_Antispam” y “Any” como destino. Esto significa que el tráfico permitido va desde el primer objeto hacia cualquiera ubicado en la zona Internet. El protocolo de comunicación permitido es SMTP.

5.4.2.3 Carga del equipo

Dado que no fue posible simular una red con el número de usuarios de red equivalente al de la empresa, se tomó como referencia los valores obtenidos de un equipo actualmente en producción en otra empresa con un total de 90 usuarios.

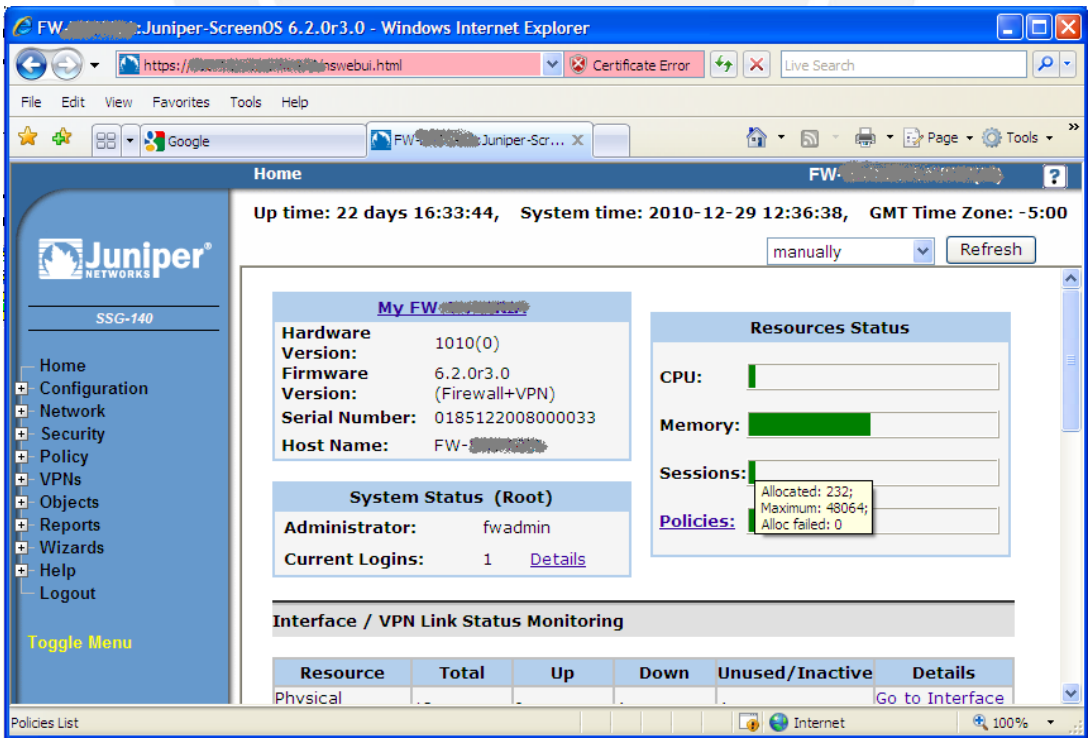

FIGURA 5.5 CAPTURA DE PANTALLA DE REPORTE DE RECURSOS DEL FIREWALL PERIMETRAL

Nótese bajo el cuadro “Resources Status” que el total de sesiones concurrentes es de 232 (sobre 48064 sesiones concurrentes soportadas por el equipo), muy por debajo del valor estimado en el punto 3.3.4.1.que fue de 1320 sesiones concurrentes. Nótese también que el consumo de CPU está por debajo del 5%, y el uso de memoria es menor al 50%.

5.4.2.4 Prueba de servicios

a) Publicación de acceso remoto VPN

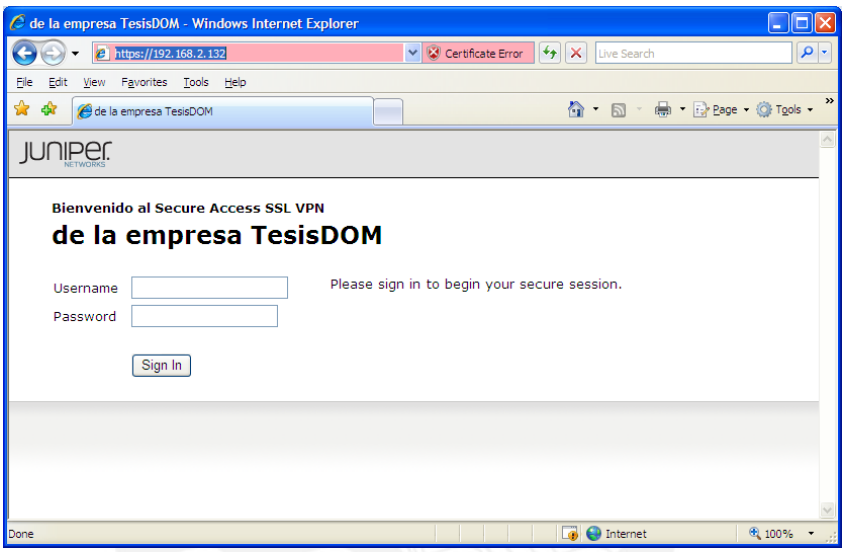

FIGURA 5.6 CAPTURA DE PANTALLA DE VENTANA DE LOG-IN PARA ACCESO VPN

La figura 5.6 muestra la interface web que debe ser utilizada por los usuarios remotos para poder conectarse via VPN-SSL. El acceso a la VPN-SSL se mostrará mas adelante.

b) Publicación de servicio de correo electrónico.

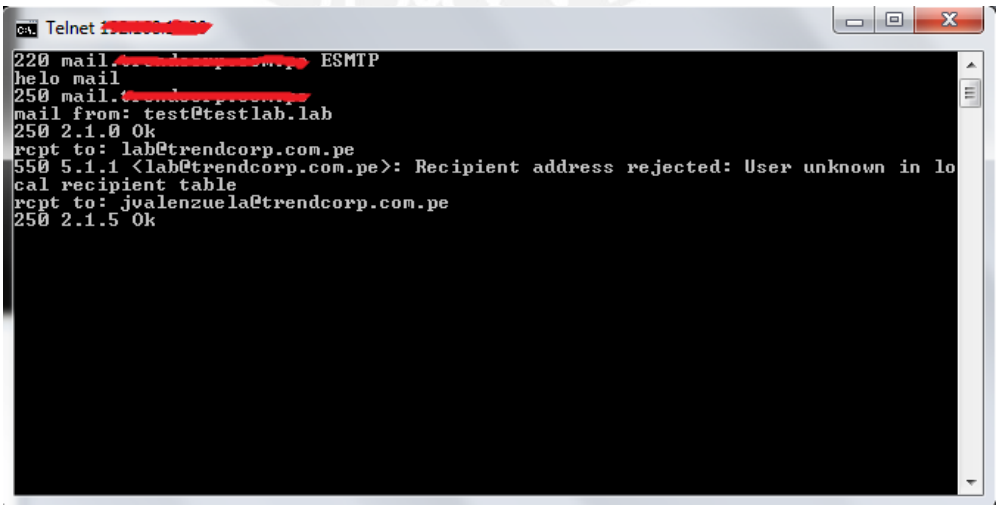

FIGURA 5.7 CAPTURA DE PANTALLA DE COMUNICACIÓN SMTP PARA ANTISPAM

La figura 5.7 muestra una prueba de conexión con el servidor de correo de prueba montado en el ambiente de simulación. La prueba consistió en la ejecución del comando “telnet <ip servidor destino> 25”, el cual permite simular una conexión SMTP con el servidor de correo remoto.

5.4.3 Acceso remoto seguro (VPN SSL).

El equipo de VPN SSL operará con dos interfaces de red. Una interface externa que se publicará hacia Internet y una que irá conectada a la red de usuarios.

5.4.3.1 Parámetros de red

El equipo de VPN SSL operará con la siguiente configuración de red.

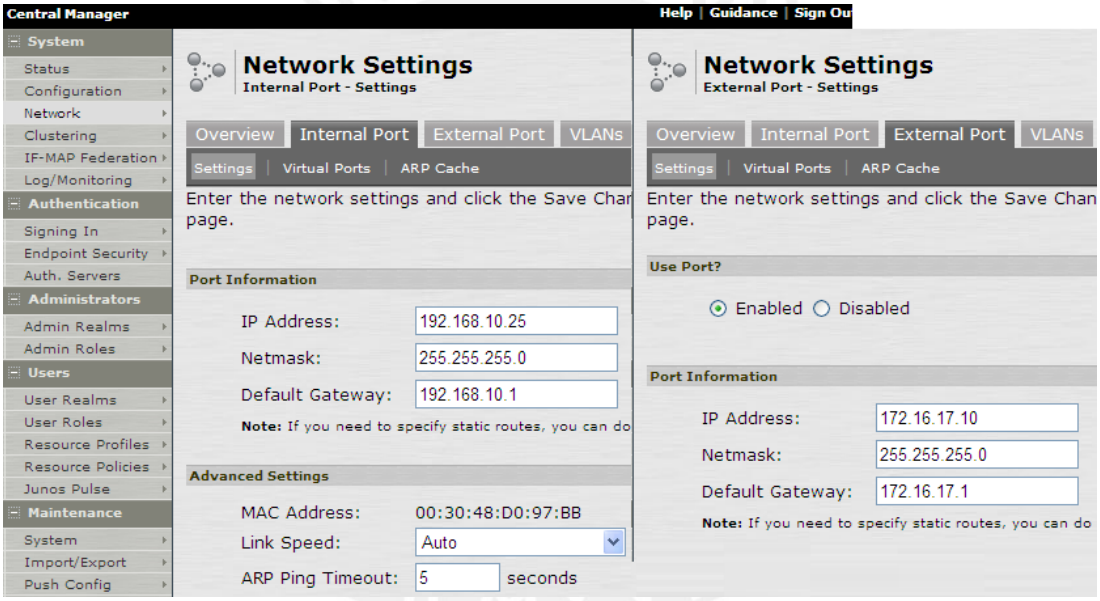

FIGURA 5.8 CAPTURA DE PANTALLA DE LA CONFIGURACION DE RED DEL SECURE ACCESS

La figura 5.8 muestra la configuración de red del equipo Juniper SecureAccess. La interface “Internal Port” muestra la dirección IP que tendrá el equipo en la red interna. La interface “External Port” muestra la configuración de la interface ubicada en la DMZ.

5.4.3.2 Usuarios y roles de acceso

Se trabajará únicamente con usuarios locales y usuarios del directorio activo debido a que no se contaba con los *tokens* para realizar las pruebas.

Todo usuario que intente conectarse deberá estar incluido en alguno de los dominios de autenticación, asociados a un servidor de autenticación: *System*

Local y TesisDom, que son los servidores de autenticación local y la integración con el directorio activo, respectivamente.

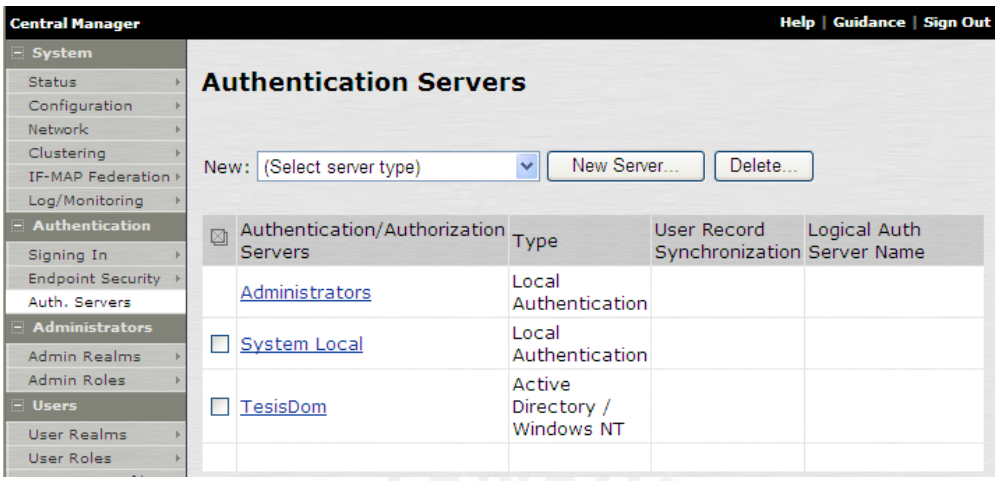

FIGURA 5.9 SERVIDORES DE AUTENTICACION

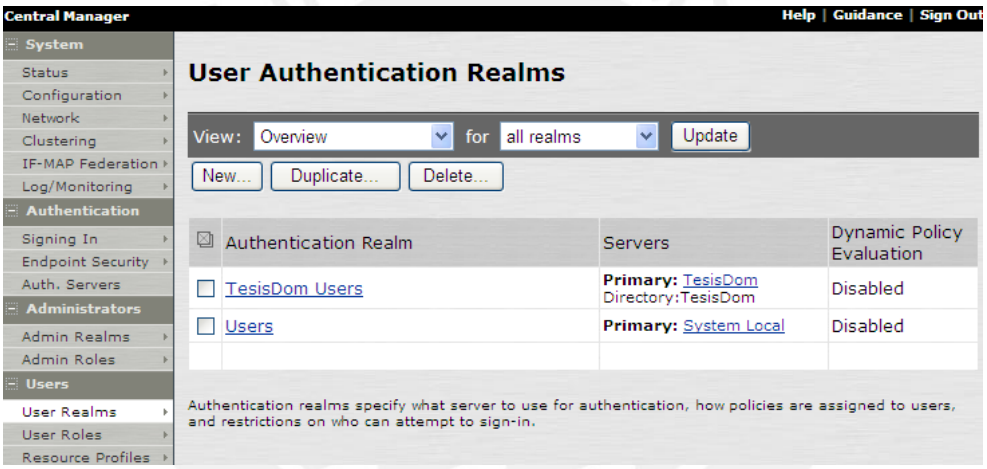

FIGURA 5.10 DOMINIOS DE AUTENTICACION

La figura 5.9 muestra los diferentes servidores de autenticación que están definidos en el equipo. Para el laboratorio utilizado, es importante notar el servidor “TesisDom”, que corresponde al servidor de dominio utilizado para éste ejemplo.

En la figura 5.10 se puede apreciar la asociación del dominio de autenticación “TesisDmon Users” con el servidor “TesisDom”, lo cual significa que todos los usuarios del dominio “TesisDom Users” deben usar sus credenciales del dominio “TesisDom” para poder acceder de manera remota.

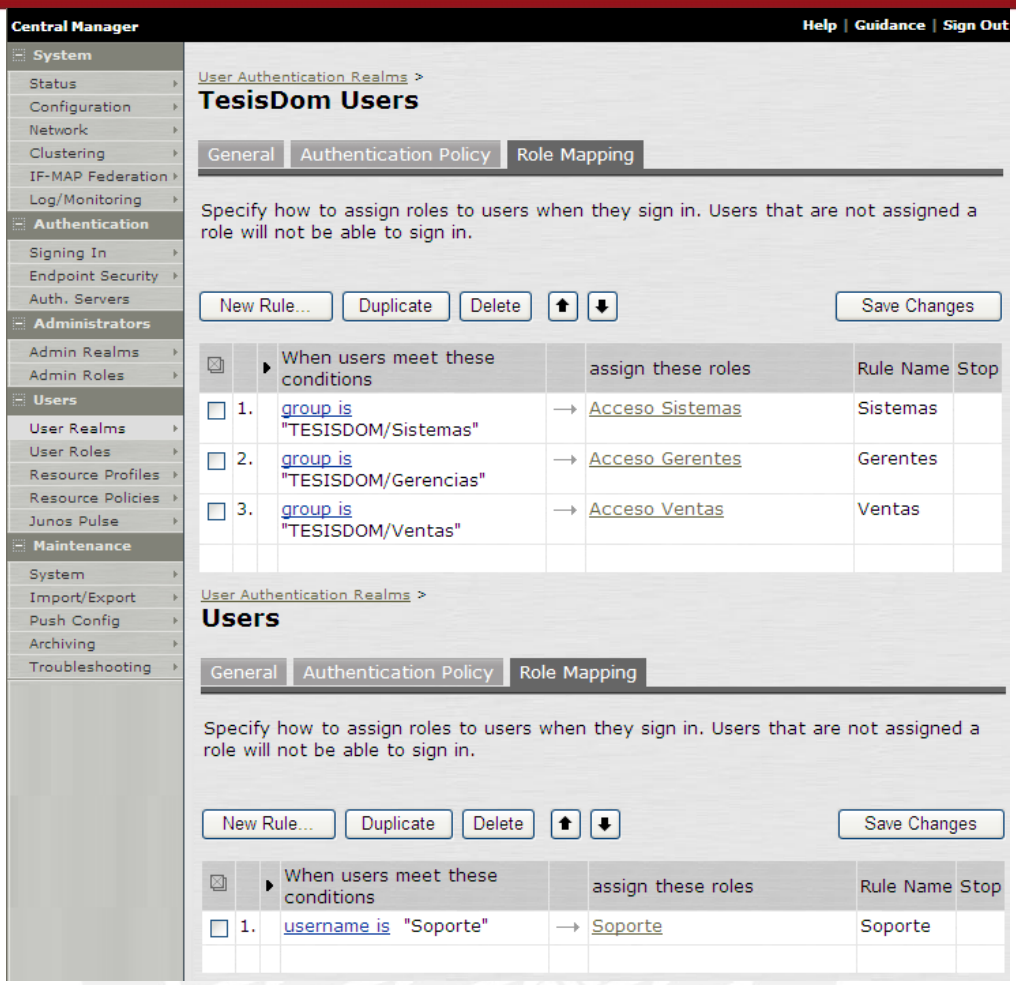

FIGURA 5.11 DOMINIOS DE AUTENTICACION

Las figuras 5.9, 5.10 y 5.11 muestran la configuración que el equipo VPN-SSL debe tener para cumplir con los requerimientos del cliente, contenidos en las tablas 5.6 y 5.7.

Cuando un usuario intente conectarse a la VPN SSL, el equipo verificará si el usuario pertenece a alguno de los grupos mostrados en la FIGURA 5.11. Dependiendo del grupo al que pertenezca el usuario, se le asignará un perfil de acceso diferente.

Cada perfil cuenta con accesos y permisos diferentes que van de acuerdo con la TABLA 5.6, donde se muestran los privilegios que debe tener los usuarios remotos.

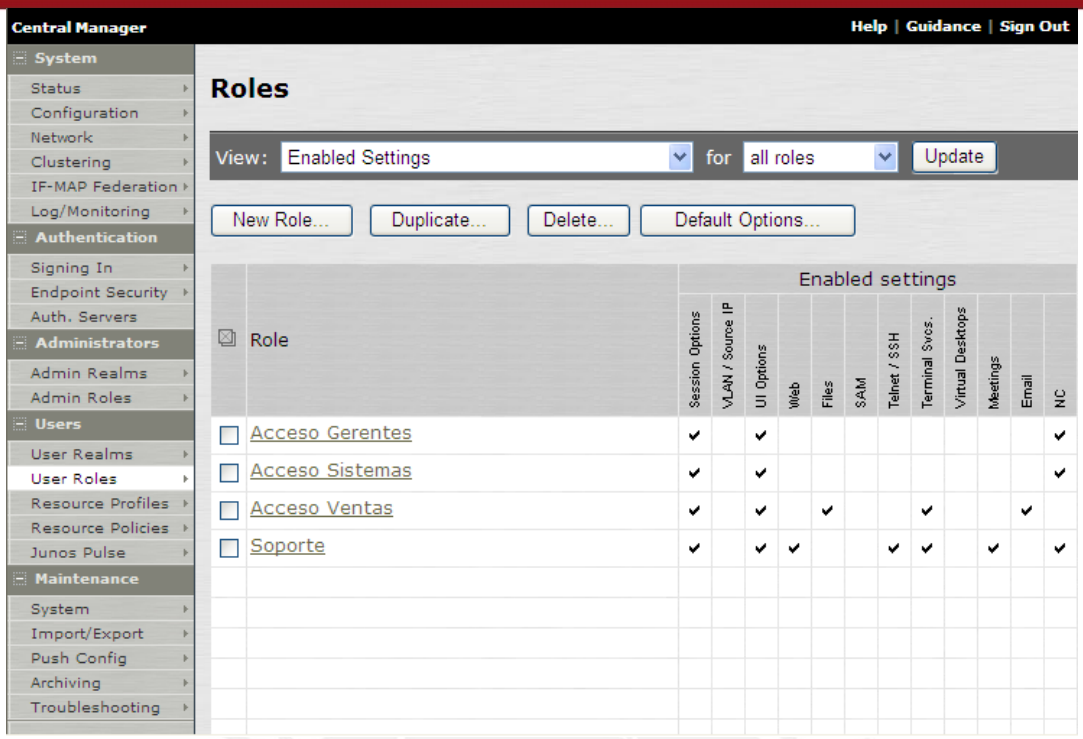

FIGURA 5.12 PERFILES DE ACCESO VPN SSL

La figura 5.12 muestra los roles de acceso o permisos que tendrán cada uno de los grupos previamente mostrados en la figura 5.11. Dichos roles de acceso se encuentran definidos en la tabla *5.6: Usuarios en el concentrdor VPN.*

5.4.3.3 Prueba de servicios

a. Publicación del servicio. Recordar que el equipo se encuentra publicado por el firewall perimetral.

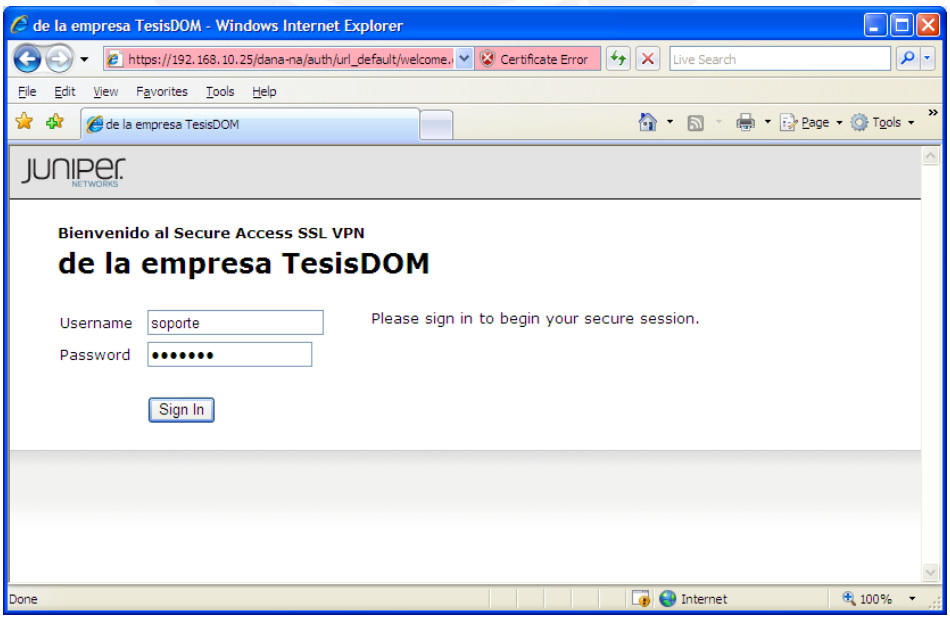

FIGURA 5.13 PRUEBA DE INTERFACE DE AUTENTICACION DE LA VPN SSL

La figura 5.13 muestra la interface de acceso para los usuarios remotos que pretendan acceder vía VPN-SSL a la red del cliente. Es importante notar que es necesario ingresar una cuenta de usuario y su contraseña respectiva para poder ingresar.

b. Descarga e instalación del cliente VPN

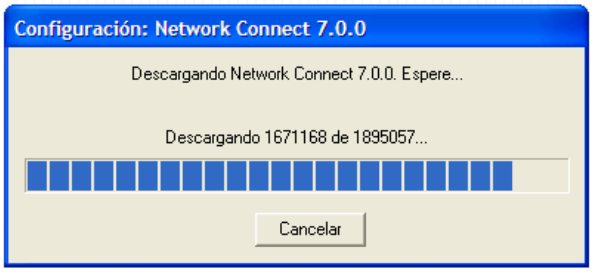

FIGURA 5.14 DESCARGA DEL CLIENTE VPN SSL

La figura 5.14 muestra la descarga del software requerido para establecer el túnel VPN-SSL entre el concentrador ubicado en el cliente y la computadora remota. Cabe mencionar que la descarga del cliente se inicia luego de que se haya realizado una autenticación satisfactoria.

FIGURA 5.15 CLIENTE CONECTADO

La figura 5.15 muestra la realización satisfactoria de una conexión VPN. En la ventana se puede apreciar la siguiente información:

- Direccion IP provista por el concentrador VPN-SSL: 192.168.10.200
- Estado de la conexión: Conectado.
- Duración de la conexión: 00:00:06
- Cantidad de información transferida: Bytes enviados y recibidos.

c. Prueba de conectividad

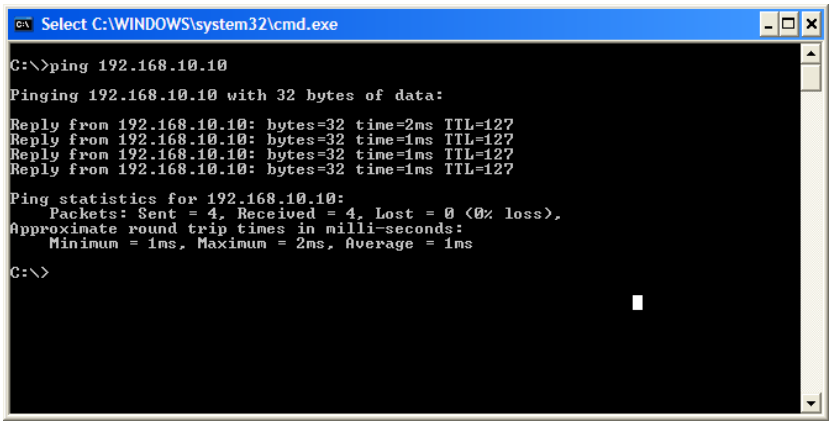

FIGURA 5.16 CAPTURA DE PANTALLA DE PRUEBA DE CONECTIVIDAD BASICA

La figura 5.16 muestra una prueba de conectividad básica realizada desde el cliente remoto hacia uno de los servidores de la red interna. Ésta prueba consistió en un ping ICMP entre el equipo remoto y un equipo ubicado en la red interna.

5.4.4 Acceso a Internet a través del proxy

El proxy de navegación a internet funcionará con la siguiente configuración.

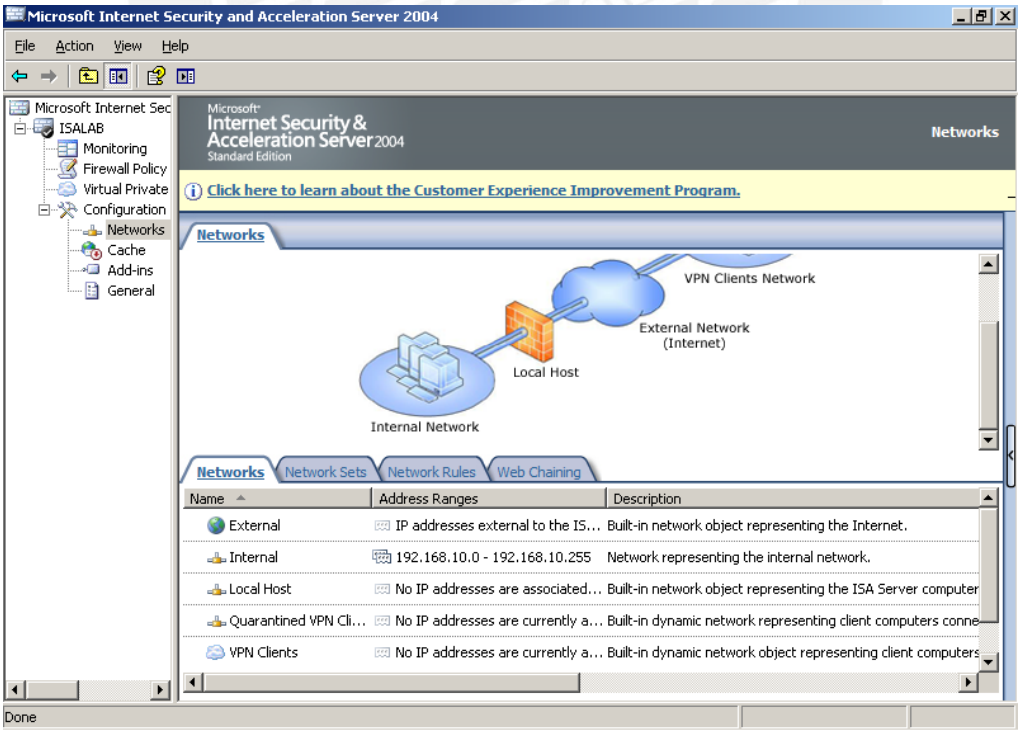

FIGURA 5.17 ARQUTECTURA DE IMPLEMENTACION DEL SERVIDOR ISA 2004

La figura 5.17 muestra la pantalla de inicio del servidor ISA Server 2004. Se puede apreciar en el marco superior la topología de red en la que se encuentra configurador. Es decir, en modo firewall, con dos interfaces de red. En el marco inferior se hace mención a las redes (segmentos de red) asociadas a cada zona de seguridad.

5.4.4.1 Parámetros de red

El servidor Microsoft ISA Server 2004 cuenta con dos interfaces de red, asociadas a las zonas de seguridad *External* (Local Area Connection) e *Internal* (Local Area Connection 2). La configuración de ambas interfaces se muestra a continuación.

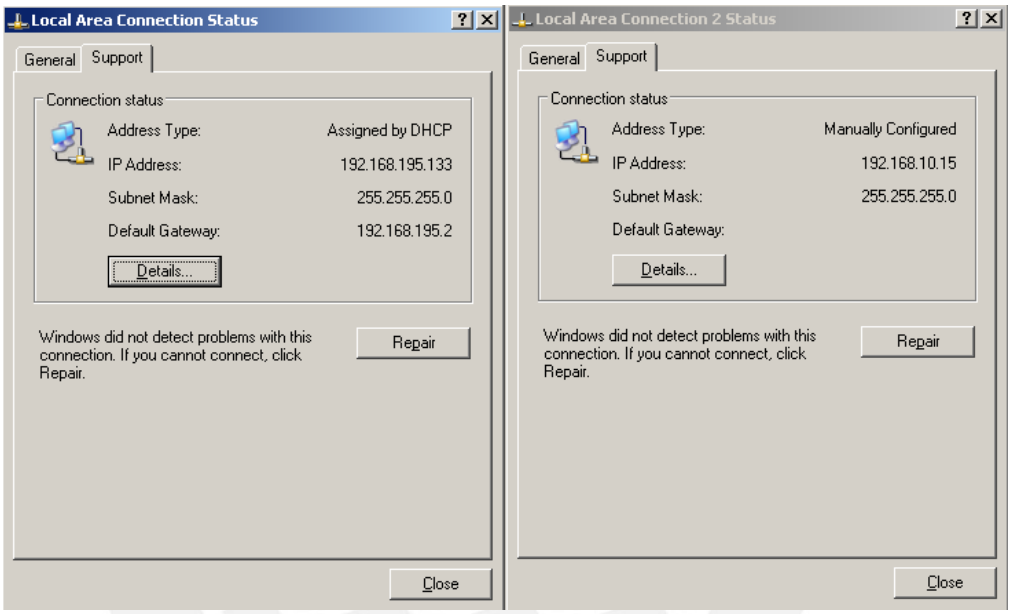

FIGURA 5.18 DATOS DE RED DEL SERVIDOR ISA SERVER 2004

Como se puede apreciar en la figura 5.18, el equipo cuenta con dos interfaces con direcciones IP distintas, lo que es razonable debido a que el equipo se encuentra operando en el nivel 3 de OSI. Es necesario mencionar que únicamente la interface ubicada en la zona externa cuenta con una ruta predefinida o *Default Gateway*.

5.4.4.2 Reglas de acceso

Las reglas de acceso mencionadas en el punto 5.3.2.4 se establecieron de la siguiente manera en el dispositivo.

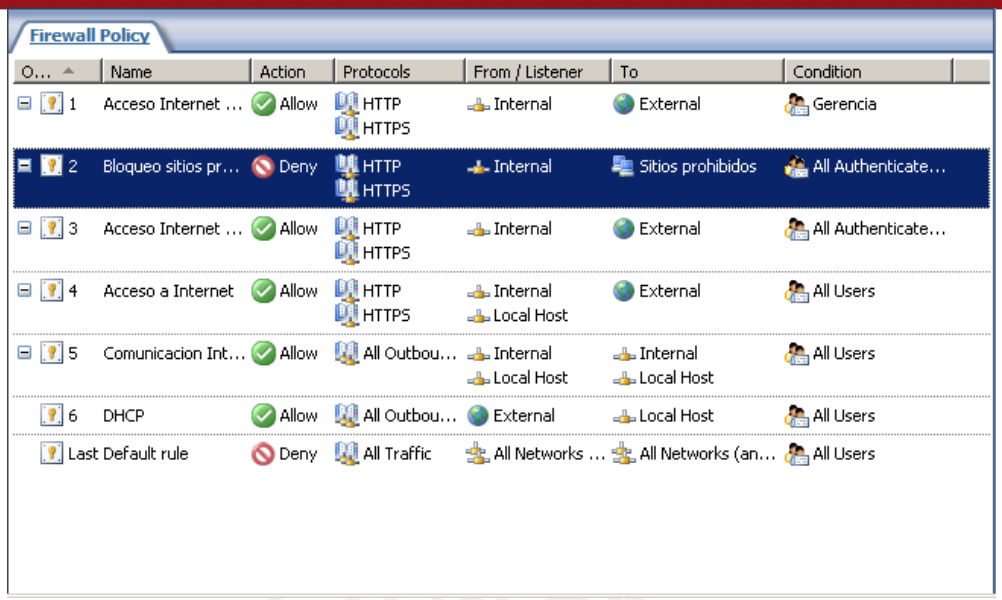

FIGURA 5.19 REGLAS DE ACCESO APLICACADAS EN EL SERVIDOR ISA SERVER 2004

Tal y como se puede apreciar en la figura 5.19, las reglas 3 y 4 del Servidor ISA Server 2004 permiten el acceso a internet a los usuarios ubicados en la zona “Internal” hacia la zona “External”. La regla 1 permite el acceso a internet de manera irrestricta a los gerentes. La regla 2 bloquea el acceso a ciertos sitios web para los demás usuarios, y el acceso a los demás sitios permitidos es garantizado por las reglas 3 y 4.

5.4.4.3 Prueba de servicios

Se realizaron pruebas de navegación con diferentes cuentas de acceso y se aseguró que ningún usuario no autenticado podía salir a navegar a internet.

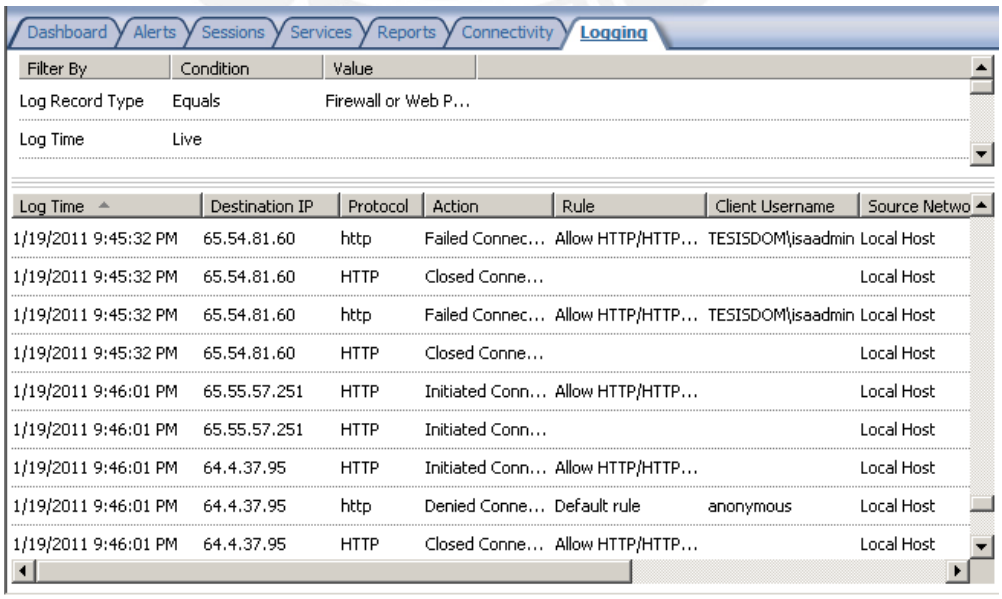

FIGURA 5.20 EXTRACTO DEL LOG DEL ISA SERVER 2004

En la figura 5.20 se puede apreciar una muestra del log del servidor ISA SERVER 2004 en la cual se muestra los intentos de salida a internet realizados por usuarios autenticados y no autenticados de la red interna, y la aplicación de la regla respectiva.

Como se puede apreciar en la octava entrada del log mostrado en la figura 5.20, los usuarios anónimos no pueden salir a navegar a internet. Esto está de acuerdo con la política establecida donde solo usuarios autenticados pueden salir a navegar.

5.5 Certificación del diseño.

Se verifica el cumplimiento de los requerimientos de la empresa presentados en el punto 2 del Capítulo 3.

TABLA 5.9 CUMPLIMIENTO DE REQUERIMIENTOS DE LA SOLUCION

ID	Requerimiento	Cumplimiento
1	**Requerimientos de administración y gestión**	
	Gestión centralizada y delegada de las soluciones de control de acceso.	El firewall perimetral, el firewall interno y el concentrador VPN SSL serán gestionados desde la consola centralizada de Juniper, Network & Security Manager (NSM)
	Capacidad de generación de reportes correlacionados.	El NSM es capaz de correlacionar los logs provenientes de todos los equipos que gestiona.
	Control de acceso a Internet de direcciones URL y protocolos.	El control granular de los protocolos y direcciones URL es realizado por el servidor ISA Server 2004, que cumple la función de proxy de navegación en la red.
	Mínimo impacto sobre los demás elementos de red y usuarios.	El único cambio que podría afectar a los usuarios internos es la necesidad de configurar el proxy en su navegador de internet, sin embargo, esto se salvó aplicando este cambio de manera global en todas las computadoras mediante una política de seguridad en el controlador de dominio.
	Reutilizar en la medida de lo posible los productos de seguridad con los que actualmente cuenta la empresa.	Se está conservando la licencia de Microsoft ISA Server 2004. La licencia de GroupShield de McAfee no se conserva debido a que la empresa decidió optar por otra solución antispam.
1.1	**Instalación y mantenimiento de la configuración de la solución de control de accesos perimetral.**	
	Definición de los grupos, roles y responsabilidades para la administración lógica de los firewalls, creación y modificación de la política de seguridad y generación de reportes.	El NSM permite crear cuentas de acceso con diferentes perfiles que permiten restringir el acceso a los dispositivos de seguridad y registrar todos los cambios y accesos realizados mediante un registro de eventos de auditoría.

	No permitir la conexión de direcciones de red internas desde el Internet hacia la DMZ (antispoofing).	El firewall Juniper SSG5 cuenta con la configuración que evita que una dirección IP registrada en una zona de seguridad pueda acceder al firewall desde una zona diferente.
	Bloquear todo tráfico entrante/saliente no declarado como permitido.	Se definió en el firewall un grupo de políticas "Clean Up" para esta función
	Implementar una DMZ que filtre y analice cualquier tráfico, para prohibir el acceso directo desde y hacia el Internet, desde la red de usuarios.	Los únicos equipos que tienen acceso hacia internet son el Antispam y el Proxy de Navegación.
	Utilizar NAT para enmascarar todo el tráfico saliente hacia Internet.	Tanto el Antispam, el proxy y el servidor de correo están enmascarados tras las direcciones IP IP_Pub_Correo, IP_Pub_01 y IP_Pub_OWA.
	Todo acceso requerido desde internet debe realizarse a través de un medio seguro y encriptado.	El correo web es accedido a través de HTTP sobre SSL (HTTPS). Los otros accesos son realizados mediante la VPN SSL.
1.2	**Asignación de un único ID por usuario**	
	Identificar a todos los usuarios con un único usuario antes de brindarle acceso a los sistemas desde internet.	Todos y cada uno de los usuarios que acceden remotamente cuentan con un usuario único de acceso. Ver tabla 12.
	Implementar al menos uno de los siguientes métodos de autenticación para todos los usuarios: • Contraseña • Token • Biometría	Las contraseñas que deben ingresar los usuarios son una combinación de un código que ellos conocen y el número que arroja el token, y que cambia cada minuto.
	Implementar autenticación de dos factores para el acceso remoto de los empleados, administradores y terceros.	Todos y cada uno de los usuarios que acceden remotamente cuentan con un usuario único de acceso. Ver tabla 12.
	Habilitar el acceso remoto al proveedor solo durante el tiempo necesario para la tarea requerida.	El perfil de acceso para el proveedor será activado manualmente cuando sus servicios sean requeridos.
	Requerir una longitud mínima de las contraseñas a un mínimo de 9 caracteres.	La contraseña esta conformada por 8 dígitos que entrega el token + una contraseña no menor de 7 dígitos que el usuario conoce.
	Forzar que las contraseñas de los usuarios cuenten con caracteres numéricos y alfanuméricos.	El equipo Juniper SA2500 permite forzar el cumplimiento de este requerimiento.
	Prohibir el re-uso de contraseñas con una antigüedad menor a cinco cambios.	El equipo Juniper SA2500 permite forzar el cumplimiento de este requerimiento.

	Bloquear una cuenta de usuario luego de seis intentos fallidos de acceso.	El equipo Juniper SA2500 permite forzar el cumplimiento de este requerimiento.
1.3	**Evaluar constantemente la seguridad de los sistemas y procesos**	
	Realizar escaneos de vulnerabilidades externos e internos constantemente y cada vez que se implemente un nuevo sistema, componente de red, o se realice algún cambio en la topología de la red o a nivel del firewall.	No es parte de la presente tesis.
	Realizar pruebas de penetración al menos una vez al año y cada vez que se realice una modificación en la red.	No es parte de la presente tesis.
	Utilizar sistemas de detección de intrusos para monitorear todo el tráfico de la red y alertar sobre eventos sospechosos.	El SSG5 cuenta con licenciamiento de prevención de intrusos el cual será activado y configurado en el proceso de implementación.
	Mantener los detectores de intrusos actualizados	El NSM estará configurado para actualizar de manera diaria su base de datos de ataques de red.
2	**Requerimientos técnicos**	
	Capacidad de alta disponibilidad en modo activo-pasivo en ambos firewalls.	El equipo Juniper SSG5 cuenta con la capacidad de funcionar en modo activo-pasivo.
	Capacidad de configuración de enlace de respaldo en el firewall perimetral.	El equipo Juniper SSG5 es capaz de manejar hasta 3 enlaces a internet diferentes.
	Aplicación de filtro de paquetes dinámico en los firewalls.	El equipo Juniper SSG5 cumple con esta funcionalidad.
	Bloqueo de ataques de negación de servicio.	El equipo Juniper SSG5 cumple con esta funcionalidad.
	Capacidad de bloqueo de ataques o intentos de intrusión.	El equipo Juniper SSG5 cumple una vez activada la licencia de prevención de intrusos.
2.1	**Firewall Perimetral e Interno**	
	Capacidad para configurar túneles VPN	Si cumple.
	Soporte de IPv6	Si cumple.
	Soporte de traslación de direcciones de red (NAT)	Si cumple.
	Soporte de VoIP	Si cumple.
	Control de flujo y ancho de banda	Si cumple. Por regla
	Capacidad de prevención de intrusos, filtro de contenido y antivirus embebido	Si cumple. Por regla
2.2	**Control de Acceso Remoto (VPN SSL)**	
	Acceso basado en políticas	Si cumple.

	Granularidad en las políticas	Si cumple.
	Control de acceso de acuerdo a regulaciones de seguridad	Si cumple.
	Comunicación encriptado entre el cliente y el dispositivo VPN	La comunicación entre el SA2500 y el usuario es via HTTPS.
	No necesidad de cliente instalado	El equipo cliente solo requiere instalar un componente de tipo Active-X o java.
2.3	**Control de acceso a Internet**	
	Capacidad de aplicar políticas por usuarios y grupos de usuarios definidos en el directorio activo de la empresa.	El Microsoft ISA 2004 es capaz de aplicar políticas por usuarios y grupos de usuarios de directorio activo.
	Filtro de protocolos de Internet	El ISA 2004 es capaz de identificar protocolos que viajan encapsulados sobre HTTP y HTTPS como mensajería instantánea y p2p.
	Capacidad para filtrar direcciones en internet por su dirección y/o su dirección IP.	El ISA 2004 es capaz de crear listas de URL y direcciones IP, y utilizarlas en sus políticas de acceso.

5.6 Cumplimiento de requerimientos del cliente.

En el punto 3.2 se presentó los requerimientos generales del cliente con respecto a la solución de seguridad requerida.

ID	Requerimiento	Cumplimiento
1	Una solución de les permita proteger la red de ataques provenientes desde internet.	El firewall Juniper SSG5 cuenta con la funcionalidad de inspección de estado y protección contra ataques de denegación de servicio y basados en anomalías de red, lo cual eleva de manera considerable el nivel de seguridad de la red.
2	Aprovechar de manera efectiva el servicio de internet, permitiendo tener visibilidad y control en todo momento del tráfico saliente y entrante.	El firewall Juniper SSG5 cuenta con la funcionalidad de calidad de servicio (QoS) que permite administrar de manera inteligente el ancho de banda entregado por el proveedor de servicio de Internet, de manera que se priorice la comunicación de aquellos servicios y aplicaciones importantes para el negocio.
3	Control granular de acceso a Internet de direcciones URL y protocolos.	El servidor ISA Server permite generar políticas de control de acceso por URL y protocolos basado en perfiles de acceso asignados por usuarios o grupos de usuario de dominio. Esto, complementado con la funcionalidad de QoS del firewall perimetral, brinda un control bastante efectivo.

4	Seguridad y granularidad en el acceso a los usuarios que se conectan de manera remota desde internet, pudiendo llevar un registro de sus accesos.	El equipo Juniper SA700 permite establecer el nivel de cifrado a ser utilizado para encriptar la comunicación con los clientes remotos. Adicionalmente, cuenta con la funcionalidad de *Host Checker*, que permite evaluar el nivel de seguridad del dispositivo remoto antes de permitirle acceder a la red corporativa.
5	Mínimo impacto sobre los demás elementos de red y usuarios. Es decir, que la implementación de la nueva solución de seguridad no afecte de manera negativa en la manera en que los usuarios desempeñan sus funciones.	Debido a que el alcance de ésta tesis es el diseño de la solución, esto no pudo ser validado, sin embargo, en la figura 5.5 se muestra las condiciones de operación de un equipo de similares características, cumpliendo la función de firewall perimetral para una red de de aproximadamente 100 usuarios nombrados.
6	Reutilizar en la medida de lo posible los productos de seguridad con los que actualmente cuenta la empresa	Se mantiene operativo y reubicado el servidor ISA Server 2004. El producto GroupShield fue removido del servidor de correo pero no fue reutilizado debido a que la empresa ya había tomado la decisión de cambiar de solución antivirus/antispam de correo electrónico. El router de Internet se mantiene debido a que pertenece al proveedor de servicio. Todos los demás elementos de red se conservaron.

Finalmente, el problema inicial reportado por el cliente y que fue mencionado en el punto 3.1.1, se encuentra cubierto según se expone.

- El firewall perimetral permite realizar un control exhaustivo del trafico entrante y saliente, además de notificar cuando se exceda cierto comportamiento de la red, en cuanto al acceso a internet.
- El equipo VPN-SSL es capaz de registrar cada intento de acceso, así sea fallido, además de realizar un control de seguridad en los dispositivos que deseen conectarse desde internet.
- El antispam permite controlar el tráfico de correo saliente, deteniendo cualquier intento de inundar internet con correos spam o maliciosos.

Conclusiones

- El servidor de correo, que compartía recursos con el antispam, presentaba un alto consumo de recursos debido a que cada correo entrante debe ser analizado por los motores de análisis del antispam para luego ser enviado al motor del servicio de correo y finalmente depositado el correo en la casilla del usuario. En cada una de estas etapas, una copia temporal del correo es escrita en el disco duro. Esta es una razón adicional para justificar la implementación de una solución antispam fuera del servidor de correo electrónico. Una evaluación posterior realizada posteriormente a la implementación de la solución propuesta corroboró ésta teoría.

- Las formulas utilizadas en el punto *3.3.4.1 Dimensionalmiento del Firewall Perimetral* para calcular el número de sesiones concurrentes no son un cálculo exacto y puede variar de acuerdo a los hábitos de uso de internet de los usuarios de la empresa. Sin embargo pueden proveer un dato bástate útil y que puede ser utilizado para dimensionar un equipo para éste propósito. En caso se identifique que existen otras aplicaciones que puedan significar un aumento en el numero de sesiones, como por ejemplo: telefonía por internet, telefonía IP a través de un proveedor externo; debe replantearse la formula o utilizar algún otro método para calcular el total de sesiones concurrentes que debe soportar el equipo. En caso de no poder obtener una formula convincente, es necesario medirlo de manera práctica. Una buena práctica para este fin es colocar alguno de los equipos propuestos en modo transparente de manera que nos permita obtener la información necesaria.

- La selección de los fabricantes o marcas de los productos no necesariamente debe basarse en la información provista por Gartner. Existen además otras empresas dedicadas a evaluar los distintos productos existentes en el mercado. Sin embargo, un dato bastante apreciado en el mercado local son las empresas que actualmente utilizan ese producto. La selección del producto muchas veces se puede realizar basándose únicamente en referencias.

- Tal y como mencionó en los puntos 4.3 y 4.5, cada red cuenta con requerimientos específicos que deben ser considerados como prioridad al diseñar su arquitectura o topología de red, sin embargo, la presente tesis puede servir como referencia o base para dicho diseño.

Recomendaciones

- En la actualidad existe una gran variedad de productos de seguridad. Todos ellos ofrecen una gran cantidad de funcionalidades adicionales que terminan por marear a la empresa y pueden provocar que opten por un producto que no va de acuerdo a lo que necesitan. Es este aspecto es muy importante que la empresa tenga en claro sus necesidades respecto a seguridad de la información para poder seleccionar el producto y/o solución que mejor cumpla con estos requerimientos y se ajuste a la capacidad de adquisición de la empresa.

- Es importante que, en el caso de que la empresa no cuente con una persona especialista en seguridad de la información, se busque orientación por parte de un experto en el tema antes de adquirir y/o implementar alguna solución.

- En temas de seguridad de la información, existen muchas alternativas de solución para un problema. Por ello es importante entender y analizar a profundidad el problema antes de salir a comprar programas o equipos. Más importante aun es tener en cuenta que la solución que le funcionó bien a una empresa, no necesariamente va a funcionar bien en la nuestra.

- Un dato importante al seleccionar los productos de seguridad a implementarse es el dimensionamiento de los equipos. Si se consideró que la solución deberá tener un tiempo de vida de 5 años, por ejemplo, se debe considerar que los equipos sean capaces de soportar los requerimientos de la red en el mismo periodo.

- Hasta la mejor solución de seguridad es inefectiva si no cuenta con una política de seguridad efectiva y el personal que lo administra no tiene los conocimientos necesarios para entender y generar una respuesta ante algún incidente.

- Tanto la política de seguridad aplicada en los productos de seguridad lógica como los procedimientos de mantenimiento de la solución de seguridad y respuesta ante incidentes deben estar plasmados en un documento oficial de la empresa y que debe ser revisado constantemente.

- Finalmente, si bien existen estándares en temas de seguridad de la información, es importante que son un recopilatorio de buenas prácticas que funcionan bien en la mayoría de las empresas, pero que no es una obligación aplicarla en su totalidad. Se deben tomar únicamente aquellos puntos que se consideren necesarios y apliquen a nuestro escenario.

Bibliografía

[STA2005] STAMP, MARK. “Information Security, Principles and Practice” Estados Unidos de América. 2005

[SET2005] STEWART, James Michael et al.
CISSP: Certified Information Systems Security Professional. Study Guide 3a. Ed. Sybex. 2005
San Francisco, EUA

[FER2006] FERRARI, Elena y THURAISINGHAM, Bhavani
Web and Information Security. IRM Press. 2006
Philadelphia, EUA

[TIP2004] TIPTON, Harold y KRAUSE, Micki
Information Security Management Handbook. 5a. Ed. CRC Press. 2006
Florida, EUA

[STE2005] STEINBERG, Joseph y SPEED, Timothy
SSL VPN, Understanding, evaluating, and planning secure, web-based remote access.1a. Ed. Packt Publishing. 2005
Birmingham, Reino Unido

[PWR2000] POWER, Richard
Tangled Web. Tales of Digital Crime from the Shadows of Cyberspace. 1a. Ed. Que/Macmillan. 2000
Estados Unidos de América

[HRS2002] HARRIS, Shon
All in One. CISSP Certification. 2a. Ed. Mc. Graw Hill. 2002
California, EUA

[ISC2005] ISACA
Information Security Harmonisation. 2005
Estados Unidos de América

[CURT1997] CURTIN, Matt
Introduction to Network Security. 1997
Estados Unidos de América

[CRON2003] CRONJE, Gerhard
Choosing the best Firewall. SANS Institute. 2003
Estados Unidos de América

[HRN2001] HERNANDEZ, Claudio
Hackers Segunda Edición. 2001
España

[CIS2003] Cisco Microsystems
The Science Of Intrusion Detection System. 2003

[JNP2010] Juniper Networks. [Consultado 2010/08/23]
URL: http://www.juniper.net

[CPS2010] Checkpoint Software Technologies [Consultado 2010/08/23]
URL: http://www.checkpoint.com

[SAN2007] The SANS Institute [Consultado 2007/09/09]
URL: http://www.sans.org

[CIS2007] Cisco Systems Inc. [Consultado 2007/09/16]
URL: http://ww.cisco.com

[ISO2010] International Organization for Standardization. [Consultado 2010/08/21]
URL: http://www.iso.org/iso/

[ISE2010] ISO27000.es. [Consultado 2010/08/21]
URL: http://www.iso27000.es/

[RSA2010] RSA, The Security Division of EMC [Consultado 2010/09/16]
URL: http://ww.rsa.com

[GAR2010] GARTNER [Consultado 2010/05/21]
URL: http://www.gartner.com

[MCF2010] Mcafee. [Consultado 2010/08/26]
URL: http://www.mcafee.com

[TRM2010] Trendmicro [Consultado 2010/08/29]
URL: http://www.trendmicro.com