



**Universidad Central de Venezuela  
Facultad de Ingeniería.  
Escuela de Ingeniería Eléctrica.**



**DISEÑO E IMPLANTACIÓN DE LA INFRAESTRUCTURA DE ZONAS DE  
SEGURIDAD PARA LA EMPRESA**

**KELSY**

**TRABAJO DE GRADO PRESENTADO ANTE LA ILUSTRE UNIVERSIDAD  
CENTRAL DE VENEZUELA PARA OPTAR AL TÍTULO DE  
ESPECIALISTA EN COMUNICACIONES Y REDES DE  
COMUNICACIONES DE DATOS**

Presentado por:

**Ing. José Raúl Quiñónez Keller**

**Caracas, Octubre del 2005**

**© José Raúl Quiñónez Keller**  
**Hecho el Depósito de Ley**  
**Depósito Legal Ift487200562083**



**Universidad Central de Venezuela  
Facultad de Ingeniería.  
Escuela de Ingeniería Eléctrica.**



**DISEÑO E IMPLANTACIÓN DE LA INFRAESTRUCTURA DE ZONAS DE  
SEGURIDAD PARA LA EMPRESA**

**KELSY**

**TRABAJO DE GRADO PRESENTADO ANTE LA ILUSTRE UNIVERSIDAD  
CENTRAL DE VENEZUELA PARA OPTAR AL TÍTULO DE  
ESPECIALISTA EN COMUNICACIONES Y REDES DE  
COMUNICACIONES DE DATOS**

Tutor Académico:

**Prof. Vincenzo Mendillo**

**Caracas, Octubre del 2005**



**UNIVERSIDAD CENTRAL DE VENEZUELA  
FACULTAD DE INGENIERÍA  
ESCUELA DE INGENIERÍA ELÉCTRICA**

**POSTGRADO EN ESPECIALIZACIÓN EN COMUNICACIONES Y REDES  
DE COMUNICACIÓN DE DATOS**

**DISEÑO E IMPLANTACIÓN DE LA ARQUITECTURA DE ZONAS DE  
SEGURIDAD PARA LA EMPRESA KELSY**

**Autor:** Ing. José Raúl Quiñónez Keller      **Tutor:** Prof. Vincenzo Mendillo

Octubre de 2005

**RESUMEN**

El presente trabajo de especial de grado tiene como objetivo implantar un sólido esquema basado en zonas de seguridad perimetrales de alta disponibilidad con balanceo de carga para el portal de servicios Web de una empresa grande, con el fin de garantizar la disponibilidad de los recursos y servicios de la red, permitiendo así aumentar la calidad de los procedimientos relacionados con el área de negocios. Esta nueva arquitectura de zonas de seguridad perimetrales debe brindar confiabilidad, escalabilidad, rendimiento y niveles de seguridad adecuados, para cubrir las demandas de protección de toda la plataforma tecnológica existente.

Para alcanzar el objetivo se realizó un estudio y análisis de la plataforma actual de seguridad, lo cual permitió evaluar opciones que conllevaron a reforzar la seguridad del acceso a todas las áreas de negocio de la empresa, mejorando y brindando una mayor protección a toda la red. El diseño del sistema propuesto se implantó satisfactoriamente, solventando así las vulnerabilidades existentes mediante mecanismos de seguridad tanto técnicos como administrativos, disponibles a través de la tecnología de firewall del alto rendimiento con categoría “carrier class”, obteniendo los resultados esperados y cubriendo así los requerimientos de la empresa.

## DEDICATORIA

*A Dios por haberme dado la dicha de estar en este mundo.*

*A mi madre por darme el ser, por inculcarme las ganas de luchar y dar todo lo que se quiere, por apoyarme y levantarme cada vez que lo necesito.*

*A mi esposa Gaby... por ser tan especial, por llenarme de alegría con su mejor sonrisa, por su constante apoyo y por darme a un ángel que llenará mi vida de más alegría e ilusiones.*

*A mis hijos por obligarme a luchar cada día más por alcanzar mis metas.*

*De verdad los quiero muchísimo a todos...*

*El autor*

## **AGRADECIMIENTO**

A mi Madre y Familiares... por brindarme su amor y apoyo incondicional durante mis estudios.

A mis esposa...por sus buenos consejos, sus palabras de aliento y chistes oportunos que me llenaron de fuerza, alegría y motivación, en los momentos de más tensión.

A mi tutor, Vincenzo Mendillo, por impulsarme a culminar la tesis y brindarme su apoyo y consejos con su gran experiencia.

A todos Mil Gracias

## INDICE GENERAL

Resumen .....	i
Dedicatoria .....	ii
Agradecimiento .....	iii
<b>Introducción</b> .....	<b>7</b>
<b>CAPÍTULO I: El Problema</b>	
<b>I.1 Formulación del Problema</b> .....	<b>9</b>
<b>I.2 Objetivo Estratégicos</b> .....	<b>12</b>
<b>I.3 Objetivos General</b> .....	<b>12</b>
<b>I.4 Objetivos Específicos</b> .....	<b>13</b>
I.5 Justificación .....	13
I.6 Alcance y Limitaciones .....	15
<b>CAPÍTULO II: Marco Teórico</b>	
<b>II.1 Antecedentes</b> .....	<b>16</b>
<b>II.2 Conceptos Básicos</b> .....	<b>17</b>
II.2.1 La Información .....	17
II.2.2 La Integridad .....	17
II.2.3 La Disponibilidad u Operatividad .....	18
II.2.4 La Privacidad o Confidencialidad .....	18
II.2.5 La Autenticidad .....	18
II.2.6 Protección Contra Réplica .....	19
II.2.7 No Repudio .....	19
II.2.8 Consistencia .....	19
II.2.9 Confidencialidad .....	20

II.2.10 Auditoria .....	20
II.2.11 Amenaza .....	20
II.2.12 Riesgo .....	21
II.2.13 Daño .....	21
II.2.14 Vulnerabilidades .....	22
II.2.15 Fiabilidad .....	22

### **II. 3 Tipos de Ataques más Comunes**

II.3.1 IP Spoofing .....	23
II.3.2 Ping flood .....	24
II.3.3 Ping de la muerte .....	24
II.3.4 Syn flood .....	24
II.3.5 Land Attack .....	25
II.3.6 Teardrop .....	25
II.3.7 TCP hijacking .....	25
II.3.8 Sniffers .....	25
II.3.9 DdoS attacks .....	26
II.3.10 Ingenieria Social .....	26
II.3.11 Escaneo de Redes .....	27
II.3.12 Hurto de Password .....	27
II.3.13 Explotación de Vulnerabilidades .....	27

### **II.4 Firewall**

II.4.1 Concepto de Firewall .....	28
II.4.2 Tipos de Firewall .....	29
II.4.2.1 Packet Filter .....	29
II.4.2.2 Application Level Gateway .....	29
II.4.2.3 Proxy Circuit Level Gateway .....	30
II.4.2.4 Stateful Packet Inspection .....	30
II.4.2.5 Deep Packet Inspection .....	31
II.4.3 Firewall de Hardware (Appliance) contra Firewall Basados en Software .....	32



II.4.4 Zonas de Seguridad DMZ (Perímetros de Seguridad) .....	34
II.4.5 Desarrollo de las Zonas de Seguridad Perimetales .....	37
II.4.5.1 Importancia de las Zonas de Seguridad .....	38
II.4.6 Firewall Basados en ASIC (Circuitos Integrados de Aplicaciones Específicas), para implementar DMZ .....	38
II.4.6.1 Routers Virtuales .....	40
II.4.6.2 Interfaces .....	41
II.4.6.3 Políticas .....	42
II.4.6.4 Plantillas de Protección contra Ataques Comunes .....	42
II.4.7 VPN ( Redes Privadas Virtuales) .....	45
II.4.7.1 Aspectos Funcionales .....	47
II.4.7.2 IPSEC .....	48
II.4.7.3 AH .....	50
II.4.7.4 Tipos de Configuraciones AH .....	51
II.4.7.5 Protocolo ESP .....	52
II.4.7.6 Tipos de Configuraciones ESP .....	53
II.4.7.7 Protocolo IKE .....	54
II.4.8. VPN Mediante Tecnología ASIC .....	56
II.4.8.1 VPN Basadas en Rutas .....	56
II.4.8.2 VPN Basadas en Políticas .....	56
II.4.9 Alta Disponibilidad .....	58
II.4.9.1 Tolerancia a Fallos .....	59
II.4.9.2 Obejetivo de la Alta Disponibilidad .....	59
II.4.10 Administración de los Firewall ASIC y Ejemplos de Configuración .....	59

### **CAPÍTULO III: Sistema Actual**

<b>III.1</b> Enfoque del Sistema Actual.....	70
<b>III.2</b> Plataforma Tecnológica del Sistema de Seguridad Actual.....	72
III.2.1 Servicios y Accesos Disponibles.....	75
III.2.1.1 Acceso a Internet .....	75

III.2.1.2 Acceso Remoto Dial-Up .....	75
III.2.1.3 Enlaces VPN Y RAS para los Aliados de Negocio.....	77
III.2.1.4 Extranet .....	77
III.2.1.5 LAN y WAN.....	77
III.2.1.6 Direccionamiento IP De las 3 Zonas Actuales.....	77
III.2.1.6.1 Zona Trust.....	77
III.2.1.6.2 Zona Untrust.....	78
III.2.1.6.3 Zona DMZ.....	78
III.3 Especificaciones del Sistema de Seguridad actual .....	78
III.4 Políticas de Seguridad Generales Aplicadas en el firewall.....	79
III.4.1 Política de Acceso al Exterior Zona (Untrust).....	79
III.4.2 Política de Detección de Intrusos.....	80
III.4.3 Publicación del Portal de Servicios.....	80
III.5 Limitaciones en el Entorno del Sistema de Seguridad Actual.....	80
III.6 Análisis y Elección de los Nuevos Dispositivos firewall .....	80

## **CAPÍTULO IV: Sistema Propuesto**

IV.1 Solución Conceptual Del Sistema Propuesto.....	82
IV.2 Consideraciones del Diseño .....	83
IV.2.1 Documentar Adecuadamente la Arquitectura de firewall .....	83
IV.2.2 Análisis de los Requerimientos de Seguridad de la Organización.....	84
IV.2.3 Segmentación de las Zonas de Seguridad.....	84
IV.2.4 Integración de los dispositivos firewall con otros Controles de Seguridad.....	86
IV.3 Diseño de la Solución de Nuevas Zonas Seguridad.....	87
IV.3.1 Nuevo Esquema de Zonas de Seguridad.....	89
IV.3.1.1 Zona MGT Administrativa.....	89
IV.3.1.2 Zona Confiable ( Trust).....	89
IV.3.1.3 Zona VPN y Aliados.....	89

IV.3.1.4 Zona de Servicios Web.....	90
IV.3.1.5 Zona Extranet.....	90
IV.3.1.6 Zona Bancaria.....	90
IV.3.1.7 Zona de Servidores Públicos.....	90
IV.3.1.8 Zona no Confiable Internet ( Untrust).....	91
IV.3.1.9 Zona de Base de Datos.....	91
IV.4 Diseño del Direccionamiento IP de las Zonas.....	91
IV.5 Políticas Aplicadas a las Zonas de Seguridad.....	95
IV.6 Notación para Documentar las Reglas del firewall.....	95
IV.7 Consideraciones Operacionales para los Enlaces de Conexión Internet.....	99
IV.8 Mecanismos de Balanceo de Cargas.....	99
IV.8.1 Sistemas para el balanceo de las Cargas HTTP y HTTPS.....	99
IV.8.2 Ventajas que Ofrece el Balanceo de Cargas.....	100
IV.9 Configuración del SLB.....	102
IV.9.1 Tipos de Métricas disponibles para balanceo del Tráfico.....	104
IV.9.1.1 Least connections.....	104
IV.9.1.2 Round Robin.....	104
IV.9.1.3 Weighted.....	105
IV.9.1.4 Server Response Time Only.....	105
IV.9.1.5 Least connection and server response time <i>weights</i> .....	106
IV.9.1.6 Least local connections.....	106
IV.9.1.7 Least local session.....	106
IV.9.2 Métrica Seleccionada para Solución.....	106
IV.10 Configuración de los Enlaces VPN.....	111
IV.10.1 VPN Basadas en Políticas.....	111
IV.11 Alta Disponibilidad de los Equipos firewall.....	115
IV.11.1 Confiabilidad.....	116
IV.11.2 Escalabilidad.....	116
IV.11.3 Sistema de Monitoreo, Control y Gestión de Fallas.....	116

IV.12 Plan de Implantación.....	117
IV.12.1 Migración.....	119
IV.12.2 Asignación de Recursos.....	119
<b>CONCLUSIONES.....</b>	<b>121</b>
<b>RECOMENDACIONES.....</b>	<b>123</b>
<b>REFERENCIAS BIBLIOGRÁFICAS.....</b>	<b>125</b>

## INTRODUCCIÓN

Es fácil leer en las noticias cotidianas del mundo de la seguridad informática, los frecuentes ataques de negación de servicio, robo de información, destrucción de sistemas y muchos otros daños y pérdidas económicas, causados por los hacker a muchas organizaciones.

La seguridad de las redes se ha convertido en un asunto prioritario en la mayoría de las corporaciones, el reto de la seguridad de redes ha captado la atención de prácticamente todos los miembros de las juntas directivas y alta gerencia.

La transferencia de datos electrónicos, el aumento exponencial de usuarios que hacen uso de la Internet, y el crecimiento del número de empresas que cada día hacen uso de las redes para su gestión de trabajo diario, trae como consecuencia que las organizaciones tanto privadas como públicas tengan la necesidad de integrar la seguridad de su información tanto física como electrónica, en todas las facetas del negocio.

La conciencia de implantar mecanismos de protección en la redes corporativas, se inicia en lo más alto de la organización y desciende hacia las contribuciones individuales. Las organizaciones actualmente reconocen, que ante los múltiples ataques registrados contra sitios en las redes distribuidas, es de vital importancia la inversión en tecnología de seguridad que protejan a las empresas de potenciales ataques que puedan afectar la continuidad operativa de la misma.

El presente trabajo especial de grado, representa una solución para la empresa bajo estudio y consiste en la implantación de una arquitectura de zonas de seguridad perimetrales de alta disponibilidad, con capacidad de balanceo de carga en los servicios del portal Web. Dicha empresa cuenta actualmente con servicios, aplicaciones, y redes extranet que requieren un sólido esquema de seguridad que permita un acceso seguro a Internet y a todas las aplicaciones de negocio, y que a su vez pueda brindar confidencialidad, confiabilidad, escalabilidad, alto desempeño y rendimiento, de la mano con una mayor seguridad para cubrir las demandas de protección de toda su plataforma tecnológica.

# **CAPÍTULO I**

## **PLANTEAMIENTO DEL PROBLEMA**

### **I.1 Formulación del Problema**

Hoy en día la seguridad no sólo se considera un problema tecnológico, sino un asunto que afecta directamente a la capacidad de mantener la continuidad funcional y operativa de la empresa y repercute directamente en la confianza de los clientes en los sistemas de gestión de negocio de la empresa. Por esta razón muchos de los ataques registrados en las empresas, nunca salen a la luz pública por el miedo afectar la reputación de la empresa y la confianza de los clientes. Así mismo la simple conexión hacia Internet en cualquier corporación, y la realización de operaciones electrónicas en la WWW, ponen en peligro los activos informáticos y la información vital tan importante para el funcionamiento de cualquier empresa, sin embargo la rápida implementación de nuevos programas de Internet gratuitos para explotar los potenciales huecos de seguridad de casi cualquier cosa que tenga un punto de conexión a la red, supone un riesgo aun mayor y un reto para los administradores de la seguridad en los tiempos actuales.

Los gerentes de seguridad de sistemas se enfrentan a la tarea de encontrar un medio eficaz de reducir al mínimo los incidentes de seguridad. Se proponen el reto de crear una arquitectura de seguridad que integre los objetivos comerciales de la compañía y los aspectos tecnológicos, mediante la creación de un mapa de seguridad de sus activos, vulnerabilidades y riesgos. No obstante esta tarea resulta ardua, las redes actuales están formadas por un laberinto de aplicaciones y de elementos de hardware que presentan numerosas vulnerabilidades, por ende los gerentes de seguridad de sistemas esperan de los fabricantes de software y hardware, que éstos les ayuden a evaluar y administrar la seguridad de la red de una forma más eficaz.

Una arquitectura de seguridad perimetral bien diseñada y adecuadamente implantada es una solución rápida, confiable y efectiva para la protección de los activos informáticos de cualquier empresa. A su vez una barrera de protección efectiva, contribuye a facilitar la integración de redes y diversos servicios de una manera organizada y simplificada. Muchas organizaciones han eliminado sus redes paralelas integrándolas mediante la utilización de esquemas de seguridad multizonas, obteniendo mejoras significativas en la seguridad, tiempos de respuestas, facilidad de administración, etc. Por tal motivo se diseñará e implantará un sistema de seguridad a la empresa KELSY C. A. La cuál tiene una década dedicándose al sector de servicios de asesoría legal y gestión en materia de impuestos, cubriendo las diversas áreas de especialización en su ramo que son de importancia para el desarrollo del país.

Básicamente los problemas que en la actualidad presenta la empresa en su plataforma de seguridad general, deben ser atendidos y solucionados de forma eficiente y rápida,



para así solucionar todas las gestiones de negocio a nivel nacional, estos son los siguientes:

- 1) Zona de seguridad genérica única y poco flexible, no adecuada al crecimiento de nuevos servicios de cara a sus clientes.
- 2) Problemas en referencia al direccionamiento IP y a la seguridad en las capas inferiores, al no existir VLAN( Redes Virtuales) en los Switch capa 2, donde se realizan las conexiones.
- 3) Limitaciones en referencia al número de conexiones VPN( Redes privadas virtuales), que actualmente se pueden establecer con las empresas aliadas de negocio.
- 4) Falta de una plataforma con redundancia y tolerancia a fallos.
- 5) Problemas de la arquitectura de seguridad por sus limitaciones, ya que actualmente los servidores y aplicaciones de negocio no están confinados a una zona de seguridad, todos los servicios incluyendo su portal Web están directamente funcionando en LAN, y las conexiones desde Internet llegan directamente a su red interna.
- 6) Falta de mecanismos de balanceo de carga para su portal de negocio.

Se puede observar, que el aspecto de seguridad es crítico, ya que en la plataforma actual todas las conexiones externas llegan primero a una zona de seguridad genérica, en la cual se aplican políticas de seguridad que controlan todos los accesos a los servidores internos, pero debido a la gran diversidad de nuevos servicios implantados, aumento de las conexiones con nuevos aliados de negocio, presentando así muchos problemas para la administración de la seguridad de forma eficiente.

Como respuesta a estos problemas es necesaria la implantación de una nueva arquitectura de seguridad, basada en zonas de seguridad independientes y con total flexibilidad, escalable en el tiempo y con total redundancia y tolerancia a fallos. Para lograr esto se utilizarán dispositivos con categoría carrier class, es decir equipos diseñados con una confiabilidad profesional cuya disponibilidad es del orden del 99.9999%, lo cual significa en un año de uso continuo, están certificados para estar fuera de servicio un máximo total de 5 minutos.

## **I.2 Objetivos Estratégicos**

Reforzar la seguridad de la empresa a niveles adecuados a su realidad tecnológica y operativa, y a su vez realizar una integración segura de la infraestructura de redes de la empresa con sus aliados de negocio y los clientes, mediante la implantación de un nuevo esquema de zonas de seguridad perimetrales que minimicen los riesgos potenciales en las transmisiones de la información y el acceso de los servidores de negocio, incluyendo su portal de servicios Web.

## **I.3 Objetivo General**

Diseñar e implantar un sólido esquema de seguridad basado en zonas de seguridad de alta disponibilidad y con balanceo de carga para el portal de servicios Web, que garantice el acceso seguro a las plataformas de negocio, así como también la seguridad de la WAN y LAN de la empresa.

#### **I.4 Objetivo Específicos**

- 1) Estudio detallado y levantamiento de la información de la situación actual.
- 2) Diseñar un nuevo esquema de zonas de seguridad perimetrales, con alta redundancia y balanceo de carga para el portal Web.
- 3) Recopilar la información en referencia a los servicios y protocolos necesarios en cada servidor, y sus esquemas de acceso desde cada zona de seguridad.
- 4) Elaborar un cronograma de actividades definiendo el inicio de la instalación, recursos humanos, alcance de las pruebas, entonación, culminación y entrega de documentación.
- 5) Configurar los equipos firewalls.
- 6) Apoyar la configuración de las bondades de balaceo de carga en los SLB (Switch Load Balance), en conjunto con el área responsable de estos equipos.
- 7) Ejecutar el control de cambio.
- 8) Implantar el nuevo esquema de seguridad, en forma paralela, de manera de no impactar el ambiente de producción actual.
- 9) Realizar pruebas de funcionamiento y entonación de la solución.
- 10) Aplicar pruebas de failover.
- 11) Manejar pruebas de penetración simples por parte del personal interno de seguridad de la empresa mediante uso de herramientas no comerciales.

#### **I.5 Justificación**

En los últimos 4 años la empresa KELSY C.A. ha invertido grandes recursos en la modernización de toda su plataforma tecnológica, lo cual incluye la infraestructura de

redes, seguridad de datos, servidores de negocio, aplicativos de negocio, y portales Web. Todas estas inversiones tienen los siguientes objetivos de cara a sus clientes:

- a) Contar con tecnología de punta mediante la cual la empresa pueda operar con niveles óptimos, a través de un sistema integral de negocio, con niveles de seguridad eficientes, modernos y confiables. La empresa esta apostando fuerte a los negocios electrónicos mediante la implantación de un completo portal Web de servicios electrónicos para todos sus clientes.
- b) Incrementar la cartera de servicios que ofrece la empresa a sus clientes.
- c) Garantizar la continuidad del negocio antes potenciales fallas de los equipos de seguridad y comunicaciones.
- d) Respalda los niveles de seguridad, que impliquen que todas las comunicaciones lleguen sólo hasta la zona correcta y que minimicen los riesgos de intrusiones a zonas no autorizadas.
- e) Implantar mecanismos de auditoría.

De todo esto se deduce la gran importancia que tiene para la empresa, el contar con una adecuada infraestructura de redes y seguridad que le permita brindar un servicio sin interrupciones (Carrier Class 99.99%), los 365 días del año y las 24 horas al día y garantizar el cumplimiento de su misión la cual es: Ser una empresa modelo para el proceso de desarrollo del Estado Venezolano, de sólido prestigio, confianza y

credibilidad nacional e internacional, en virtud de su gestión transparente, sus elevados niveles de productividad, y la excelencia de sus sistemas información.

## **I.6 Alcances y Limitaciones**

La presente solución contempla el diseño e implantación de toda la arquitectura de zonas de seguridad basada en la tecnología ASIC (Circuitos Integrados de Aplicaciones Específicas) del alto desempeño. Esto incluye el diseño, configuración, implantación y pruebas de la plataforma de zonas de seguridad de redes. Se entiende que todo lo referente a las pruebas de las aplicaciones del portal Web, base de datos, configuración de los SLB (switch load balance), conectividad de redes y aplicativos de negocio es responsabilidad de las áreas respectivas, que conforman el grupo de trabajo para la implantación integral de toda la nueva infraestructura de servicios de la empresa. El área de seguridad de redes, prestara todo el apoyo necesario al grupo multidisciplinario, para poder culminar con éxito este proyecto.

Así mismo se tiene contemplado una segunda fase del proyecto que incluye sistemas de detección y prevención de intrusos y la instalación de sistemas de auditoría. Esta fase del proyecto no está contemplada en la presente solución por razones de tiempo y disponibilidad de los equipos en Venezuela. El esquema de seguridad final también incluye sistemas de filtrado Web para el control de la navegación de los usuarios, y antivirus, que serán implantados por otro grupo de trabajo paralelo, por lo tanto tampoco se incluye en la presente solución.

## **CAPÍTULO II**

### **MARCO TEORICO**

#### **II.1 Antecedentes**

Existen varios y diversos métodos para implementar una intranet segura, pero ninguno por sí sólo puede brindar la suficiente seguridad, sino que es la combinación de todos estos elementos junto con una acertada planeación de políticas de seguridad, unos requerimientos específicos y las características propias de la empresa, son los que podrían ayudar a definir una eficiente estrategia de seguridad sin que todo esto interrumpa o entorpezca las actividades de los usuarios que son para los que finalmente la intranet se construyó.

La seguridad ha sido el principal concerniente a tratar cuando una organización desea conectar su red privada al Internet. Sin tomar en cuenta el tipo de negocios, se ha incrementado el número de usuarios de redes privadas por la demanda del acceso a los servicios de Internet, tal es el caso del World Wide Web (WWW), Internet Mail (e-mail), Telnet, y File Transfer Protocol (FTP). Adicionalmente, los corporativos buscan las ventajas que ofrecen las paginas en el WWW y los servidores FTP de acceso público en el Internet.

Para proveer el nivel de protección requerida, la organización necesita seguir una política de seguridad para prevenir el acceso no-autorizado de usuarios a los recursos

propios de la red privada, y protegerse contra la exportación privada de información. Aun si una organización no esta conectada a la Internet, esta debería establecer una política de seguridad interna para administrar el acceso de usuarios a porciones de red y proteger sensitivamente la información secreta. El firewall pasa a ser un elemento imprescindible cuando la red corporativa se interconecta con otras redes de terceros o con redes públicas como Internet.

## **II.2.- Conceptos Básicos**

En la Seguridad Informática se deberán conocer las características de lo que se pretende proteger: la Información. Se define *dato* como “la unidad mínima con la que se compone cierta información”.

### **2.1- La Información**

Es una agregación de datos que tiene un significado específico más allá de cada uno de estos y tendrá un sentido particular según como y quien la procese, y tendrá un sentido particular según como y quien la procese.

### **2.2.- La Integridad**

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

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

### **2.3.- La Disponibilidad u Operatividad**

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

### **2.4.- La Privacidad o Confidencialidad**

De la información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la información puede provocar severos daños a su dueño (por ejemplo conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se “filtran” a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes). El control sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuando y como permitir el acceso a la misma.

### **2.5.- La Autenticidad**

Permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución.



Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades. Adicionalmente pueden considerarse algunos aspectos adicionales, relacionados con los anteriores, pero que incorporan algunos aspectos particulares:

### **2.6.- Protección Contra la Réplica**

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

### **2.7.- No Repudio**

Mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.

### **2.8.- Consistencia**

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

## 2.9.- Confidencialidad

Permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.

## 2.10.- Auditoria

Es la capacidad de determinar qué acciones o procesos se han llevado a cabo en el sistema, así como quién y cuando las realiza.

## 2.11.- Amenaza

En el entorno informático una amenaza se puede definir, como cualquier elemento que comprometa la integridad del sistema.



Amenazas para la seguridad. *Fuente: Seguridad Informática. Gustavo Adelgani.* Las amenazas pueden ser analizadas en tres momentos: antes, durante y después del ataque. Estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema informático.

- a. **La Prevención (antes):** mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo el cifrado de información para su posterior transmisión.
- b. **La Detección (durante):** mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.
- c. **La Recuperación (después):** mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionamiento normal. Por ejemplo recuperación desde las copias de seguridad (backup) realizadas.

## **2.12.- Riesgo**

Unas de las tantas definiciones de riesgo la presenta como “la proximidad o posibilidad de daño sobre un bien”. Ya se trate de actos naturales, errores u omisiones humanas y actos intencionales, cada riesgo debería ser atendido de la siguiente manera:

1. Minimizando la posibilidad de su ocurrencia.
2. Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.
3. Diseño de métodos para la más rápida recuperación de los daños experimentados.
4. Corrección de las medidas de seguridad en función de la experiencia recogida.

## **2.13.- Daño**

Es el resultado de la amenaza; aunque esto es sólo la mitad del axioma. El daño también es el resultado de la no-acción de la o acción defectuosa, del protector.

El daño puede producirse porque el protector no supo identificar adecuadamente la amenaza y, si lo hizo, se impusieron criterios comerciales por encima de los de seguridad, por ejemplo elegir un sistema simplemente porque es el más económico de implantar, sin importar si el mismo es seguro o adecuado a las necesidades de la organización.

#### **2.14.- Vulnerabilidades**

Son las debilidades del sistema que pueden ser explotadas y empleadas, es decir para que un ataque se concrete debe existir una vulnerabilidad y la misma debe ser explotable.

#### **2.15.- Fiabilidad**

Indicará el grado en que un sistema informático está libre de todo peligro, daño o riesgo. Esta característica es muy difícil de conseguir según los especialistas, es imposible en un 100%, por lo que sólo se habla de fiabilidad y se la define como la probabilidad de que un sistema se comporte tal y como se espera de él y se habla de sistema fiable en vez de sistema seguro.

Luego para garantizar que un sistema sea fiable, se deberá garantizar características comúnmente conocidas como son de Integridad, Operatividad, Privacidad, Control y Autenticidad. Se deberá conocer “qué es lo que queremos proteger”, “de quién lo queremos proteger”, “cómo se puede lograr esto legislativa y técnicamente”; para

luego concluir con la formulación de estrategias adecuadas de seguridad tendientes a la disminución (¿anulación?) de los riesgos.

Comprender y conocer de seguridad ayudará a llevar a cabo análisis sobre los riesgos, vulnerabilidades, amenazas y contramedidas; evaluar las ventajas o desventajas de la situación; a decidir medidas técnicas y tácticas metodológicas, físicas, e informáticas, en base de las necesidades de seguridad.

Es importante remarcar que cada unas de estas técnicas parten de la premisa de que *no existe el 100% de seguridad esperado o deseable en cualquier circunstancias* (por ejemplo: al cruzar la calle ¿estamos 100% seguros que nada nos pasará?).

### **II.3.- Tipos comunes de ataques en Internet**

Internet es conocido como el medio ideal para los hackers, mediante el cual pueden realizar ataques por ejemplo de negación de servicio desde cualquier parte del mundo. Más del 75 por ciento de las empresas sufren anualmente algún tipo de evento relacionado con la seguridad. Las fuentes de estos ataques pueden ser externos (Internet), como internos cuya fuente es la red corporativa de la empresa.

Entre los principales tipos de ataques tenemos:

**3.1- IP Spoofing:** Se basa en modificar el campo de dirección origen de los paquetes IP, por otra que queramos suplantar. Dado que los routers trabajan con base en tablas de direcciones IP, es necesario que el paquete utilice un campo opcional del encabezado denominado Source Routing.

Dicho campo le especificará a los routers que no utilicen sus tablas de enrutamiento, sino que obedezcan la ruta especificada en dicho campo.

**3.2- Ping flood:** Este ataque, también llamado “pitufu” o smurf, se basa en enviar un comando ping (petición de eco) a un grupo de equipos usando una dirección grupal o broadcast, pero sustituyendo la dirección IP real con la dirección IP de la máquina víctima. Lo que sucede entonces es que todas las máquinas que están en ese grupo le responden el ping (echo reply) a la máquina víctima, saturándola de tráfico y provocando posiblemente que se caiga o por lo menos que se degrade su tiempo de respuesta.

**3.3- Ping de la muerte:** Dado que el máximo tamaño especificado para el mensaje en el que viaja un ping es de 65 mil 535 bytes, muchos equipos y dispositivos tienen problemas para ensamblar un mensaje de mayor tamaño, causando en algunos casos una caída del sistema (denial of service).

**3.4- Syn flood (inundación de SYNs):** El equipo del atacante trata de iniciar una conexión con el equipo víctima, pero no termina el proceso sino que repite la misma petición muchísimas veces. Como para cada petición la máquina víctima asigna un área de memoria (buffers para la conexión), es frecuente que después de diversos inicios de conexión se tenga una conexión de buffer o memory overflow, lo que puede ocasionar la caída del equipo (negación del servicio). El nombre del ataque proviene de que la bandera de sincronización (SYN) se ocupa para indicar un inicio de conexión. Existen diversas variantes de este ataque.

**3.5- Land Attack:** Este ataque se basa en poner la misma dirección (vía IP spoofing) de origen y destino. Muchos equipos al ver un paquete de esas características, entran en un ciclo infinito (loop) hasta que se cae el sistema.

**3.6- Teardrop:** Se basa en el envío de un mensaje TCP en diversos paquetes que se traslapan. Algunos sistemas operativos tienen problemas para reensamblar paquetes traslapados, ocasionando caídas.

**3.7- TCP hijacking (secuestro de conexiones TCP):** Este ataque fue realizado probablemente por primera vez por Kevin Mitnick en contra de los equipos de T. Shimomura, conocido experto en seguridad. Consiste en romper una conexión TCP entre dos computadoras que ya han realizado su proceso de autenticación, y tratar de reestablecer la comunicación con una de ellas, simulando ser la otra. El ataque es complicado puesto que se tiene que “poner a dormir” a un equipo, hacer IP spoofing de su dirección, y tratar de adivinar el número de secuencia de los mensajes TCP para que el equipo al que se quiere entrar no se percate del ataque.

**3.8- Sniffers de passwords (husmeadores):** Este no es un ataque activo como los demás. Aquí se trata de “sembrar” en algún equipo, un programa que cuando se ejecute, actúe como la primera interfaz entre el usuario y el sistema operativo. De esta forma, cuando el usuario se autentique e introduzca su nombre y password, realmente el programa ante quien se autentifica no es el sistema operativo, sino el husmeador de passwords. El mismo, para no ser detectado, envía dicha información al sistema operativo para que el usuario pueda entrar, al mismo tiempo que graba en un archivo, el nombre y password del usuario.

**3.9- DDoS attacks (Ataques distribuidos de negación de servicio):** Los ataques de Denial Of Service Distribuidos (DDoS) son variantes de algunos de los ataques de negación de servicio como el smurf pero que surgen de diversas máquinas atacantes. Para que se pueda ejecutar, el atacante ha “sembrado” previamente programas maliciosos en decenas o cientos de equipos. Todos estos equipos en una fecha determinada o ante instrucciones específicas del atacante, realizarán algún ataque de negación de servicio. Algunas de las variantes más conocidas son: Trin00, TFN (tribe flood network), TFN2K, Stacheldraht (barbed wire) y mstream.

En todos estos tipos de ataques lo que se persigue, es causar el daño a la empresa y a sus activos informáticos y a la información como tal. Estos atacantes son denominados de muchas formas y con distintos calificativos por ejemplo: hacker y varias palabras para referirse a los distintos tipos de ciberpiratas (hackers si no tienen motivos criminales, crackers si los tienen, phreaks si son especialistas en “jugar” con la infraestructura telefónica, etcétera), lo cierto es que si el objetivo de la seguridad en primera instancia es protegernos como empresa o persona de ellos.

Es importante entender las distintas formas de ataque para prevenirnos de ellas adecuadamente. Y aunque no se puede citar en este trabajo de grado, todas las diferentes técnicas y métodos (o sus variantes) que usan los hackers para atacar, se mencionan algunos de sus ataques más comunes.

**3.10- Ingeniería Social:** Esta técnica, conocida como “ingeniería social”, es la utilización de preguntas inteligentes hechas en forma amable a las personas adecuadas, haciéndose pasar por otra persona para obtener algún tipo de información.



**3.11- Escaneo de Redes:** Existen muchas herramientas de dominio público que permiten con una conexión de Internet, analizar nuestra red y dar información valiosa (direcciones de servidores, servicios que prestan, configuración de los mismos, etcétera). Entre estas herramientas se encuentran el famoso comando utilitario ping (que hace pings por rangos) y traceroute (para saber por dónde pasan los paquetes y así “descubrir” los routers de la red). También existen otros comandos más poderosos, o un sinfín de utilerías no comerciales y otras costosas. Unos son bien conocidos como Sniffer de Red, el Iris, Retina, Network Inspector, etc.

**3.12- Hurto de Passwords.** Existen también muchas herramientas de dominio público para averiguar passwords. Una vez que se conoce el tipo de equipo que tenemos, es más factible realizar este tipo de ataque y entrar a nuestros equipos incluso con claves “privilegiadas”. Normalmente estas herramientas se basan en la copia del password file, aunque existen variantes que incluso pueden interceptar dichos passwords cuando viajan en la red (sobre todo en la LAN de nuestra empresa).

**3.13- Detectar “huecos” de seguridad (vulnerabilidades) en sistemas operativos y servicios que se están ejecutando en las máquinas.** En Internet existen “bibliotecas” completas que relacionan todos los huecos de seguridad para un ambiente en particular e incluyen los programas (exploits) que explotan dichos huecos. Si no hemos instalado todas las actualizaciones y “parches” de seguridad sobre nuestros equipos, los hackers pueden tomar ventaja de esos huecos y entrar fácilmente a ellos. Algunos de los sitios más visitados para enterarse de dichos huecos y sus respectivos exploits son: [www.rootshell.com](http://www.rootshell.com) y [www.antonline.com](http://www.antonline.com), aunque también es muy útil acudir a [noticias@hispasec.com](mailto:noticias@hispasec.com).

Otra variante de ataques comunes es aprovecharse de páginas Web (código HTML) con diferentes huecos de seguridad. Una de las maneras comunes de penetrar un sistema o por lo menos inhabilitarlo, es realizando algunos trucos en las formas HTML. Por ejemplo, es común que el programador que definió una forma HTML no se asegure que la información que el usuario ha escrito para llenar en un campo, no incluya caracteres especiales o esté fuera de especificaciones. ¿La consecuencia? Un atacante puede introducir información inválida y ocasionar que se caiga el servidor (debido a un buffer overflow).

En algunos casos la explotación de este tipo de huecos puede incluso darle acceso privilegiado (root o administrador) al atacante.

## **II.4.- Firewall**

**4.1- Concepto de Firewall:** Un firewall es un dispositivo que funciona como barrera defensiva entre redes, permitiendo las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local e Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el Web, smtp, ftp.

Un firewall actúa entre los niveles 3 (red) a 7 (aplicación) de OSI.

Sus funciones son básicamente las siguientes:

- Llevar contabilidad de las transacciones realizadas en la red.

- Filtrar accesos no autorizados a máquinas (mediante filtrado de paquetes, o bien observando el contenido de las unidades de protocolo de transporte, sesión, presentación y aplicación).
- Alertar en caso de ataques o comportamiento extraño de los sistemas de comunicación.

## **4.2- Tipos de Firewall**

Básicamente existen 3 tipos de firewall con características y funciones claramente definidas:

### **4.2.1- Packet Filter**

Filtran tráfico en base a características del paquete como direcciones de origen y destino, y puertos de origen y destino, número de protocolos, Flag TCP ACK. Trabajan a nivel de capas de enlace, red y de transporte del modelo OSI. Estos firewalls no incorporan esquemas de autenticación. Básicamente este tipo de firewall se pueden implantar utilizando routers sencillos, por lo tanto son básicos y son fácilmente atacables utilizando IP Spoof.

### **4.2.2- Application-Level Gateways**

Filtran tráfico a nivel de aplicación, debe existir por lo tanto un application-level gateway para cada protocolo y servicio que se desea filtrar (FTP, HTTP, SMTP, etc). Este tipo de firewalls no utilizan reglas de control de acceso pero en cambio aplican restricciones para garantizar la integridad de la conexión (filtran comandos y estructuras incorrectas o no aprobadas de para un protocolo o servicio específico).

### **4.2.3- Proxy Circuit-Level Gateways**

Estos tipos de firewall implementan el concepto de circuitos virtuales a través de redes que son separadas de manera lógica por el dispositivo. Para establecer una conexión entre ambas redes el cliente debe conectarse al dispositivo, quien a su vez se conecta con el servidor en la otra red (cliente y servidor nunca interactúan de manera directa). Los conceptos de NAT (“Network Address Translation”) y Masquerading son aplicados por estos dispositivos para mantener una relación entre conexiones de las distintas redes a través de los circuitos virtuales.

Básicamente actúan como proxy, y son implementados en la capa 7 del modelo OSI, y típicamente son más lentos que los firewall Packet Filter.

Actualmente además de los tres tipos de firewall básicos, también existen dispositivos con capacidades más avanzadas que les permiten ir mas lejos en el control del trafico y paquetes que circulan por sus interfaces:

### **4.2.4- Stateful Packet Inspection**

Este tipo de firewall se caracterizan porque examinan los paquetes IP y pueden dejarlos pasar o descartarlos según las reglas programadas, ya que mantienen siempre una tabla de estado de todas las sesiones. Cada nueva comunicación es examinada y se le asigna un estado en la tabla de sesiones. El lleva el control de todas las comunicaciones activas en todo momento controlando e inspeccionando todo el flujo del tráfico. La tecnología de tablas de estado permite un escrutinio más preciso del tráfico en los firewalls que lo implementan, al poder dar seguimiento a las diferentes conexiones que pasan por el firewall.

Típicamente se almacena información como:

- Actividad de la conexión (por ejemplo: inactiva, activa o en proceso de cierre).
- Características de identificación del paquete (dir. de origen y destino, puertos de origen y destino, protocolo, no. de secuencia, etc.).
- Origen de solicitud de inicio de la conexión.
- Dirección actual de la transmisión de paquetes.

#### **4.2.5- Deep Packet Inspection**

Este tipo de firewall se caracteriza por realizar análisis del tráfico en las cabeceras IP entre las capas 3 y 4 del modelos OSI, puede detectar ataques forjados y puertos abiertos. La elección del tipo de firewall adecuado depende de las necesidades de seguridad de cada empresa u organización pero típicamente se puede clasificar su uso de la siguiente manera:

- Filtrado perimetral entre redes con diferentes niveles de confianza y separación de redes: *packet filters* y *circuit-level gateway*
- Filtrado general a nivel de ruteo: *packet filters* (los routers son dispositivos que pueden considerarse *packet filters*).
- Filtrado específico para acceso a servicios públicos (servicios proporcionados por servidores en zonas desmilitarizadas como son HTTP, SMTP, FTP, etc.) y control de acceso a servicios críticos en zonas de seguridad internas (por ejemplo acceso a bases de datos corporativas en la red local).

*Application level gateways* no se puede considerar que un tipo de firewall sea mejor que otro, ya que cada uno posee funciones específicas.

La combinación de los 3 tipos de firewall mas las características *Stateful Packet Inspection* y *Deep Packet Inspection*, en una arquitectura de seguridad ofrece el mayor nivel de seguridad posible.

Es importante recordar que los productos de firewall existentes hoy en día suelen combinar características *Stateful Packet Inspection* y *Deep Packet Inspection* e incluso todas las características en un solo producto. El utilizar un solo producto que combina diferentes tipos de firewall tiene el inconveniente de generar un punto único de fallo pero es aceptable para la mayoría de las configuraciones, si se realizan configuraciones en cluster de alta disponibilidad con tolerancia a fallos.

#### **4.3- Firewalls integrados con hardware (“appliance”) vs. Firewalls basados en software**

La elección de uno u otro dependerá del caso específico y del análisis que haya realizado cada organización o empresa.

A continuación se comparan algunas características de ambos tipos de firewalls que pueden ser útiles en la selección de alguno de ellos:

	<b>Firewall integrado con Hardware (“Appliance”)</b>	<b>Firewall basado en software</b>
<b>Tipo de Instalación</b>	Estos dispositivos están listos para conectarse y configurarse tan pronto como salen de la caja. Requieren menor tiempo de puesta en producción, aunque este campo es muy variable y depende de muchos factores.	Requiere un tiempo variable: se necesita instalar el sistema operativo, configurarlo, instalar “drivers” de dispositivos de hardware y finalmente instalar el software de firewall antes de iniciar la configuración.
<b>Escalabilidad</b>	Estos dispositivos incluyen hardware y un sistema operativo extensivamente probado y adecuado por el fabricante para garantizar un correcto desempeño y compatibilidad.	Es necesario configurar manualmente dispositivos y sistema operativo para garantizar un desempeño adecuado. Se requiere efectuar también de un reforzamiento de la seguridad a nivel sistema operativo, es decir, un proceso de hardening para garantizar que el sistema operativo no presente

		potenciales huecos de seguridad.
<b>Flexibilidad en configuración de hardware y sistema operativo</b>	Las opciones de configuración en hardware y sistema operativo subyacente están limitadas por el fabricante para garantizar estabilidad y seguridad.	Existe mayor libertad para modificar la configuración de hardware y sistema operativo en caso necesario.
<b>Poder de procesamiento</b>	Generalmente estos dispositivos utilizan ASIC( circuitos integrados de aplicaciones específicas) por lo tanto son muchos más rápidos y eficientes.	Su velocidad de procesamiento esta limitada por los servicios o sistemas que compartan el tiempo de CPU, del servidor donde se instale.

#### 4.4 - Zonas de Seguridad DMZ (Perímetros de Seguridad)

Un firewall con funciones de protección DMZ( zona desmilitarizada) es una solución efectiva para empresas que ofrecen a sus clientes la posibilidad de conectarse a su red

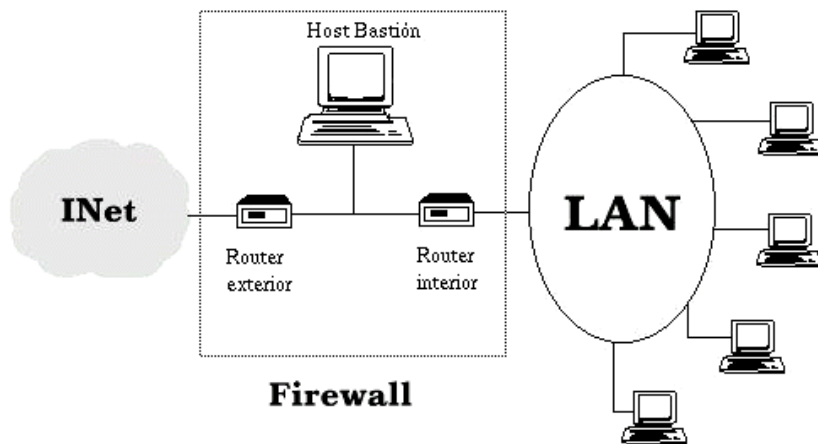


a partir de cualquier medio externo, ya sea a través de Internet, enlaces dedicados DPL( enlaces privados digitales), Frame Relay o cualquier otra ruta. La decisión de optar por un firewall con DMZ debe basarse en la cantidad de usuarios externos que acceden a la red y la frecuencia con la que lo hacen, cantidad de sistemas que acceden.

La tendencia actual en referencia a la implantación de sólidos esquemas de seguridad, tiene como norte la arquitectura DMZ, también conocida como red perimétrica o *De-Militarized Zone* (DMZ) es con diferencia la más utilizada e implantada hoy en día en una gran cantidad de empresas, ya que añade un nivel de seguridad en las arquitecturas de firewall situando una subred (DMZ) entre las redes externa e interna, de forma que se consiguen reducir los efectos de un ataque exitoso al *host* bastión, o servidores corporativos. Como es bien conocido por la mayoría de los profesionales del área de seguridad, en los modelos anteriores toda la seguridad se centraba en el bastión, de forma que si la seguridad del mismo se veía comprometida, la amenaza se extendía automáticamente al resto de la red. Como la máquina bastión es un objetivo interesante para muchos piratas, la arquitectura DMZ intenta aislarla en una red perimetral de forma que un intruso que accede a esta máquina no consiga un acceso total a las subredes protegidas.

Las DMZ es la arquitectura más segura, pero también la más compleja; en su implantación básica se utilizan dos *routers*, denominados exterior e interior, conectados ambos a la red perimétrica como se muestra en la figura. En esta red perimetral, que constituye el sistema firewall, se incluye el *host* bastión y también se podrían incluir sistemas que requieran un acceso controlado, como arreglos de módems o el servidor de correo, que serán los únicos elementos visibles desde fuera de la red.

El *router* exterior tiene como misión bloquear el tráfico no deseado en ambos sentidos (hacia la red perimétrica y hacia la red externa), mientras que el interior hace lo mismo pero con el tráfico entre la red interna y la perimetral: así, un atacante habría de romper la seguridad de ambos *routers* para acceder a la red protegida; incluso es posible implementar una zona desmilitarizada con un único *router* que posea tres o más interfaces de red, pero en este caso si se compromete este único elemento se rompe toda nuestra seguridad, frente al caso general en que hay que comprometer ambos, tanto el externo como el interno. También podemos, necesitar mayores niveles de seguridad, para definir varias redes perimétricas en serie, situando los servicios que requieran de menor protección en las redes más externas: así, el atacante habrá de saltar por todas y cada una de ellas para acceder a los equipos.



Arquitectura básica de una DMZ.

Esta arquitectura de firewall elimina los puntos únicos de fallo presentes en las redes previas antes de llegar al bastión (por definición, el sistema más vulnerable) un atacante ha de saltarse las medidas de seguridad impuestas por el router externo. Si lo consigue, como hemos aislado la máquina bastión en una subred, estamos reduciendo el impacto de un atacante que logre controlarlo, ya que antes de llegar a la red interna también debe comprometer también al segundo *router*; en este caso extremo (si un pirata logra comprometer el segundo *router*). Actualmente estas arquitecturas se puede implantar en firewall con múltiples interfaces de seguridad. Aunque, como hemos dicho antes, la arquitectura DMZ es la de mayores niveles de seguridad pueden proporcionarnos, no se trata de la panacea de los cortafuegos, tampoco se puede decir que es un sistema 100% seguro.

#### **4.5- Desarrollo de las Zonas de Seguridad Perimetrales**

En la actualidad el desarrollo acelerado de tecnologías de redes, servicios asociados, y sistemas integrados, son unos de los elementos cada vez más vital para la gestión de negocio de cada empresa en la era de la economía digital. Las organizaciones dependen cada vez más del buen funcionamiento de los sistemas informáticos para la realización de su actividad diaria de negocio. Mantener operativa una red con niveles de seguridad más que aceptables los 365 días, es una tarea de vital importancia para cualquier empresa que quiera garantizar la operatividad de sus funciones. Las implicaciones de conseguir que una red distribuida geográficamente funcione sin problemas de seguridad, supone un reto aún mayor para el diseño de un esquema de zonas de seguridad sólido y eficiente. Últimamente se viene dedicando gran atención a los conceptos de zonas de seguridad DMZ aplicadas a servicios y redes distribuidas y heterogéneas.

#### **4.5.1- Importancia de las Zonas de Seguridad**

En los entornos empresariales actuales bien sean privadas o gubernamentales e independientemente de su objeto y condición, se hace necesaria la modernización desde el punto de vista informático, de su negocio mediante nuevas tecnologías, que la ayuden a ser mas eficientes en sus procesos.

Esta apertura empresarial digital está basada en la interconexión de sus sistemas de negocio informáticos con la Internet, con objeto de mantener un flujo constante de información con todos aquellos elementos necesarios para el desarrollo del área de negocio.

Esta necesidad de implantar barreras de protección se hace máxima debido a que un problema de seguridad puede afectar de forma directa el negocio de la empresa, y de forma indirecta la imagen corporativa sobre la que está basada la confianza de los clientes. Niveles de seguridad perimetrales adecuados permitirán a las empresas desarrollar su negocio en toda su extensión en forma confiable y controlada, evitando que determinados incidentes afecten de forma drástica la gestión de negocio de la empresa.

#### **4.6-. Firewall Basados en ASIC (Circuitos Integrados de Aplicaciones Especificas), para implementar DMZ**

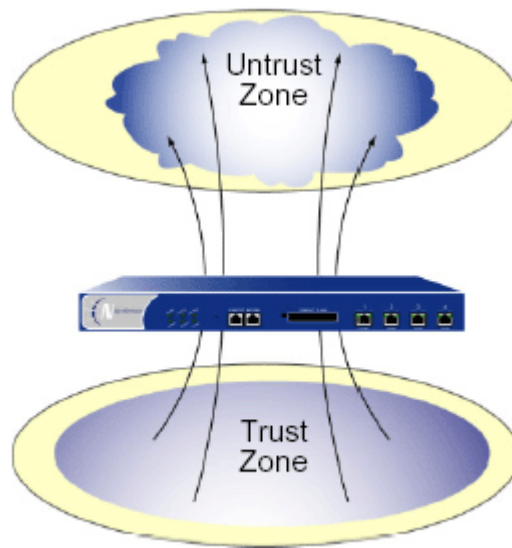
Los fabricantes de equipos de comunicaciones hacen uso de ASIC, para combinar una gran cantidad de funciones lógicas en un dispositivo, Sin embargo estos dispositivos tienen un costo inicial alto, por lo tanto se usan principalmente cuando es

necesario una gran cantidad de procesamiento de datos y se requiere un rendimiento con categoría carrier class.

La aplicación de ASIC para la construcción de zonas de seguridad DMZ en los firewall, utilizando interfaces físicas, es una solución muy flexible que brinda gran capacidad y velocidad de procesamiento y elevados niveles de seguridad. En el interior del dispositivo, se crea una subred virtual (en el sentido clásico del término) con determinadas “Zonas de Seguridad” interconectadas entre sí mediante una serie de routers virtuales.

Las zonas de seguridad están asociadas a los distintos segmentos presentes en la red. En una red típica éstas podrían corresponderse respectivamente con los segmentos dedicados a las estaciones de trabajo, a los servidores internos y a los servidores desmilitarizados (DMZ). En esta figura que se muestra a manera de ejemplo, se deberían definir en el dispositivo cuatro zonas de seguridad, una por cada segmento de red, y la cuarta correspondiente al enlace a la red insegura (untrust), que es generalmente Internet.

En la terminología usada en la solución implantada en la empresa, se puede definir una zona de seguridad como una colección de una o más segmentos de red, que requieren regulación del tráfico entrante y saliente utilizando para ellos políticas de acceso. Una zona de seguridad es una entidad lógica la cual tiene una o más interfaces.



#### 4.6.1- Routers Virtuales

Los routers virtuales son instancias lógicas con funcionalidad equivalente a sus homónimos reales: implementan las funciones de enrutado entre las diferentes zonas de seguridad. Así mismo, los routers virtuales son los que realizan la actividad de filtrado de paquetes entre las distintas zonas. Cada zona de seguridad tiene asociado un router virtual, y todos ellos se interconectan en una zona de seguridad especial denominada zona global.

La correspondencia entre zonas de seguridad e interfaces de red no se realiza directamente, sino mediante unas interfaces virtuales asociadas a alguna interfaz física. De esta forma resulta posible, entre otras cosas, definir más zonas de seguridad que interfaces presentes en el dispositivo, claro esto no aplica a todos los dispositivos de seguridad firewall, esta función depende del modelo.

#### 4.6.2- Interfaces

Las interfaces de las zonas permite la comunicación de todo el tráfico TCP/IP que pasas de una zona a otra. A través de las políticas se puede definir que tráfico es permitido entre las zona, bien sea en una dirección o bi-direccional. Las tablas de enrutamiento definen el camino que debe seguir el tráfico desde una interfaz a otra.

Es la interfaz física que esta presente en el dispositivo propiamente dicho, la solución implantada en la organización, las interfaces físicas están definidas por la posición en los módulos de las interfaces y en el puerto Ethernet del modulo. En el siguiente gráfico, se muestran las interfaces disponibles en el firewall.

Su orden seria el siguiente: Ethernet 1/1, Ethernet 1/2, Ethernet 2/1, Ethernet 2/2. La Ethernet 1/2 se interpretaría así: primer modulo 1 y segundo puerto 2.



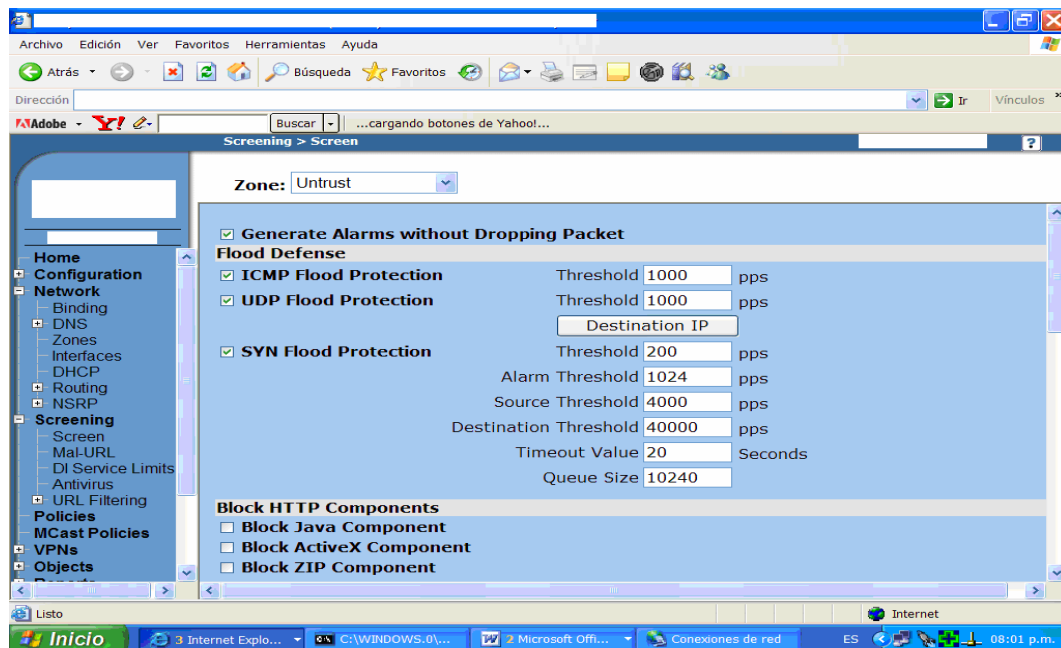
En los dispositivos que soporten VLAN(LAN Virtuales), se pueden dividir las interfaces físicas en interfaces virtuales (Subinterfaces), donde una de estas subinterfaces toma prestada su porción de ancho de banda que necesita de la interfaz física. Estas subinterfaces de forma abstracta funcionan idénticamente igual que una interfaz física definida con el 802.1Q VLAN tagging.

### 4.6.3- Políticas

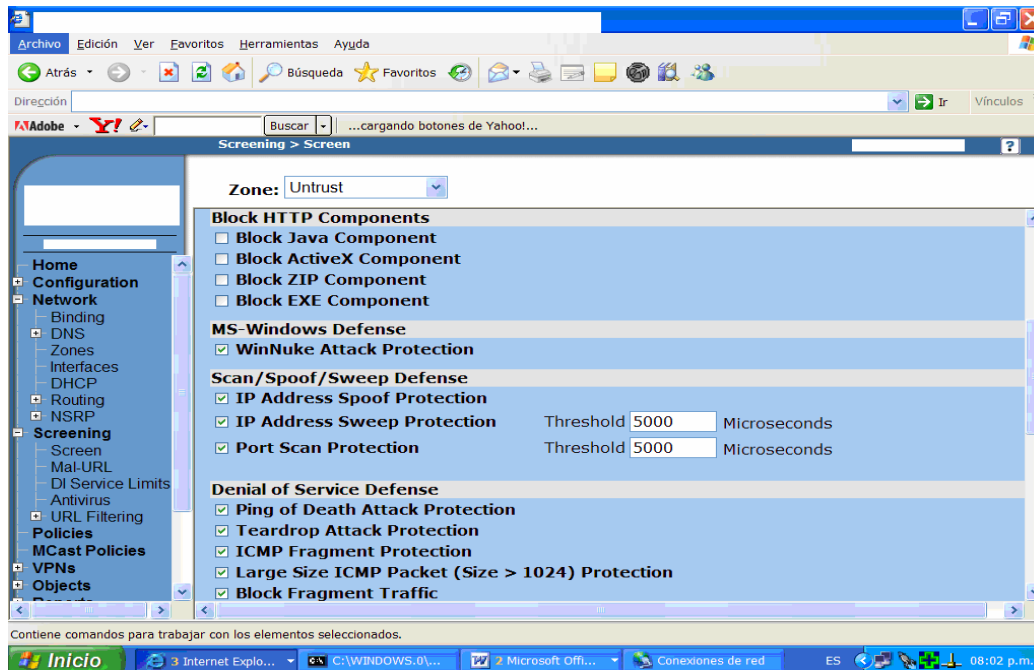
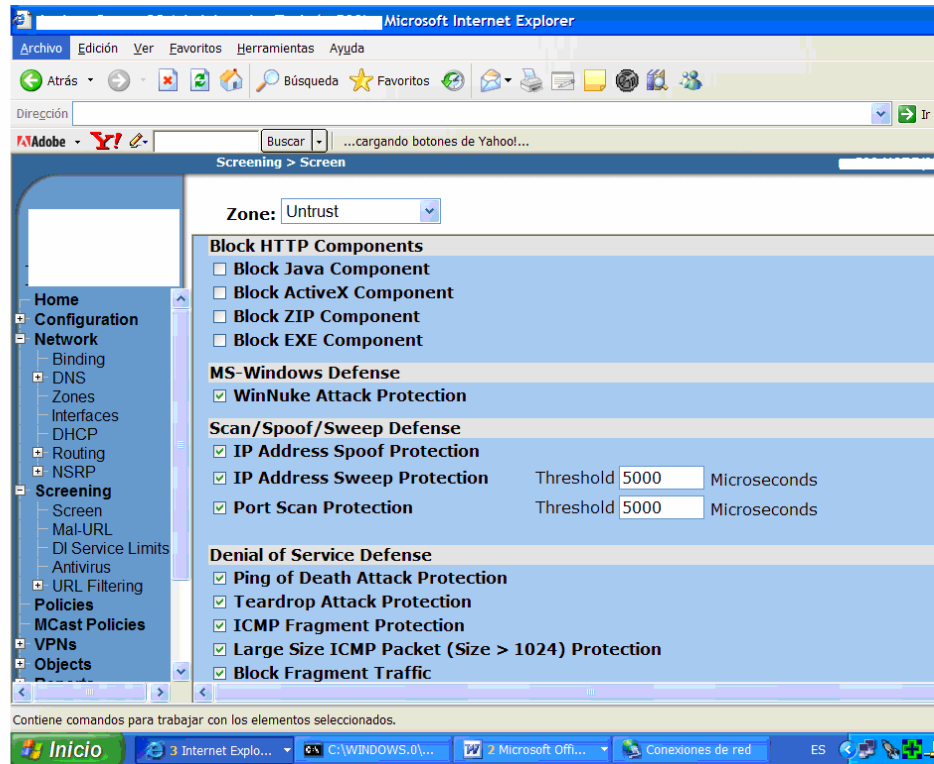
Los Firewall protegen las redes que están detrás de ellos, inspeccionando los paquetes entrantes y salientes a cada zona, y por ende permitiendo o bloqueando el tráfico según la política configurada. Por defecto estos dispositivos no dejan pasar todo el tráfico en todas las direcciones como punto inicial, entonces a través de la creación de políticas, se puede controlar el tráfico que cruza de una zona a otra zona, o también desde dos interfaces distintas asociadas a una misma zona.

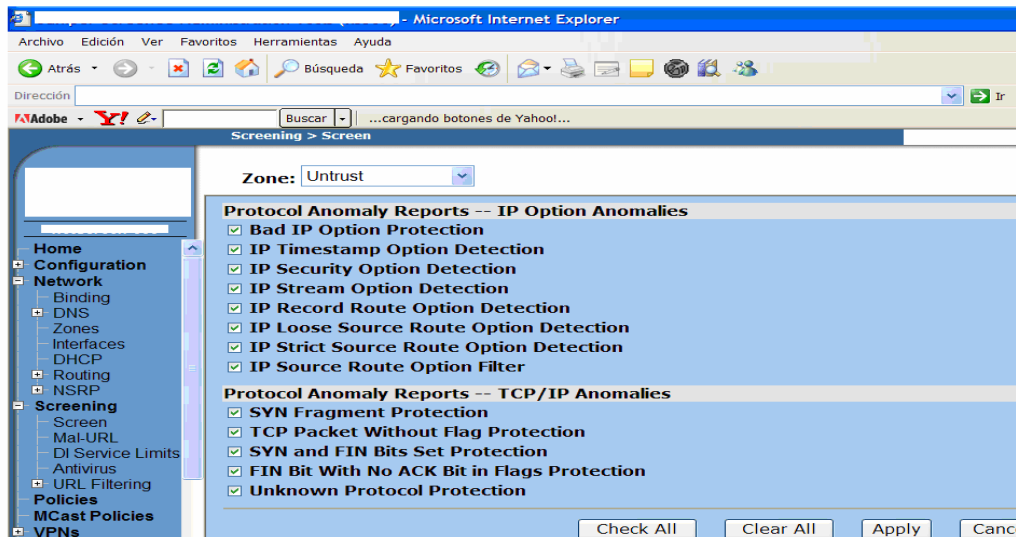
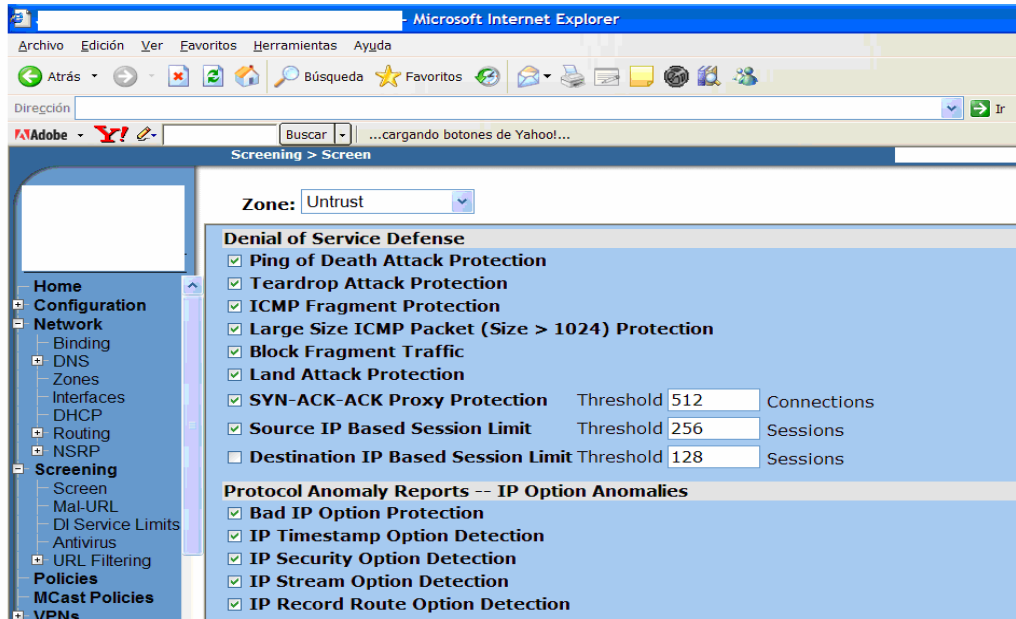
### 4.6.4- Plantillas de Protección Contra Ataques Comunes

La tecnología de firewall, utilizada en este proyecto tiene la ventaja de permitir realizar configuraciones rápidas y sencillas pero muy potentes, mediante las cuales se puede proteger la red de la empresa de los ataques de negación de servicio. En las siguientes pantallas se puede apreciar las plantillas de configuración, mediante las cuales se pueden activar los parámetros de protección por zonas específicas.









#### 4.7- VPN (Redes Privadas Virtuales)

Con este concepto lo que se persigue es simular una red privada sobre una red pública, por ejemplo, Internet. Como se muestra en la figura siguiente, la idea es que la red pública sea vista desde dentro de la red privada como un túnel lógico que une las dos o más redes que pertenecen a la red privada. Es decir una red privada que se extiende, mediante unas técnicas de encapsulación y encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte (Internet). Los paquetes de datos de la red privada viajan por medio de un “túnel” definido en la red pública. En las siguientes figuras se pueden ver ejemplo de VPN.

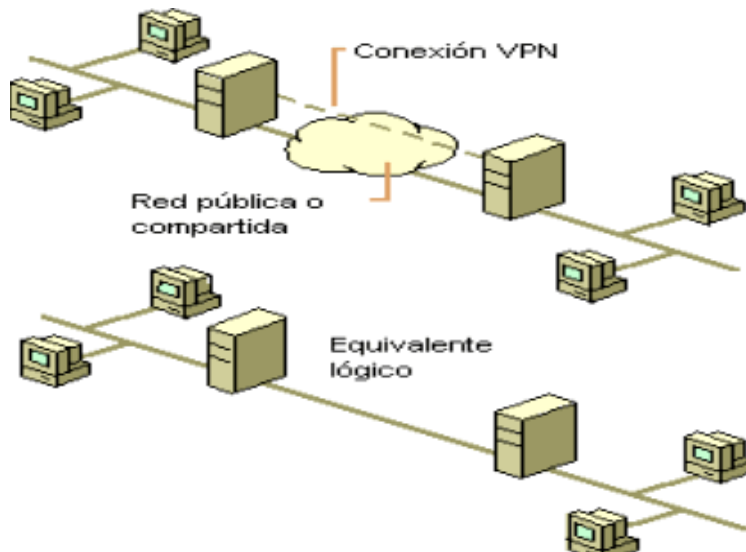


Figura 1

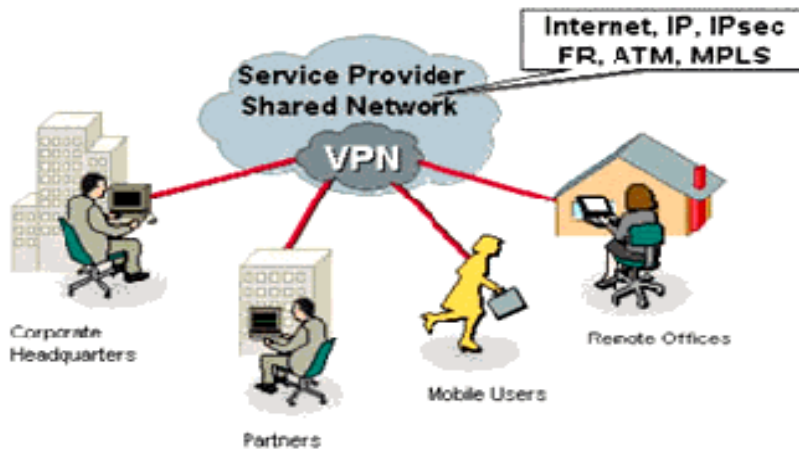


Figura 2

En la figura anterior (figura 2), se muestran como viajan los datos a través de una VPN:

- a) Desde un servidor dedicado los datos parten, llegando a un firewall que hace la función de una pared para detener a los intrusos.
- b) Después los datos llegan a nube de Internet donde se genera un túnel dedicado únicamente para los datos, es decir se genera un túnel desde el firewall de la derecha hacia el firewall de la izquierda, esto para garantizar la confidencialidad de la información.
- c) Luego estos datos son entregados al cliente remoto, en texto plano es decir los datos ya están en su estado nativo sin encriptar, una vez establecido el túnel, la información viaja de en forma bi-direccional.

Las VPN pueden enlazar oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas mediante los protocolos como, IP, Ipsec, Frame Relay, ATM, etc.

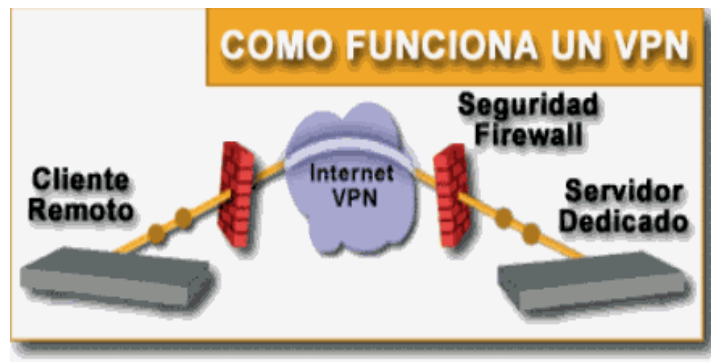


Figura 3

La tecnología de túneles (“tunneling”) es un modo de transferir datos en la que se encapsula un tipo de paquetes de datos dentro algún protocolo, no necesariamente diferente al del paquete original. Al llegar al destino, el paquete original es desempacutado volviendo así a su estado original. En el traslado a través de Internet, los paquetes viajan encriptados. La encriptación debe ser realizada en tiempo real. Por eso, los flujos a través de una red son encriptados utilizando mecanismos de clave secreta que son solamente buenas para sesiones de flujo.

#### 4.7.1- Aspectos Funcionales

Una buena implantación de Redes Privadas Virtuales debe brindar las siguientes características básicas.

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

En la actualidad las VPN más utilizadas se establecen mediante túneles IPsec:

#### 4.7.2- IPSec (IP Seguro, descrito en el RFC 2411)

Es un protocolo que sirve para establecer una sesión segura entre dos hosts que se comunican a través de IP, proporcionando encriptación a nivel de la capa de red. IPSec trata de remediar algunas carencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme. Las futuras implementaciones de IPv6, tendrá la ventaja de que la seguridad se gestiona de forma nativa, de manera muy similar a como se gestiona actualmente en IPSec. El mismo proporciona una base estable y duradera para proporcionar seguridad de capa de red y soporta todos los algoritmos criptográficos que se utilizan hoy en día y también puede ajustarse a algoritmos nuevos, más potentes que vayan surgiendo. El protocolo IPSec cubre las siguientes cuestiones de seguridad principales:

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

Los principales protocolos IPSec se listan a continuación:

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

#### **4.7.3- Protocolo AH - Authentication Header (Cabecera de Autenticación)**

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

AH asegura la integridad de los datos mediante la suma de comprobación que genera un código de autenticación de mensajes. Para asegurar la autenticación del origen de los datos, AH incluye una clave compartida secreta en el algoritmo que utiliza para la autenticación. Para asegurar la protección contra la reproducción, está maneja un campo de números de secuencia dentro de la cabecera AH. Es importante observar que a menudo estas tres funciones distintas se concentran y se conocen como “autenticación”. Es decir, que AH asegura que no se han manipulado los datos mientras se dirigían a su destino final.

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



#### **4.7.4- Tipos de Configuraciones AH**

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

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

Si en ambos extremos de una asociación de seguridad hay una pasarela, se utiliza la modalidad de túnel. En esta modalidad, las direcciones de origen y destino de la parte más externa de la cabecera IP no tienen necesariamente que ser iguales que las direcciones de la cabecera IP original. Por ejemplo, dos pasarelas de seguridad pueden operar un túnel AH para autenticar todo el tráfico entre las redes que conectan. De hecho, esta es una configuración muy habitual.

La principal ventaja de utilizar esta modalidad de túnel, es que la misma protege

totalmente el datagrama IP encapsulado. Además, la modalidad de túnel hace posible utilizar direcciones privadas.

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

#### **4.7.5- Protocolo ESP – Encapsulating Security Payload (Carga útil de Seguridad Encapsulada)**

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

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

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

#### **4.7.6- Tipos de Configuraciones ESP**

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

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

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

#### **4.7.7- Protocolo IKE (Internet Key Exchange)**

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

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

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

IKE es un protocolo híbrido que se obtuvo como resultado de la integración de dos protocolos complementarios: ISAKMP y Oakley. El primero de ellos define de forma genérica el protocolo de comunicación y la sintaxis de los mensajes que se utilizan en

IKE, mientras que el segundo especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente.

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

- **1 Fase:** Común a cualquier aplicación, en ella ambos establecen un canal seguro y autenticado. El canal seguro se consigue mediante el uso del algoritmo cifrado simétrico y un algoritmo HMAC. Las claves necesarias se derivan de una clave maestra obtenida mediante un algoritmo de intercambio de claves de Diffie-Hellman. Este procedimiento todavía no garantiza la identidad de los nodos, por eso es necesario añadir algún procedimiento de autenticación.
- **2 Fase:** Esta fase el canal seguro IKE es utilizado para negociar los parámetros de seguridad específicos asociados a un protocolo determinado, IPSec. Aquí se negocian las características de la conexión ESP o AH y todos los parámetros necesarios. El equipo que haya iniciado la comunicación ofrece todas las posibles opciones que tiene configuradas en su política de seguridad y sus prioridades correspondientes. El sistema receptor aceptará la primera que coincida con los parámetros de seguridad que tenga definidos. Además, ambos nodos se informan del tráfico que van a intercambiarse a través de dicha conexión.

## **4.8 - VPN Mediante Tecnología ASIC**

Los equipos de seguridad firewall utilizados en la presente solución, se pueden configurar de dos formas para establecer una VPN:

- Basadas en Políticas
- Basadas en Rutas

### **4.8.1- VPN (Basadas en Rutas)**

Utilizando un route lookup (consulta de la tabla de enrutamiento) el dispositivo puede determinar cuál tipo de tráfico debe ser encapsulado en una VPN. Si la política permite el tráfico y la ruta hace referencia a que se debe establecer un túnel con el tráfico entrante a la interfase, entonces los paquetes se encapsulan en un túnel VPN. En esta configuración se separa lo que es la aplicación de políticas de las aplicaciones de túneles VPN.

### **4.8.2- VPN (Basadas en Políticas)**

Una Policy lookup (consulta de la política), determina cuál tráfico debe ser encapsulado, es decir, cuando la política se ejecuta, entonces la acción a ejecutar es establecer el túnel VPN.

Las políticas basadas en rutas, son una buena elección para VPN de sitio a sitio, Aquí se pueden apreciar las pantallas básicas para las configuraciones de las VPN:

Microsoft Internet Explorer - VPNs > AutoKey IKE

Archivo Edición Ver Favoritos Herramientas Ayuda

Dirección: ...cargando botones de Yahoo!...

VPNs > AutoKey IKE

New

Name	Gateway	Security	Monitor	Configure
No entry available				

Toggle Menu

- Policies
- MCast Policies
- VPNs
  - AutoKey IKE
  - AutoKey Advanced
    - Gateway
    - P1 Proposal
    - P2 Proposal
    - XAuth Settings
    - VPN Groups
  - Manual Key
  - L2TP
  - Monitor Status
- Objects
- Reports
- Wizards
- Help
- Logout

Microsoft Internet Explorer - VPNs > AutoKey Advanced > Gateway

Archivo Edición Ver Favoritos Herramientas Ayuda

Dirección: ...cargando botones de Yahoo!...

VPNs > AutoKey Advanced > Gateway

New

Name	Type	Address/ID/User Group	Local ID	Security Level	Configure
No entry available					

- Antivirus
- URL Filtering
  - Protocol
- Policies
- MCast Policies
- VPNs
  - AutoKey IKE
  - AutoKey Advanced
    - Gateway
    - P1 Proposal
    - P2 Proposal
    - XAuth Settings
    - VPN Groups
  - Manual Key
  - L2TP
  - Monitor Status
- Objects
- Reports
- Wizards
- Help

#### **4.9- Alta Disponibilidad**

En la era de la información electrónica actual, existen ciertas aplicaciones que dada su naturaleza, deben proporcionar un servicio ininterrumpido de 24 horas al día y 7 días a la semana. Por ejemplo un servidor de base de datos corporativo o el portal de servicio de una empresa. Para conseguir estos niveles de disponibilidad se suele utilizar una configuración avanzada de hardware y de software denominada ***Cluster de Alta Disponibilidad***.

Se trata de un conjunto de dos o más máquinas, que se caracterizan porque comparten los discos de almacenamiento de datos, o sesiones activas, y que están constantemente monitoreándose entre sí. Si se produce un fallo del hardware o de las aplicaciones de alguna de las máquinas del cluster, el software de alta disponibilidad es capaz de reiniciar automáticamente los servicios que han fallado en cualquiera de las otras máquinas del cluster. Cuando la máquina que ha fallado se recupera, los servicios son nuevamente migrados a la máquina original. Esta capacidad de recuperación automática de servicios que garantice la integridad de la información y la continuidad de la comunicación ya que no hay pérdida de datos, además evita molestias a los usuarios, que no tienen por qué notar que se ha producido un problema.

No hay que confundir los clusters de alta disponibilidad con los ***clusters de alto rendimiento***. Un cluster de alto rendimiento, es una configuración de equipos diseñada para proporcionar capacidades de cálculo mucho mayores que la que proporcionan los equipos individuales, mientras que los clusters de alta disponibilidad están diseñados para garantizar el funcionamiento ininterrumpido de ciertas aplicaciones o sistemas.



#### **4.9.1- *Qué es la tolerancia a fallos***

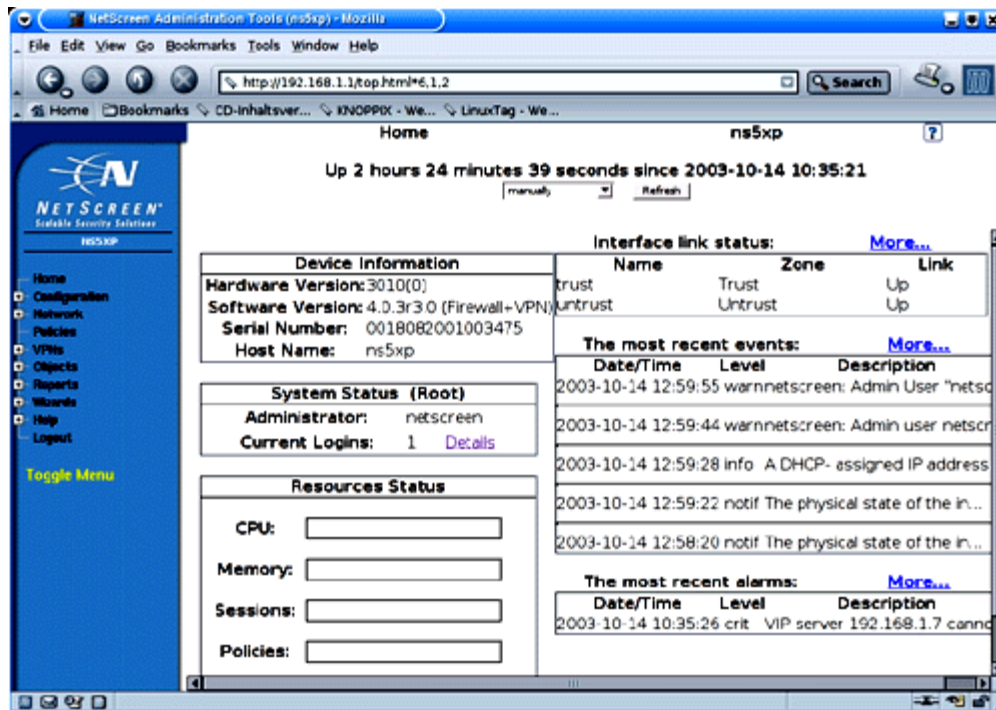
La tolerancia a fallos dota a los elementos que componen la plataforma de la capacidad de recuperarse ante los fallos de otros elementos con los que interactúan. Todo esto se traduce en, aunque falle algún elemento de la plataforma, los sistemas siguen funcionando sin ningún problema ya que; la falla será transparente para los sistemas y los usuarios.

#### **4.9.2- Cual es el objetivo de un proyecto de Alta Disponibilidad?**

- Eliminar las paradas planificadas debidas respaldos, actualizaciones de hardware y software, instalación de nuevos componentes y aplicaciones.
- Eliminar las paradas no planificadas debidas a caídas de componentes hardware como por ejemplo fallos de la CPU, corrupciones de disco, caídas de comunicaciones, etc... Las paradas no planificadas también incluyen los desastres, ya sean estos naturales (inundaciones, incendios) o no naturales (sabotajes, fallos humanos, etc.)

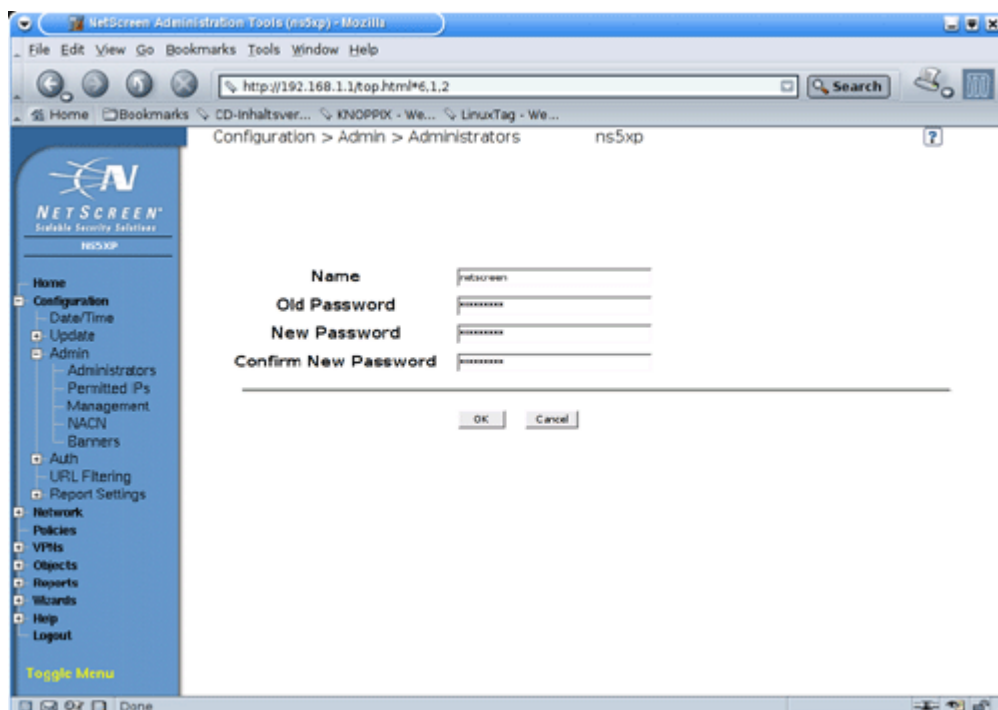
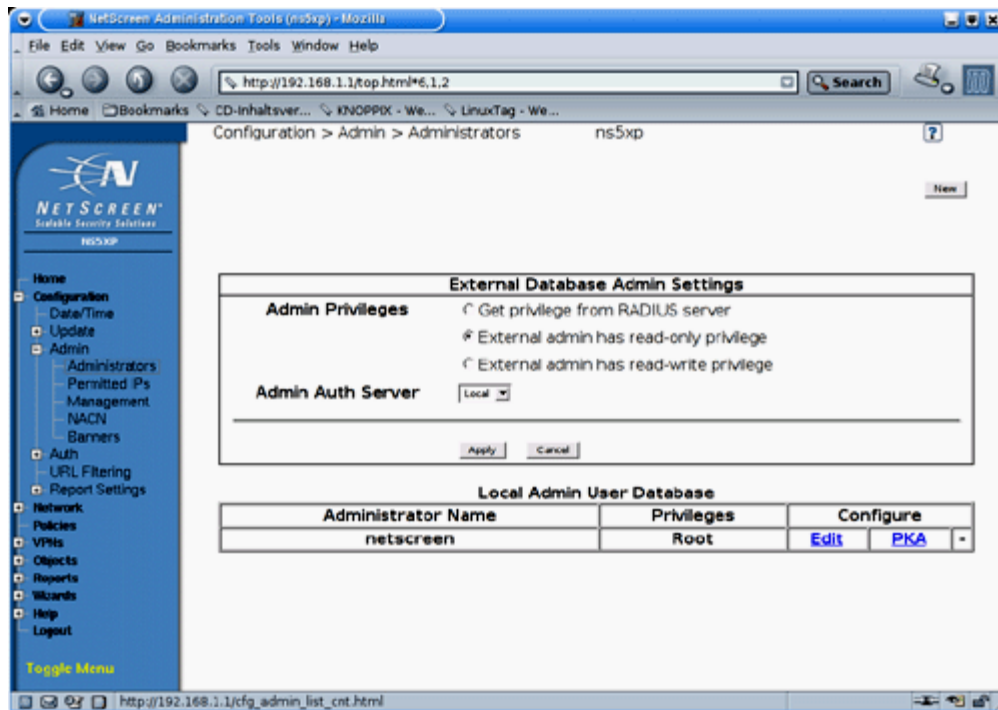
#### **4.10- Administración de los Firewall ASIC y Ejemplos de Configuración**

Los dispositivos (firewall) de la familia ASIC ofrecen dos mecanismos de configuración: mediante la interfaz Web o a través de un interfaz de línea de comandos accesible por puerto serie o, más fácilmente por red vía Telnet. En ambos casos se tiene acceso a todas las opciones de configuración del dispositivo.



La interfaz Web presenta las opciones de configuración convenientemente clasificadas, resultando muy sencillo navegar entre la enorme cantidad de parámetros correspondientes a una muy diversa funcionalidad.

Conviene aclarar en este punto que se disponen de diferentes perfiles de administración, pudiendo crearse varios usuarios administradores para realizar tareas específicas. La jerarquía entre administradores y las políticas de acceso al dispositivo pueden incluso proporcionarse mediante un servidor 'RADIUS' externo.

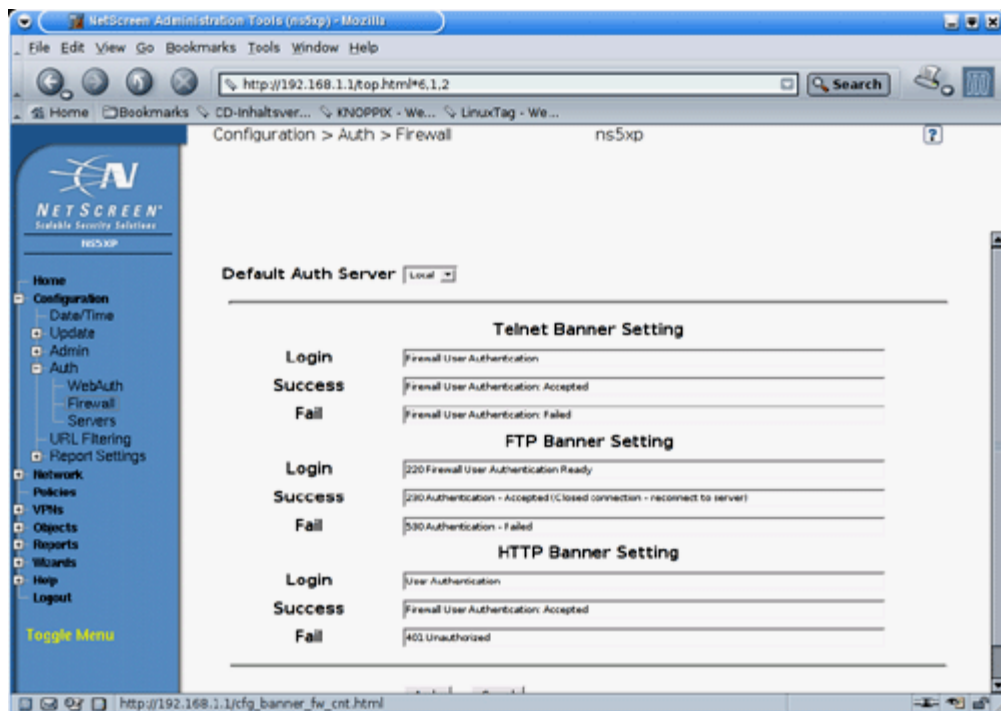


Aquí se pueden observar las opciones básicas de las políticas creadas, son las opciones de configuración más comúnmente utilizadas. También se puede utilizar el 'Incoming Policy Wizard' para crear políticas de manera mas sencilla, una vez que se dispone de la experticia requerida quizás no se utilice más esta facilidad. Se puede comprobar las reglas creadas en la opción 'Policies', donde se muestran todas las reglas de filtrado configuradas en el dispositivo.

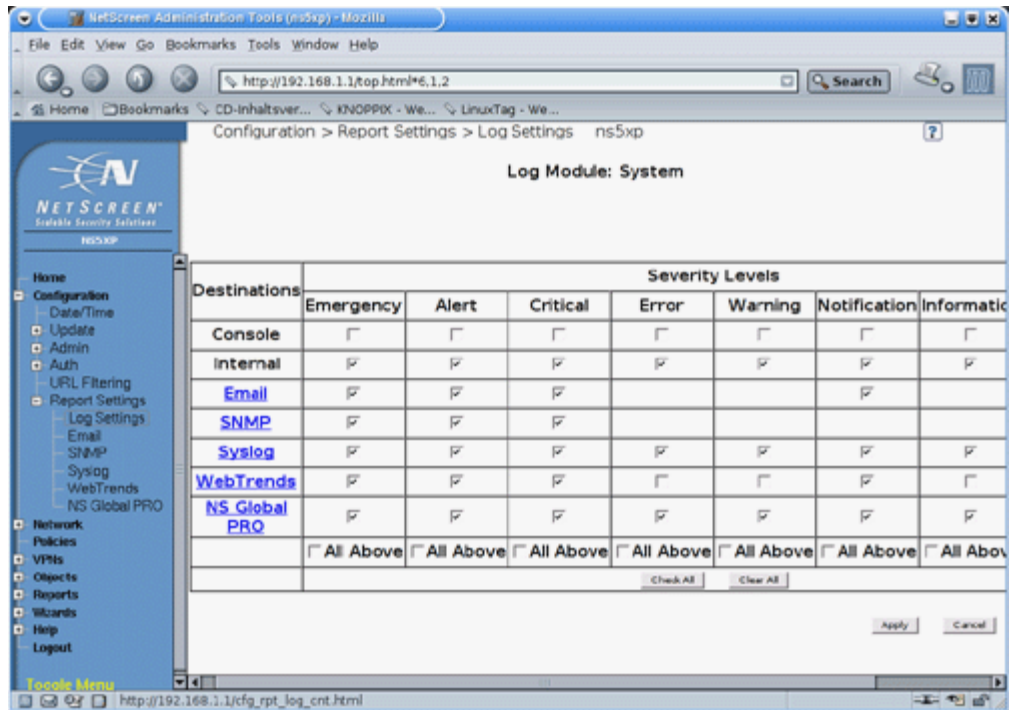


Desde esta página se puede añadir nuevas reglas y eliminar, modificar o copiar las existentes, aunque sin la facilidad aportada por el asistente. La edición manual de reglas de filtrado requiere algo de experiencia con el dispositivo.

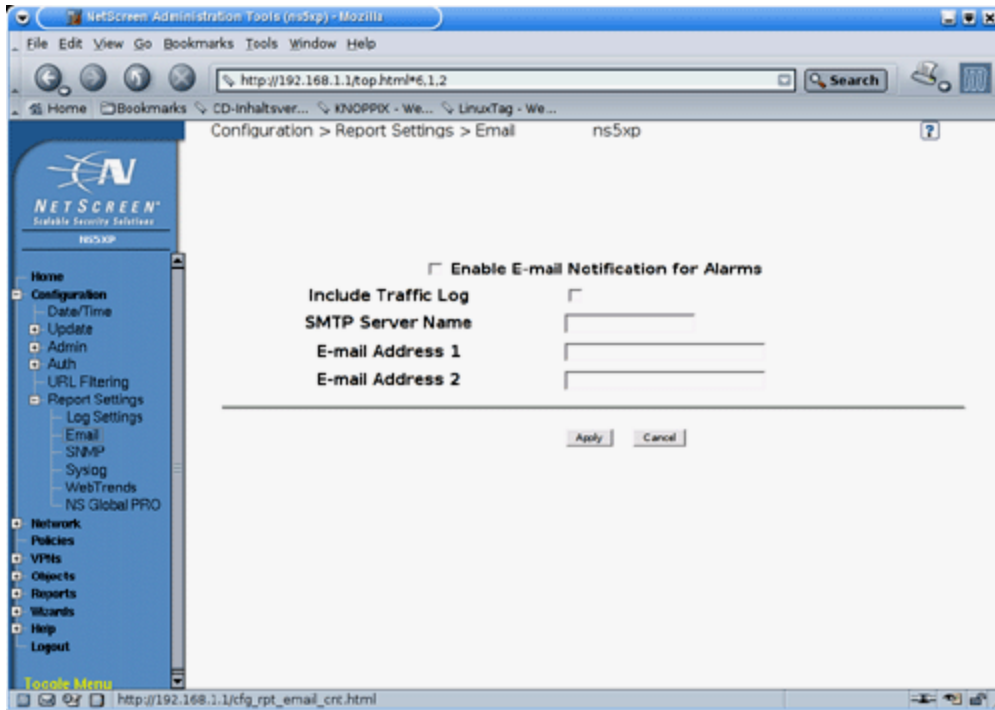
La tecnología de firewall seleccionada en la presente solución, permite modificar la cadena de texto que se muestra en diferentes etapas de la autenticación en cualquier de los servicios por los que se puede acceder al dispositivo. Esto es muy útil para dificultar la identificación del dispositivo firewall, esto es uno de los pasos iniciales antes de ejecutar un ataque a una red.



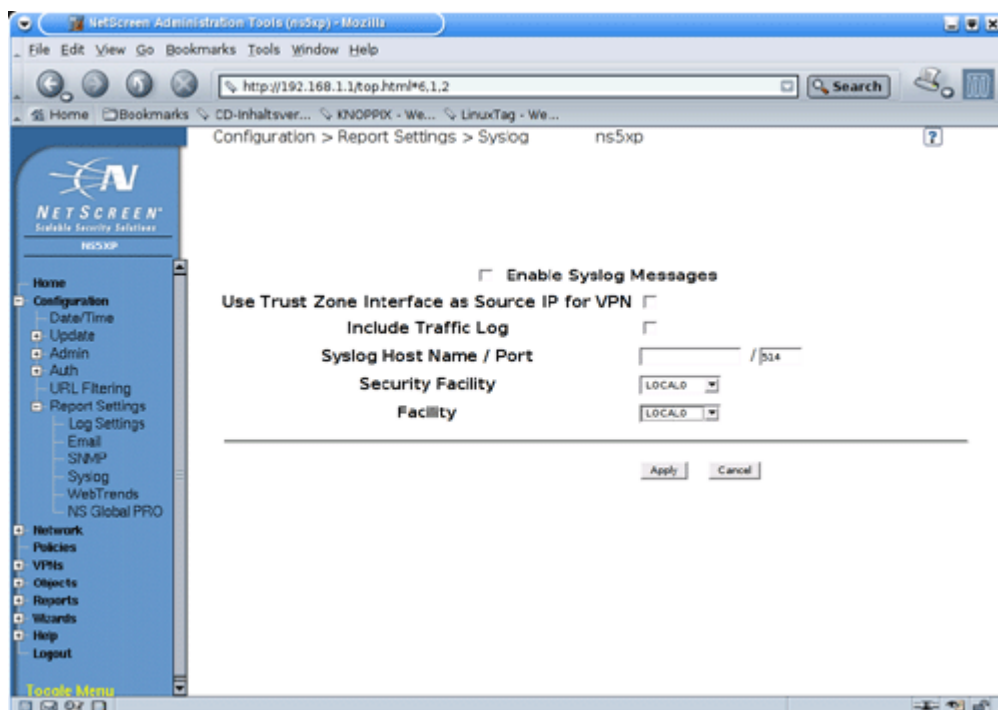
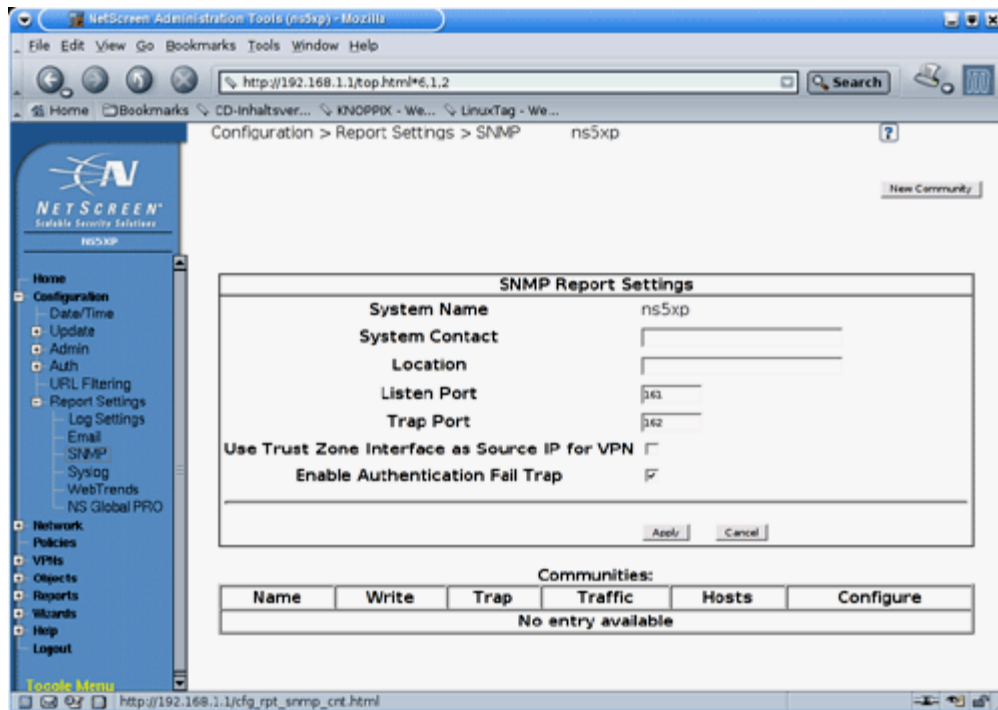
Las opciones para configurar el registro de eventos son muy completas, permitiendo enviar la información a servidores centralizados con diferentes protocolos de comunicación.



Además de los habituales mecanismos de registro de eventos locales, entre las posibilidades se prevé el envío de notificaciones especialmente urgentes por correo electrónico.

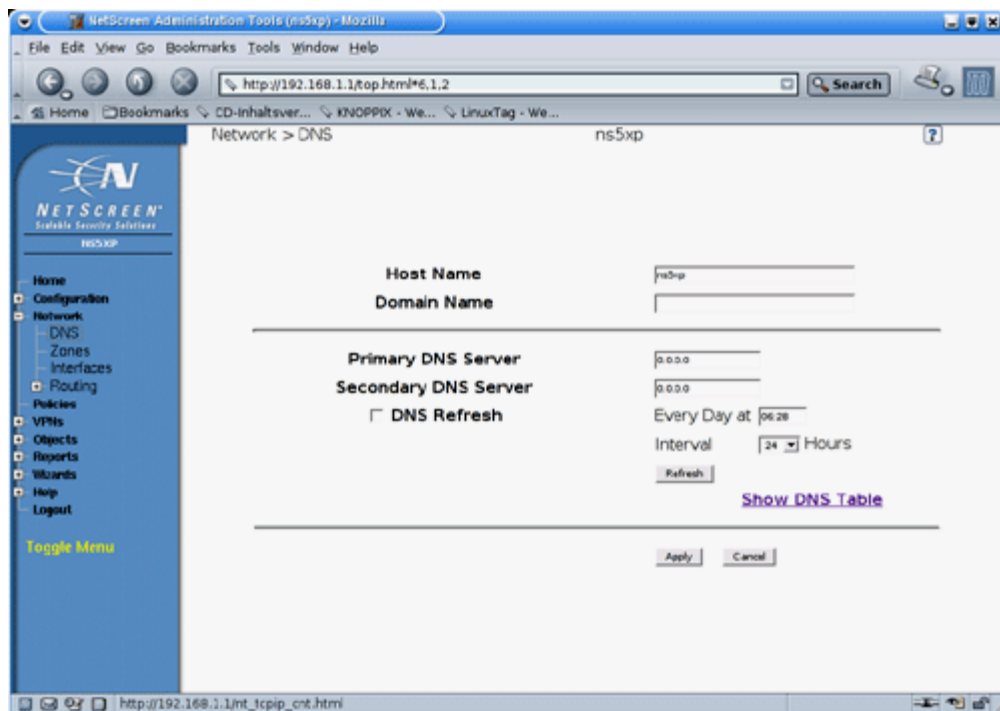


También se incluye, como es común, un soporte para el protocolo SNMP y el estándar “de facto” Syslog. Las herramientas syslog permiten recolectar de manera centralizada y sencilla, toda la información de tráfico, alarmas, eventos, y errores que generan los dispositivos, en este caso los firewall. Luego esta información se puede utilizar como insumo para futuros análisis y detección de tráfico anómalo, o para realizar trazas de auditoría.

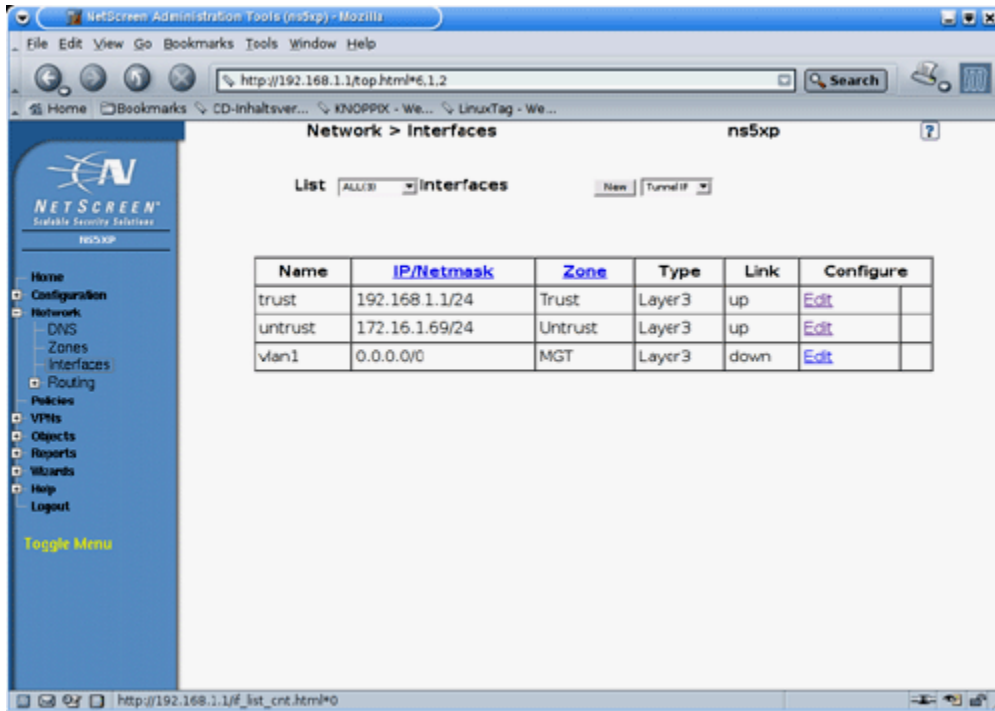




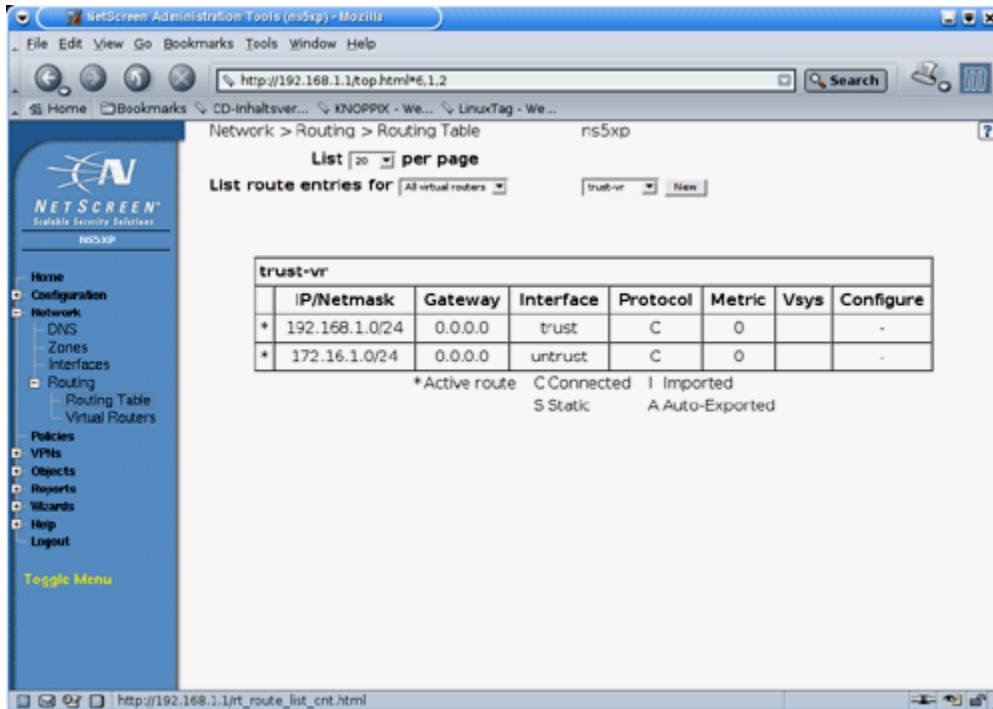
Las opciones se encuentran bajo el encabezado 'Network' hacen referencia a la propia configuración del dispositivo en la red, sin entrar en las labores de filtrado que realiza.



Los interfaces de red se refieren tanto a las interfaces físicas como a los virtuales, creados mediante segmentación lógica o perteneciente a interfaces de red privada virtual (VPN).



También se puede visualizar la tabla de rutas completa o desglosada por cada router virtual.



Como se puede apreciar, el dispositivo cuenta con todas las opciones necesarias para adaptarlo a casi cualquier entorno de red existente. Entre las opciones avanzadas, encontramos la interfaz para la gestión de redes privadas virtuales (VPN), bastante compleja en sí misma, y para el control de diversos parámetros de los informes generados.

Sin embargo, la sección Wizards no sólo contiene un asistente para la apertura de servicios al exterior, sino que incluye herramientas para facilitar la gestión de la funcionalidad más demandada. Entre otros, existe un asistente para la creación de enlaces de red privada virtual.

## **CAPÍTULO III**

### **SISTEMA ACTUAL**

#### **III.1.- Enfoque del Sistema Actual**

La gestión de negocio de la empresa Kelsy C.A. implica la interconexión con múltiples entidades externas, banca nacional, aliados de negocio, localidades remotas, etc, por lo tanto el factor seguridad es crítico y así lo entienden los gerentes de la Gerencia de Informática. La empresa cuenta con un portal Web de servicios integrados que actualmente está en proceso de evolución mediante la incorporación de nuevos productos para todos sus clientes. Este portal es utilizado actualmente aproximadamente por más de 250.000 clientes directos de la organización a nivel nacional y este número de clientes crece día a día, por lo cual la disponibilidad del servicio es de vital importancia para la empresa.

El sistema de seguridad perimetral que esta en producción actualmente, está basado en una zona de seguridad genérica DMZ, implantada a través de un firewall de prestaciones medianas centralizado en la sede de Caracas.

Dicho equipo consta de 3 interfaces físicas para el manejo de los perímetros de seguridad:

- a) **Trust:** Mediante esta interfaz se establecen todas las políticas de seguridad desde y hacia WAN-LAN de la empresa.
- b) **Untrust:** Mediante esta interfaz se establecen todas las políticas de seguridad desde y hacia Internet.
- c) **DMZ:** Mediante esta interfaz se establecen todas las políticas de seguridad desde y hacia las redes externas de la empresa: Banca, aliados de negocio, extranet, etc.

Este firewall es la columna vertebral de toda la arquitectura de seguridad perimetral de la empresa, todas las funciones de protección de la WAN-LAN están centralizadas en este sistema, que se pueden resumir de la siguiente manera:

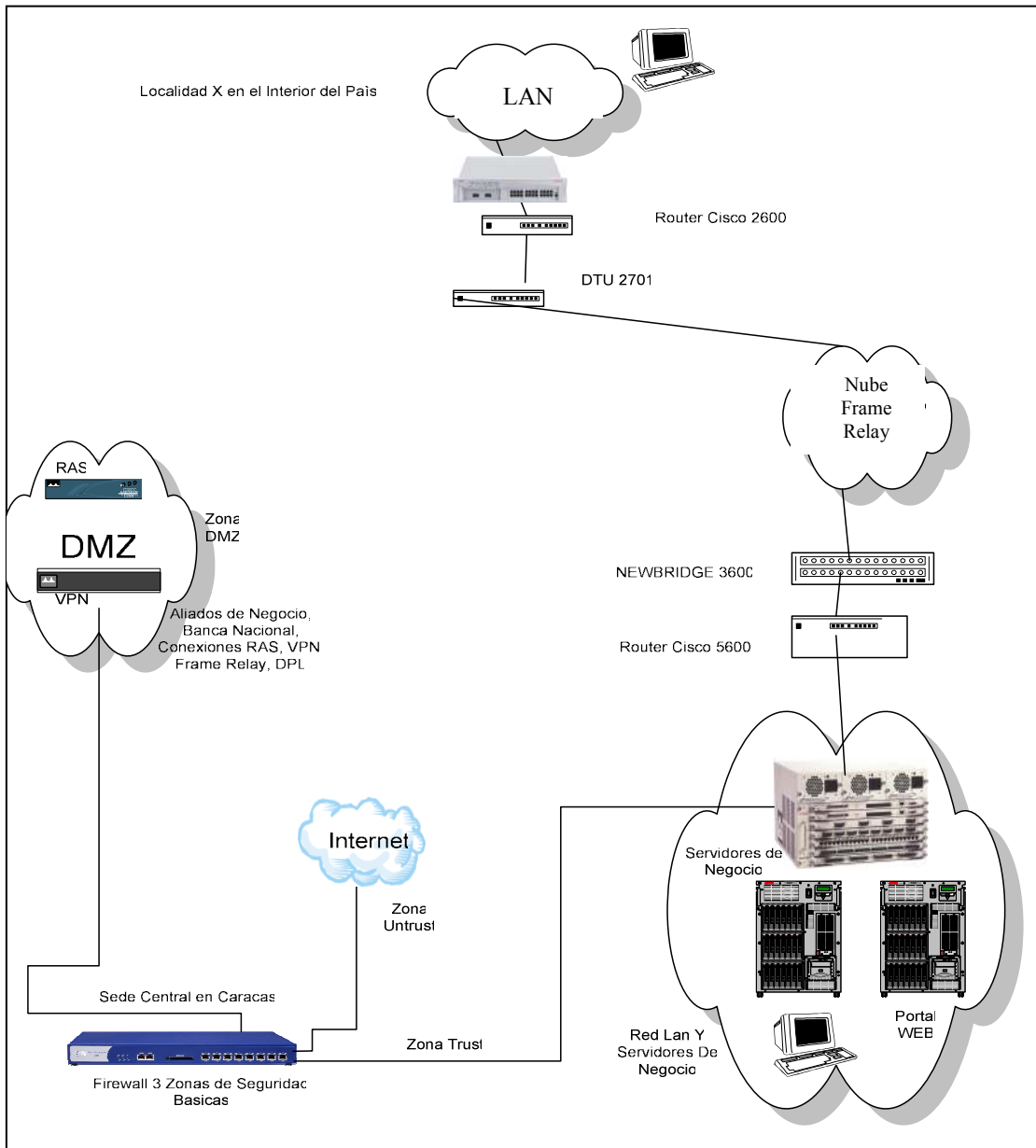
- 1) Publicar todos los servidores que deben ser accedidos desde la red pública Internet, o desde cualquiera de las redes externas que tienen conectividad hacia la red de la empresa y por ende hacia los aplicativos de negocio públicos.
- 2) Controlar el acceso desde cualquier zona DMZ, hacia la red de servidores de negocio, que se encuentran en la LAN.

- 3) Permitir la conexión de manera controlada y segura hacia los servidores de correo, vía Outlook Web Access.
- 4) Proteger la red interna de todas las conexiones remotas vía VPN, o mediante discado telefónico, de manera controlada mediante la aplicación de sólidas políticas de seguridad, en el firewall.

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

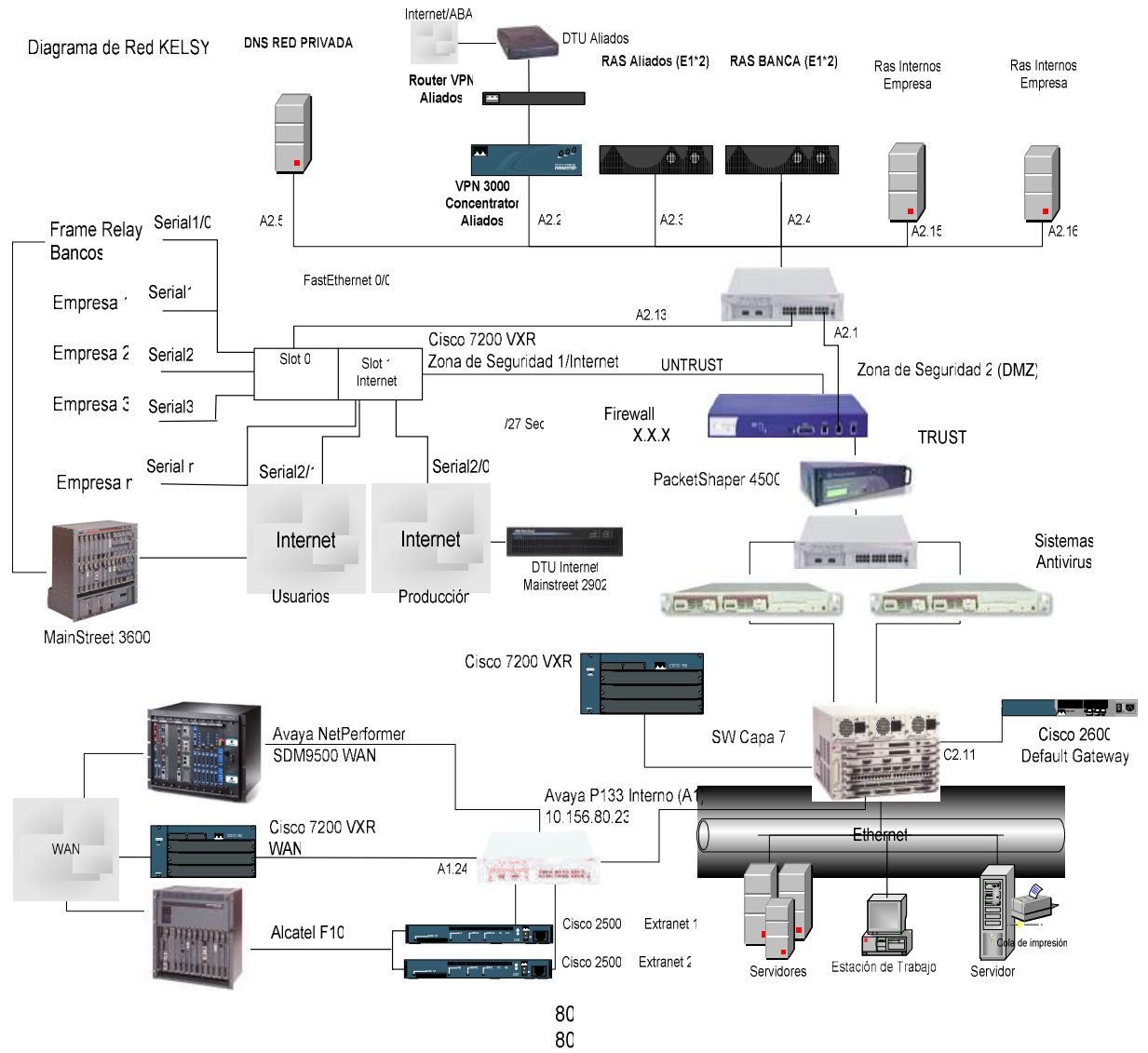
El estudio y análisis que se le realizó a la plataforma tecnológica del actual esquema de zonas de seguridad, permitió evaluar las alternativas que conllevaron a la actualización y migración de toda la arquitectura de seguridad, con el objetivo de mejorar y brindar una mayor protección a todos los activos informáticos, principalmente al portal de servicio de la organización y a las bases de datos críticas, para así garantizar la disponibilidad de la información y continuidad de los sistemas y por ende del negocio ante potenciales intentos de ataques tanto internos como externos.

A continuación se muestra un esquema general de la plataforma tecnológica de seguridad actual.



**Esquema Resumido de la Sistema Actual**

En detalle el esquema actual de seguridad se puede observar a continuación:



**Esquema detallado del Sistema Actual**



## **2.1.- Servicios y Accesos Disponibles**

### **2.1.1.- Acceso a Internet**

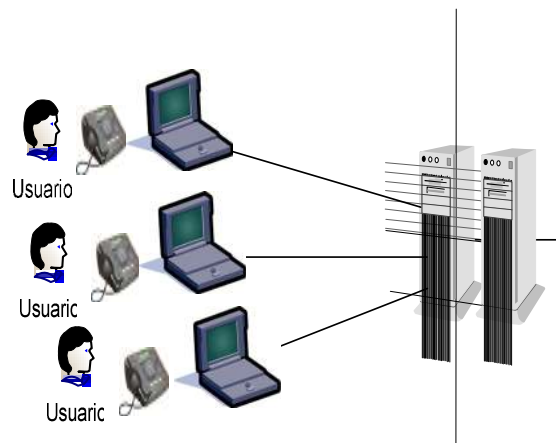
El acceso a Internet de toda la WAN a nivel nacional, esta centralizado en Caracas tal como se muestra en el esquema detallado y se realiza a través de dos enlaces E1, controlados mediante la interfaz untrust del firewall. Un enlace se utiliza para la navegación de los usuarios y otro para el portal de servicios de la organización. Estos dos enlaces E1 están implantados a través de un router Cisco VXR 7200.

El acceso a Internet de todos los usuarios es controlado mediante un sistema basado en hardware. Este sistema esta interconectado al directorio que se encuentra basado en tecnología Microsoft. Este arreglo le permite al dispositivo de filtrado Web realizar las consultas vía NTLdap, y determinar los perfiles de cada usuario para la navegación Web. NTLdap en la versión utilizada por Microsoft, del famoso LDAP (Lightweight Directory Access Protocol) en sí es un servicio de directorio ordenado y distribuido para buscar información en un entorno de red. LDAP puede considerarse una base de datos (aunque su sistema de almacenamiento puede ser otro diferente) al que pueden realizarse consultas.

### **2.1.2.- Acceso Remoto Discado para los Empleados de la Organización:**

Los empleados de la empresa con las siguientes características, tienen acceso remoto discado a la empresa:

- Móviles (usuarios que por motivos de trabajo requieren viajar constantemente por todo el país).
- Gerentes.
- Administradores de sistemas críticos de negocio.
- Administradores de sistemas informáticos críticos.
- Casos especiales.



Dichos empleados tienen acceso para realizar conexiones discadas desde su laptop personal, o desde sus casas, hacia la empresa, utilizando para tal efecto servidores RAS internos, que están configurados con los distintos perfiles de usuarios que implican distintos niveles de acceso a los sistemas y a la información. Estas conexiones son registradas y controladas las 24 horas del día y los 365 días de año.

### **2.1.3.- Enlaces VPN y RAS para los Aliados de Negocio**

Los aliados de negocio tienen acceso a las aplicaciones de negocio, a través de enlaces VPN y por medio de líneas discadas donde se aplican rigurosos mecanismos de autenticación, autorización y seguimientos de todas las actividades realizadas.

### **2.1.4.- Extranet**

En la banca nacional, tiene acceso directo a las aplicaciones de negocio de la organización, mediante las cuales se realizan los intercambios de datos desde las respectivas aplicaciones, vía enlaces Frame Relay .

### **2.1.5.- LAN y WAN**

La LAN y WAN de la organización son controladas y protegidas mediante la zona trust del firewall, esto permite la aplicación de políticas de seguridad detalladas para el acceso a la DMZ y para el acceso a Internet.

### **2.1.6.- Direccionamiento IP de las 3 Zonas Actuales**

Actualmente la empresa cuenta con un rango de direcciones IP, para cada una de las zonas en producción a través del firewall las cuales son:

#### **2.1.6.1- Zona Trust:**

**Segmento de Red:** 10.26.80.07

**Mascara:** 255.255.0.0

#### **2.1.6.2- Zona Untrust:**

**Segmento de Red E1:** 200.44.70.0

**Mascara:** 255.255.255.0

**Segmento de Red E1:** 200.200.31.0

**Mascara:** 255.255.255.248

#### **2.1.6.3- Zona DMZ:**

**Segmento de Red:** 192.32.0.0

**Mascara:** 255.255.0.0

La zona DMZ a su vez está dividida en distintos rangos aplicados a las distintas redes de acceso, aliados, banca, extranet, vpn, etc. Como no se dispone de mas interfaces físicas en el firewall actual, se tuvo que segmentar la zona genérica DMZ para poder brindar acceso a las redes externas, hacia los aplicativos de negocio de manera segura y controlada.

### **III.3.- Especificaciones del Sistema de Seguridad Firewall Actual.**

La plataforma de seguridad actual esta basada en firewall con tecnología ASIC (*Circuitos Integrados de Aplicaciones Especificas*), tipo **Appliance** (hardware), para así garantizar un alto desempeño. El mismo posee las siguientes características físicas:

- 3 interfaces Fast ethernet (**Trust, Untrust, DMZ**).
- Capacidades VPN por hardware (no implementada actualmente).

- Sistema de administración Web.
- Capacidades de Cluster (HA).
- Mecanismos de defensa típicos mediante plantilla automática.
- Sistemas de autenticación de usuarios remotos.
- Muchas otras características avanzadas.

### **III.4.- Políticas de Seguridad Generales Aplicadas en el Firewall**

#### **4.1.- Política de Acceso Web al Exterior Zona (Untrust):**

Esta política tiene configurada reglas para el acceso a Internet, a través de protocolos específicos que permiten controlar todo el tráfico saliente. Básicamente para la navegación la política establece que toda conexión Web saliente, puede ser realizada únicamente por el sistema de filtrado Web. Este dispositivo a su vez controla la navegación de todos los usuarios a nivel nacional, y solo permite navegar los usuarios autenticados en el directorio activo y con permisos efectivos, por lo tanto en los navegadores de los usuarios deben tener configurado un proxy.

En el sistema de filtrado Web están configuradas algunas reglas como por ejemplo: acceso o restricción a contenidos tales como audio (mp3, mp2, rmi, etc.), video (mpeg, asf, wmf, vid, etc.) por grupos y horarios. Entre los protocolos controlados se encuentran HTTP, FTP, SMTP, POP3, H.323, MSN Messenger, PNM, RTSP, etc.

#### **4.2.- Política de Detección de Intrusos**

Esta es una plantilla automática, configurable, que cuenta con mecanismos integrados de detección de intrusos que avisan cuando se inicia un determinado tipo de ataque contra la red. Por ejemplo, se tiene configurado para que notifique si se detecta un intento de exploración de puertos, IP spoofing, ICMP flood, Syn flood, ect.

#### **4.3.- Publicación del Portal de Servicios**

Las reglas de publicación en Web permiten el acceso seguro al portal Web, servidores de correo, y demás sistemas públicos Web.

### **III.5- Limitaciones en el Entorno del Sistema de Seguridad Actual**

Un factor de riesgo de gran peso a considerar en la plataforma actual, es todo referente a la alta disponibilidad de los servicios. Potencialmente si por algún motivo firewall central queda fuera de servicio por fallas técnicas, por un tiempo prolongado o un tiempo corto, la empresa quedaría sin servicios y toda comunicación externa sería afectada. La alta disponibilidad fue un factor a considerar de vital importancia, para el diseño del nuevo esquema de zonas de seguridad.

### **III.6- Análisis y Elección de los Nuevos Dispositivos Firewall**

El análisis y estudio que se le realizó a la plataforma de seguridad de la organización, conjuntamente con la información producto de las investigaciones de la Gerencia de

Seguridad sobre las diferentes tecnologías de firewall que se ofrecen actualmente en el mercado, condujo a identificar las necesidades y requerimientos que deben cumplir los nuevos firewall que vayan a implantar. Estos requerimientos se exponen a continuación:

- Capacidades de alta disponibilidad.
- Alto desempeño con categoría carrier class.
- Estabilidad en el tiempo.
- Interfaz de administración sencilla, amigable, basada en Web, con ayuda en línea, de manera que pueda simplificar su administración sin consumir mucho tiempo.
- Contar con una amplia garantía en Venezuela, con soporte técnico de la compañía que lo fabrica y poseer una certificación avalada por la casa matriz.
- También se debe contar con un contrato de soporte que garantice la solución de problemas, incluso con reemplazo de partes, en periodos de menos de 24 horas, 5x24.
- Equipada con múltiples puertos físicos (8 puertos mínimo), para crear múltiples zonas de seguridad en la red.
- Adicionalmente debe soportar conexiones VPN vía hardware, de alto desempeño.
- La solución debe ser basada en hardware ASIC tipo appliance, para garantizar un mejor desempeño, con categoría carrier class.

## **CAPÍTULO IV**

### **SISTEMA PROPUESTO**

#### **IV.1.- Solución Conceptual Del Sistema Propuesto**

La conceptualización de la nueva plataforma de seguridad se fundamenta en la utilización de tecnología ASIC de alto desempeño con categoría carrier class, a través de la cual se busca proteger a todos los sistemas de negocio de la empresa y a la red corporativa en general. Esta tecnología permitirá obtener múltiples ventajas tanto económicas como tecnológicas en el diseño e implantación del nuevo esquema de seguridad.

La nueva arquitectura de zonas de seguridad será capaz de controlar todo el tráfico generado independientemente de donde se origine, de forma completamente centralizada, con capacidad alta disponibilidad y balanceo de carga, sin la necesidad de crear redes paralelas para cada una.

Para poder realizar un nuevo diseño de zonas de seguridad óptimo y funcional, adaptado a las necesidades de seguridad de la empresa, se realizó primero un análisis profundo de la situación actual, mediante el cual se pudieron detectar todas las fallas de seguridad en la red perimetral.



Para tal efecto se realizaron mesas de trabajos con todas las áreas involucradas responsables de los aplicativos de negocio, portal de servicios Web, bases de datos, etc. De estas mesas de trabajo se pudo levantar toda la información que sirvió como insumo para determinar qué servicios eran necesarios para cada sistema, puertos, que servidores deberían tener acceso a determinadas base de datos, qué personas estaban autorizadas para acceder a servicios, todo esto con miras a la creación de las políticas de cada zona de seguridad. También se tomaron decisiones en referencia a la ubicación física de cada servidor en su respectiva zona de seguridad funcional.

#### **IV.2.- Consideraciones de Diseño**

Las siguientes consideraciones de diseño se tomaron en cuenta para generar la solución final.

##### **2.1.- Documentar adecuadamente la arquitectura del firewall**

La falta de consistencia suele provocar brechas de seguridad al permitir tráfico innecesario para los propósitos de la organización, incrementando así los riesgos de seguridad.

Así mismo en ocasiones esto provoca la negación de servicios legítimamente requeridos por la organización, creando la necesidad de crear reglas de excepción para satisfacer dichos requerimientos; esto complica la administración del firewall y suele generar problemas de estabilidad.

## **2.2.- Análisis de los requerimientos de seguridad de la organización**

Seleccionar un producto o sistema inadecuado con lleva un impacto negativo en el balance costo-beneficio para la organización y proporciona una protección inadecuada, sobrada o insuficiente. La falta de un análisis de los requerimientos de seguridad de la organización junto con restricciones de presupuesto suelen ser las causas más comunes de estos problemas. La incompatibilidad con dispositivos de red y otras aplicaciones de red es también frecuente. Esto se evitara en la empresa realizando una matriz de evaluación (técnica-económica), para la elección de la solución que más se adaptará a los requerimientos de la misma.

## **2.3.- Segmentación de las zonas de seguridad**

Es importante realizar una clasificación de todos los recursos y aplicativos informáticos, con el fin de ubicarlos en su zona de seguridad adecuada, de acuerdo a las características del origen del tráfico cursado.

El concepto de zona desmilitarizada, se aplica ampliamente en el presente diseño de zonas de seguridad, una DMZ como se le conoce comúnmente es definida como una zona donde se colocan sistemas que por sus características presentan altos riesgos de seguridad. Los sistemas que se colocan en estas zonas son aquellos, que ofrecen servicios hacia el exterior con un potencial riesgo de seguridad para los sistemas.

Sistemas que típicamente se colocan en este tipo de zona son:

- Servidores de FTP, base de datos, servidores de red, servidores de directorio activo, correo, DNS y Web, entre otros; todos ellos ofrecen servicios al exterior o también deben ser utilizados internamente en la empresa por sus trabajadores.
- Puntos de acceso inalámbricos (wireless), RAS, VPN.
- Enlaces de comunicaciones con entes externos, etc.

Debido a que la empresa tiene servicios de este tipo como son:

- Correo.
- Portal de servicios Web.
- Aplicativos de negocio, que son accedidos vía enlaces VPN, DPL, Frame Relay y RAS.

Dichos servicios necesitan ser accedidos desde el exterior y se justifica la aplicación del concepto de zonas de seguridad (DMZ), para poder brindar protección perimetral a los sistemas internos de la corporación.

A cada zona de seguridad protegida se le asigna una interfaz de red en el firewall con su respectivo direccionamiento IP.

El presente diseño también contempla la creación de una zona de seguridad para la protección de las bases de datos o sistemas críticos internos de la empresa.

Estos recursos serian:

- Servidores de bases de datos corporativas con información altamente confidencial (información de clientes, procesos criticos, etc.).
- Servidores críticos de operación interna, como son servidores de nómina y bases de datos de recursos humanos, etc.
- Sistemas automatizados de producción que utilizan redes locales.
- Otros sistemas importantes para la gestión de negocio de la empresa.

La razón de utilizar zonas de seguridad solo para uso interno, radica en el hecho de que muchos incidentes de seguridad informática se originan en el interior de las organizaciones, como es bien conocido por los administradores de la seguridad.

#### **2.4.- Integración de los dispositivos firewall con otros controles de seguridad**

Desde el punto de vista de costo la integración de firewalls con otros controles de seguridad (antivirus, IDS, control de contenido Web, sistemas de auditoria, etc.), en un mismo dispositivo suele traer beneficios, ya que la cantidad de recursos invertidos para implementar y administrar estas soluciones suelen ser menores; sin embargo, desde el punto de vista de seguridad se generan puntos únicos de fallo (“single points of failure”).

Dado que en esta configuración los controles comparten recursos como memoria, ciclos de procesador y tarjetas de red, un fallo grave en alguno de ellos afectaría a los demás controles ubicados en el mismo dispositivo, comprometiendo así todo el esquema de seguridad de la empresa. Debido a esto se tomo la decisión de no integrar todos estos servicios en un solo dispositivo único.

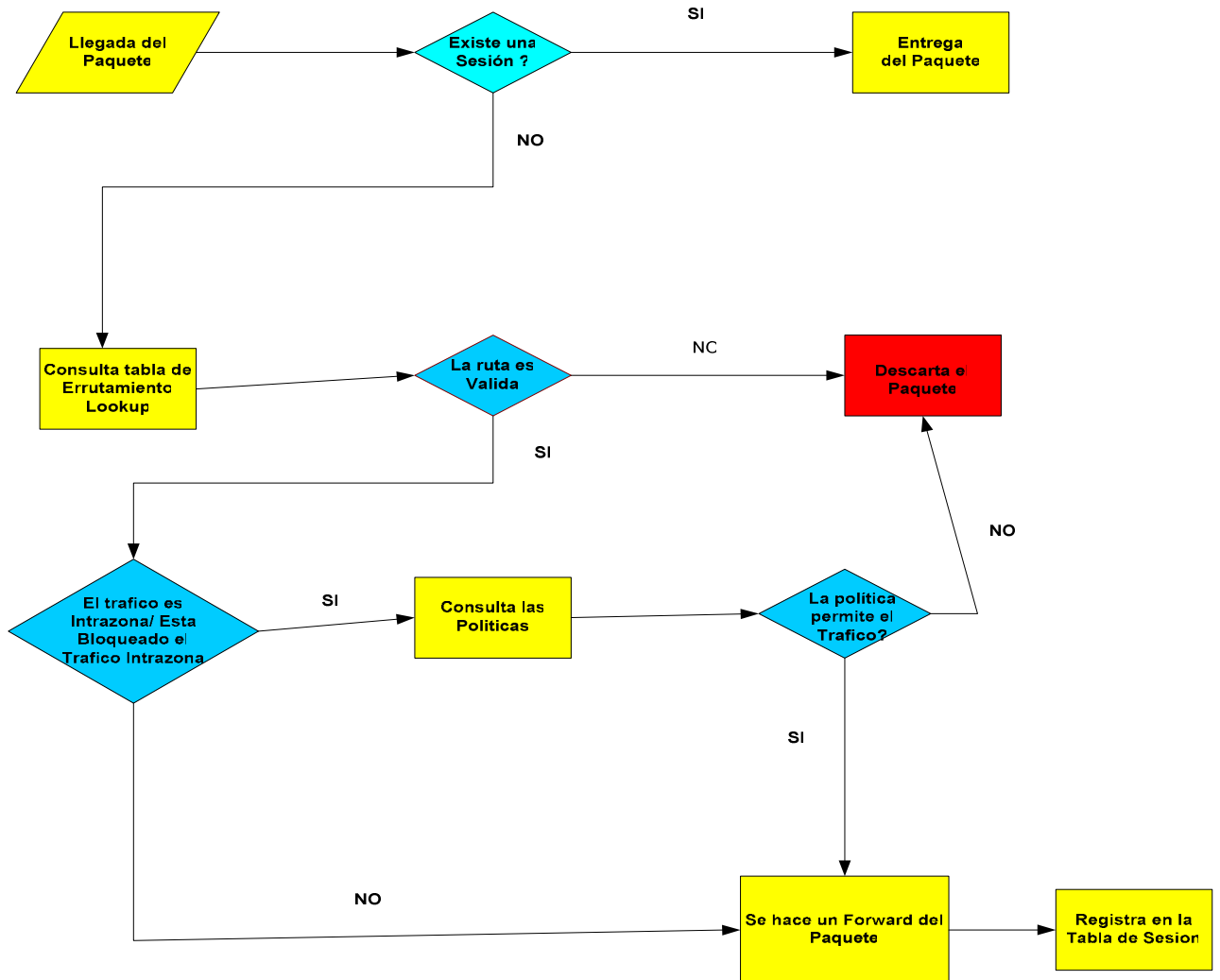
### **IV.3.- Diseño de la Solución**

La nueva arquitectura de zonas de seguridad se fundamenta es un diseño escalable, basado en los estándares y las mejores practicas aplicadas internacionalmente. Toda la tecnología es de alto desempeño ASIC (Circuitos Integrados de Aplicaciones Especificas). Dichos equipos también cumplen con la categoría carrier class, cuya confiabilidad es 99.999%, y permiten las siguientes ventajas:

- Optimizar y mejorar estrategias de seguridad a través de la arquitectura y mitigación de riesgos.
- Maximizar retornos de inversión (ROI).
- Mejorar la disponibilidad de los servicios.
- Reducción de pérdidas, por paradas inesperadas

La solución combina los diferentes tipos de firewall, packet filter, application-Level, Circuit-Level, y también funciones, stateful inspection y deep inspection, de tal forma

que la plataforma de seguridad permita el control exacto y al detalle de todo el tráfico cursado a través de las zonas de seguridad. Básicamente el proceso de decisión a través del firewall será el siguiente:



**Proceso de Decisión del Flujo de un Paquete**

El nuevo diseño ubica los niveles de seguridad más altos, en las zonas o puntos de acceso a los servicios de alto riesgo.

### **3.1.- Nuevo Esquema de Zonas de Seguridad**

El nuevo diseño contempla utilizar las siguientes 8 zonas de seguridad, son 9 zonas pero una en realidad una es la zona MGT (Esta es la zona de uso excluido para la administración vía Web del la interfaz de firewall):

**3.1.1- Zona MGT Administrativa:** Básicamente esta zona es de uso exclusivo para la administración de los firewall, las interfaces de administración de los firewall serán ubicadas en esta zona según su direccionamiento IP.

**3.1.2- Zona Confiable (Trust) LAN:** Esta es la zona mediante la cual la red Lan se va a comunicar con el firewall, para acceder a todos los servicios que son controlados a través de la plataforma de seguridad. La interfaz de esta zona es Giga Ethernet, para garantizar una mejor velocidad de acceso a los servicios.

**3.1.3 - Zona VPN y Aliados:** Permite la conexión de las empresas aliadas de negocio, estas empresas pueden utilizar los sistemas y aplicaciones dispuestos para atender a este universo de clientes.

Las conexiones de los aliados de negocio generalmente son a través de enlaces VPN contratadas con terceros, o conexiones dial up. La interfaz de esta zona es Fast Ethernet.

**3.1.4 - Zona de Servicios WEB, Correo, FTP (IAS Internet Application Server):** Todos los servicios Web, servidores de correo front end, y servidores FTP, serán ubicados en esta zona de seguridad. La interfaz de esta zona es Giga Ethernet, para garantizar una mejor velocidad de acceso a los servicios.

**3.1.5 - Zona Extranet:** Todas las conexiones con los clientes principales de la empresa se realizarán a través de una extranet, cuya interconexión se realizara por esta zona. La interfaz de esta zona es a Fast Ethernet.

**3.1.6 - Zona Bancaria:** Mediante esta zona se realizará toda la interconexión con toda la banca a nivel nacional, para la transmisión de los pagos de los clientes, y también para que la banca pueda hacer uso de las aplicaciones de negocio de la empresa. La interfaz de esta zona es a Fast Ethernet,.

**3.1.7 - Zona de Servidores Públicos:** En esta zona serán ubicados todos aquellos servicios que utilicen los aliados de negocio, extranet, banca, es decir en la zona de servidores público como tal.



La interfaz de esta zona es a Giga Ethernet, para garantizar una mejor velocidad de acceso a los servicios.

**3.1.8 - Zona no confiable Internet (Untrust):** Mediante esta zona se establecerá las conexiones tanto entrantes como salientes con Internet, prestara servicio a todas las zonas de seguridad en correlación con las políticas aplicadas. La interfaz de esta zona es a Fast Ethernet.

**3.1.9 - Zona de Base de Datos:** En esta zona se ubicaran todas las bases de datos para los sistemas de negocio, así como también las bases de datos de los distintos sistemas y aplicaciones que se utilicen en la empresa. Esta es una zona crítica por su importancia y es una zona en la cual se debe tener mucho cuidado en la elaboración de las políticas de acceso.

#### IV.4.- Diseño del Direccionamiento IP de las Zonas

El Direccionamiento IP asignado a cada zona se puede ver en la siguiente tabla, así como también el rango de direcciones aplicados a cada servicio en cada zona.

MGT	MGT	Zona MGT Firewall 172.26.1.1( Netscreen 500 I), 172.26.1.2( Netscreen 500 II)		Mask
		172.26.1.1 Firewall 1 172.26.1.2 Firewall 2 172.26.1.3 Raul Quiñónez 172.26.1.4 Administrador 2 172.26.1.5 Disponible 172.26.1.6 Disponible		255.255.255.248
1	2/1.2(1000 BT)	Zona 1 Trust Rango IP( LAN) (10.26.80.1 a 10.26.87.170 SERVER)	Rango IP Equipos	Mask
		Ip Firewall 10.26.80.9 Operativa	10.26.80.1 a 10.26.87.255	255.255.248.0
2	1/1(100BT)	Zona 2 Rango IP ( Ras y VPN Aliados de Negocio) ( 172.26.192.51 hasta la 172.26.207.254)	Rango IP Equipos De comunicaciones y Clientes VPN	255.255.240.0
		Rango Equipos Telecom	172.26.192.4 hasta 172.26.192.254	
		IP Zona Firewall	172.26.192.1	
		FastEthernet RAS	172.26.192.2	
		FastEthernet VPN Aliados	172.26.192.3	
		Router Aliados Fast Ethernet	172.26.192.4	
		IP Administrativo SW Foundry Server Iron	172.26.192.5	
		IP para el Balanceo de Carga	172.26.192.50	
		DNS Aliados de Negocio	172.26.192.10	
		Rango Clientes Ras Reservados DHCP	172.26.193.1 hasta la 172.26.193.113	
		Rango Clientes Ras DHCP Disponibles Reservados	172.26.193.114 hasta la 172.26.193.254	
		VPN		
		Rango Disponible Clientes VPN Aliados	172.26.194.1 hasta 172.26.207.254	
		Pool IP VPN 1	172.26.194.1 hasta 172.26.194.254	

		Pool IP VPN 2	172.26.195.1 hasta 172.26.195.254	
		Pool IP VPN 3	172.26.196.1 hasta 172.26.196.254	
		Pool IP VPN 4	172.26.197.1 hasta 172.26.197.254	
<b>3</b>	<b>4/2(1000BT)</b>	<b>Zona 3( IAS) Rango IP Servidores ( Web Server y Correo)(172.26.24.51 hasta la 172.26.27.254) Internet Application Server</b>	<b>Rango IP</b>	<b>255.255.252.0</b>
		Rango Equipos Telecom	172.26.24.2 hasta la 172.26.24.50	
		IP Zona Firewall	172.26.24.1	
		IP Administrativa SW de la Zona	172.26.24.2	
		IP Switch Foundry ServerIron Balanceo de Carga	172.26.25.50	
		Email Servers	172.26.25.51 hasta la 172.26.25.60	
		WebServer	172.26.26.61 hasta la 172.26.25.254	
		Ip Diponibles	172.26.26.1 hasta la 172.26.27.254	
		<i>Servidor Web 1</i>	172.26.25.61	
		<i>Servidor Web 2</i>	172.26.25.62	
		<i>Servidor Web 3</i>	172.26.25.63	
		<i>Servidor Web 4</i>	172.26.25.64	
		<i>Servidor de Correo Front End</i>	172.26.25.51	
<b>4</b>	<b>1/2(100BT)</b>	<b>Zona 4 Rango IP Extranet ( 172.26.20.51 hasta la 172.26.23.254)</b>	<b>Rango IP</b>	<b>255.255.252.0</b>
		Rango Equipos Comunicaciones	172.26.20.2 hasta 172.26.20.50	
		IP Zona Firewall	172.26.20.1	
		DNS Extranet	172.26.20.10	
		Router Empresa 1	172.26.20.2	
		Router Empresa 2	172.26.20.3	
		Router Empresa 3	172.26.20.4	
		Router Empresa 4	172.26.20.5	
		Router Empresa 5	172.26.20.6	
		Router Empresa 6	172.26.20.7	
		Disponibles	172.26.20.51 hasta la 172.26.23.254	
<b>5</b>	<b>3/1(100 BT)</b>	<b>Zona 5 Rango IP FR Bancos y RAS Banca( 172.26.16.51 hasta la 172.26.19.254)</b>	<b>Rango IP</b>	<b>255.255.252.0</b>
		Rango Disponibles Para Equipos Comunicaciones	172.26.16.2 hasta el 172.26.16.50	
		IP Zona Firewall	172.26.16.1	

		Ras Banca FastEthernet Routers Banca DNS Banca  Rango Clientes Ras Banca DHCP  Rango Clientes Ras Banca DHCP Disponibles Reservados  Rango IP Disponibles	172.26.16.2 172.26.16.3 172.26.16.10 172.26.16.51 hasta la 172.26.16.113 172.26.16.114 hasta la 172.26.16.254 172.26.17.1 hasta la 172.26.19.254	
<b>6</b>	<b>4/1(1000 BT)</b>	<b>Zona 6 Rango IP Servidores Publicos ( 172.26.28.51 hasta la 172.26.31.254)</b>	<b>Rango IP</b>	<b>255.255.252.0</b>
		Rango IP Disponibles Comunicaciones IP Zona Firewall IP Switch Foundry ServerIron Administrativa IP para Balancear Sidunea  Rango IP Servidores Publicos  Disponibles Servidores	172.26.28.2 hasta la 172.26.28.50 172.26.28.1 172.26.28.20 172.26.29.50 172.26.28.51 hasta la 172.26.28.76 172.26.28.78 hasta la 172.26.31.255	
<b>7</b>	<b>2/2(1000 BT)</b>	<b>Zona 7 Rango IP DB Servidores ( 172.26.32.51 hasta la 172.26.35.254)</b>	<b>Rango IP</b>	<b>255.255.252.0</b>
		Rango Disponibles Para Equipos IP Zona Firewall  Rango IP Disponibles Servidor Base de Datos 1 Servidor Base de Datos 2 Servidor Base de Datos 3 Servidor Base de Datos 4	172.26.32.2 hasta la 172.31.32.50 172.26.32.1 172.26.32.51 hasta la 172.26.35.254 172.26.32.51 172.26.32.52 172.26.32.53 172.26.32.54	
<b>8</b>	<b>3/2(100 BT)</b>	<b>Zona 8 Rango Untrust</b>	<b>Rango IP</b>	
		IP Firewall con Enlace ( ISP 1) IP Firewall con Enlace ( ISP 2)  Direcciones Publicas: www.KELSY.com sera la 200.44.70.10 esta a su vez sera la 172.26.25.50 Correo.Kelsy.com Sera la 200.44.70.11	200.44.70.2 200.200.231.226	<b>255.255.255.0</b> <b>255.255.255.248</b>

#### **IV.5.- Políticas Aplicadas a las Zonas de Seguridad**

Las políticas aplicadas a las zonas de seguridad básicamente dejan pasar el tráfico hacia cada zona, solamente permitiendo los servicios estrictamente necesarios para cada aplicación. A su vez todo el tráfico es monitoreado constantemente por los sistemas de auditoría de seguridad.

#### **IV.6.- Notación Para Documentar las Reglas del Firewall**

A lo largo del presente trabajo se utilizará la siguiente notación para el levantamiento de la información, en referencia a las reglas que serán implantadas en los firewall las cuales plasman los requerimientos de seguridad de la empresa, en función de las distintas zonas de seguridad y los sistemas que residen en dichas zonas o perímetros de seguridad. Esta notación es general e independiente de la tecnología utilizada y es ampliamente captada en las distintas bibliografías de seguridad que se pueden encontrar en Textos e Internet.

<b>No.</b>	<b>Recurso Externo</b>	<b>Dirección. del tráfico</b>	<b>Recurso interno</b>	<b>Características del tráfico</b>	<b>Acción</b>

**No.** Identifica el número de regla en el firewall. Para efectos de ejecución se considera que cada regla se ejecuta en orden ascendente y de manera secuencial. Esto no es simplemente un consideración general, es un punto que se debe tomar en cuenta y es muy importante en el momento de programar las reglas en el firewall, ya que una mala ubicación de las reglas pudiera dejar pasar tráfico no permitido, o también bloquear tráfico permitido.

- **Recurso externo:** define cualquier recurso (sistema, dispositivo de red, etc.) ubicado en una zona no protegida (externa) desde el punto de vista del firewall, como por ejemplo Internet.

- **Dir. de tráfico:** define la dirección del tráfico través de 3 símbolos compuestos de 2 y 3 caracteres,  $\rightarrow$ ,  $\leftarrow$  y  $\leftrightarrow$ ; simbolizan tráfico iniciado desde un recurso externo a uno interno, tráfico iniciado desde un recurso interno a uno externo y tráfico entre recursos internos y externos iniciado por cualquiera de las partes (bidireccional) respectivamente; Nótese que la dirección identifica únicamente a quién inicia el tráfico y no al tráfico en sí (que es bidireccional por naturaleza).

- **Características del tráfico:** se refiere los patrones identificados por el firewall en el tráfico de red que activan la regla y se utilizan paréntesis, y los símbolos **&** (AND) y **|** (OR) para definir el patrón. Es decir el tipo de tráfico, ejemplo puertos tcp 21, 22, 26.

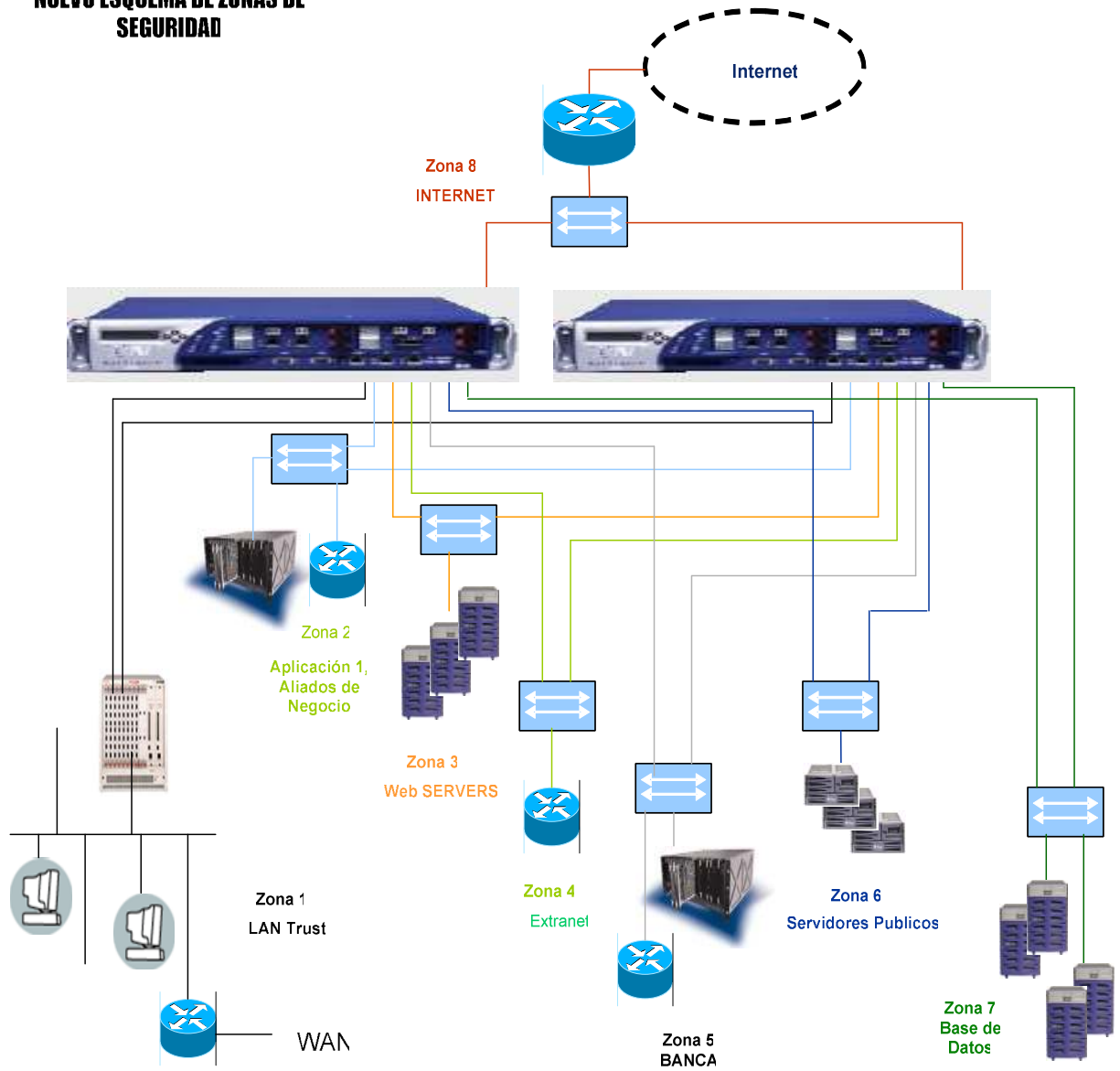
• **Acción:** Define la acción a realizar por el firewall; entre las acciones que puede ejecutar el firewall se encuentran: Aceptar (Permit) (permite el tráfico), Rechazar (Deny) (bloquea el tráfico y notifica al origen) y Descartar (Reject) (bloquea silenciosamente el tráfico), o Construir un Tunel (Tunel).

Esto se puede comprender mejor con el siguiente ejemplo

<b>No.</b>	<b>Recurso Externo</b>	<b>Dir. De Trafico</b>	<b>Recurso interno</b>	<b>Características del tráfico</b>	<b>Acción</b>
<b>1</b>	<b>Cualquiera (Any)</b>	<b>-&gt; Entrante</b>	<b>Servidor Web</b>	<b>(protocolo = TCP) &amp; (puerto destino =[80 443]) Es decir http y Https</b>	<b>Permitir Permit</b>

El esquema completo de las nuevas zonas de seguridad se puede ver en el siguiente diagrama:

### NUEVO ESQUEMA DE ZONAS DE SEGURIDAD





#### **IV.7.- Consideraciones Operacionales para los Enlaces de Conexión Internet**

Las empresas ISP deberán garantizar la operatividad de los enlaces de comunicaciones de Internet los 365 del año, las 24 horas del día, y operar una plataforma de administración necesaria para proporcionar procedimientos de monitoreo, administración y gestión centralizada como parte del servicio. Adicionalmente la empresa integradora de servicios que vendió la solución de seguridad firewall y los Switch SLB( balanceadores de carga) , debe proveer la accesoria y un contrato de mantenimiento y servicio de los equipos por un año. Dicho contrato tiene opción a la renovación y debe garantizar que durante el tiempo que dure la negociación de la renovación, se garantice la continuidad del mantenimiento y accesoria en referencia a todos los equipos.

Se tomó la decisión de contratar dos ISP diferentes para los enlaces de acceso a Internet, para así garantizar la operatividad de por lo menos un enlace, en el caso que una de la empresas sufra alguna falla en el servicio.

#### **IV.8.- Balanceo de la Carga:**

##### **8.1- Sistemas para el balance de las cargas HTTP y HTTPS**

Tecnologías de balanceo de carga se implementaron a nivel de las zonas de seguridad, Web, servidores públicos, para garantizar disponibilidad, alto rendimiento y administración de todas las transacciones HTTP y HTTPS, dirigidas hacia cada grupo de servidores que prestan servicio al portal Web. Los switches Web ServerIron 400 brindarán capacidades administrativas para

controlar y administrar el flujo de tráfico de aplicaciones, transacciones y comercio electrónico. Estos dispositivos cuentan con la seguridad IronShield. Esta característica brinda protección contra las distintas formas de ataques de negación de servicio, dichos ataques también son detectados y controlados a través de las plantillas de seguridad de los firewall.

El Balanceo de Cargas ofrece escalabilidad de todos los recursos de red, además de proveer monitoreo y control de sitio a sitio y asistencia en la identificación de problemas de rendimiento en la red.

## **8.2- Ventajas que Ofrece el Balanceo de Cargas**

Algunas de las ventajas que nos brinda la utilización de estos equipos capa (4-7) en la nueva solución de zonas de seguridad son:

- Funciones de administración del tráfico en Internet y tráficos cuyo origen puede ser cualquier zona de seguridad o perímetro, incluidos balanceo de carga de servidores a nivel global y local. SLB (Server Load Balance) de alta disponibilidad con configuración activa/activa y failover manteniendo el estado de la sesión.

Los SLB permiten servicios distribuidos basados en IP y balanceo de tráfico de manera transparente a través de distintos servidores, que pueden ser monitoreados continuamente.

- Balanceo de carga de firewalls, switcheo de caché transparente, redirección de paquetes, filtrado y priorización de paquetes y soporte para switcheo de capa 7 como cookies y URLs.

- El Server Iron proporciona la base para un servicio de alta disponibilidad, recuperación de desastres, transparencia en la ubicación del servidor y los sitios y control de costos del backbone.
- Balanceo de carga de VPN/firewall (Firewall Load balace) de alto rendimiento
- Switcheo de caché sensible al contenido y soporte superior para los principales protocolos de medios de streaming.
- **Global Server Load Balancing (GSLB):** Permite distribuir servicios transparentemente a través de múltiples site y servidores, y balancear los tráfico a través de los site o servidores, con herramientas de monitoreo
- **Firewall Load Balancing (FWLB):** Esta características le permite distribuir el tráfico a través de múltiples firewall, con la ventaja de poder realizar configuraciones de alta disponibilidad, y eliminar puntos de fallas únicos. También permite la estabilidad en la arquitectura de seguridad.
- **Transparent Cache Switching (TCS):** Esta característica elimina la necesidad de configurar las opciones de cache de cada browser de cada cliente, mejora los tiempos de respuestas de Internet o de cualquier otra zona, baja los costos de las conexiones WAN. El switch se encarga de gestionar de forma transparente y sencilla el contenido del cache.

Los Server Iron también permiten funciones de alta disponibilidad de las aplicaciones, ya que se pueden detectar condiciones de error, como por ejemplo HTTP "404 – Object not found", antes de otorgar el acceso a los clientes, y puede direccionar el tráfico hacia otro servidor que este operativo, de manera transparente para los clientes.

El mecanismo utilizado por los SLB para el balanceo del tráfico se basa en la asociación de los Virtual Server con los Real Server. Los Real Server son propiamente los servidores aplicativos en este caso los servidores Web, los servidores virtuales tienen una o mas direcciones IP (VIPs), que deben ser asociadas con los servidores reales aplicando un binding de los puertos, TCP/UDP de los servidores reales con los puertos TCP/UDP de los servidores virtuales. Cuando un cliente envía una petición TCP/UDP (peticiones) a un puerto del servidor virtual, el SI (Serveriron), envía la petición del cliente hacia el servidor real de manera transparente para el cliente.

#### **IV.9.- Configuración del SLB**

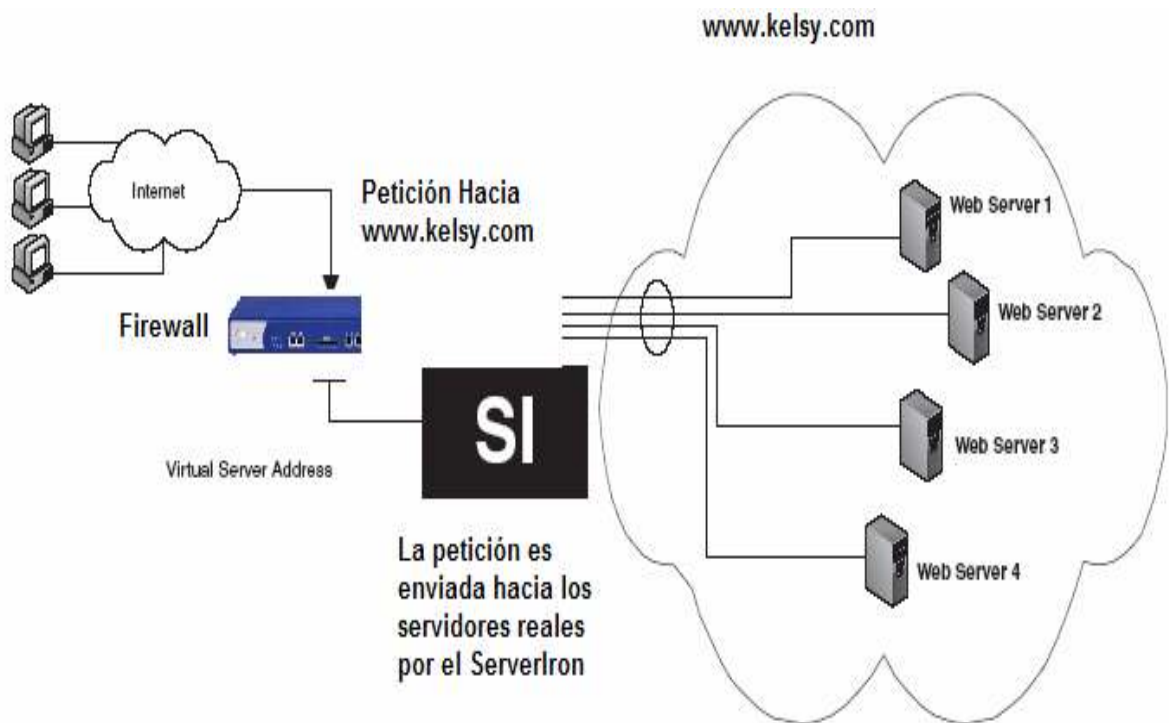
La configuración funcional del SBL se basa en lo siguiente:

La primera zona que requiere balanceo de carga, redundancia y alta disponibilidad de forma critica es la zona de los IAS (Internet Application Server), entonces en primera instancia se le asignara una dirección lógica para el balaceado de la carga HTTP y HTTPS, dicha dirección será la siguiente: 172.26.25.50, todos los servicios accesos

desde Internet y desde las demás zonas que apunten al Url `www.kelsy.com`, serán direccionados mediante las políticas NAT del firewall a esta dirección y a su vez internamente el SLB realizara el balanceo de todo el tráfico HTTP y HTTPS entre los 4 servidores Web:

El URL `www.kelsy.com` será resuelta en los DNS como la `200.44.70.10`, ésta será direccionada mediante un NAT en el firewall hacia la dirección virtual `172.26.25.60` del SI (ServerIron).

Este método básico se puede ver en la siguiente Figura:



Direcciones IP:  
Web1:172.26.25.61  
Web2: 172.26.25.61  
Web3: 172.26.25.61  
Web4: 172.26.25.61

El SI mapea una conexión lógica que parte desde el servidor virtual, hacia los servidores reales físicos estableciendo una sesión HTTP o HTTPS.

Para garantizar la alta disponibilidad en las transacciones, la nueva solución contempla una configuración activa-activa, en los switches para brindar protección de pérdidas de sesiones por falla de cualquier switches.

### **9.1.- Tipos de Métricas disponibles para el balanceo del Tráfico**

Las métricas determinan como se realizará el balanceo del tráfico de los clientes hacia los servidores reales. Entre los tipos de métricas disponibles tenemos las siguientes:

**9.1.1.- Least connections:** Esta métrica se caracteriza porque la conexión es direccionada hacia el servidor real que tiene la conexión mas reciente del cliente. Si los servidores tienen distintas capacidades de procesamiento, siempre el servidor más rápido y tendrá más conexiones que los más lentos.

**9.1.2.- Round Robin:** Aquí las peticiones de los clientes son direccionadas a cada servidor real en forma secuencial, es decir una para un servidor, luego una para el otro, y así sucesivamente hasta completar un ciclo. Si una conexión a un servidor x falla, el SLB marca ese servidor como no disponible por el momento, y envía la petición al siguiente servidor disponible. Este método garantiza igualdad de las carga en cada servidor.

**9.1.3.- Weighted:** Se asigna un peso de desempeño a cada servidor. Esta métrica es similar al *Least connections*, con la diferencia que los servidores con los mas altos pesos, recibirán mas conexiones en un tiempo determinado.

En esta configuración se debe asignar un peso a cada servidor real y esto determinará el porcentaje de conexiones que serán asignadas a cada servidor.

Ejemplo:

Weight server1 = 7

Weight server2 = 8

Weight server3 = 2

Weight server4 = 2

Weight server5 = 5

Total weight de todos los servers = 24

Como resultado de esto el Server 1 recibirá el 7/24 de número de sesiones activas.

**9.1.4.- Server Response Time Only:** Su funcionamiento se basa en direccionar la conexión al servidor con mejor tiempo de respuesta, es decir el más rápido. El cálculo del tiempo de respuesta de cada servidor se basa en paquetes TCP SYN y TCP SYN/ACK. Si por casualidad un servidor lento no es seleccionado por más de un minuto, el SI (Server iron) lo selecciona para poder calcular su tiempo de respuesta.

**9.1.5.- Least connection and server response time *weights*:** Se basa en una combinación de ambas métricas. El uso de la métrica *Server Response Time* por si sola, selecciona el servidor con mejor tiempo de repuesta, si todos los servidores tienen similares características, el resultado será un balanceo de la carga parejo en toda la granja de servidores. Si embargo si la granja de servidores tiene características de desempeño diferentes en cada servidor, es decir tiempo de respuestas diferentes en cada servidor, es de gran ayuda poder asignar un peso a cada servidor según su tiempo de respuesta esperado. El tiempo de respuesta default es weight 0, es decir no tiene peso asignado, se pueden especificar pesos desde 0 hasta 65000.

**9.1.6.- Least local connections:** El SI (Server iron) selecciona el servidor con la conexión mas reciente con el cliente, este cálculo se realiza en el WSM CPU y este CPU administra las conexiones que son cursadas por cada slot del chasis, hacia los servidores reales. El SI selecciona el servidor real con el con la mas reciente conexión con el cliente.

**9.1.7.- Least local session:** En un WSM CPU básico, el SI selecciona el servidor con la sesión activa más reciente en el WSM CPU conectada con el servidor real. El número de sesiones es actualizado cuando las entradas de las sesiones son borradas.

#### **IV.9.2.- Métrica Seleccionada Para la Solución.**

El tipo de métrica seleccionada en la solución para el balanceo de la carga es ***Round Robin***. Al ser todos los servidores Web de similares característica de



desempeño, se eligió esta métrica para una distribución equitativa de la carga en todos los servidores. Sin embargo se le activo el parámetro al SI para que una vez establecida la sesión de un cliente con un servidor, el SI direcciona el resto de las sesiones hacia el mismo servidor de tal forma, que la conexión real del cliente se mantenga y termine con un solo servidor real.

## Pantallas de Configuración

La configuración del SLB se puede apreciar en las siguientes pantallas:

The screenshot displays the Foundry Networks Device Management interface in Microsoft Internet Explorer. The left sidebar shows a tree view with 'SLB' expanded, and 'Real Server' selected. The main content area shows a table titled 'Real Server' with the following data:

Server Name	Server IP	Maximum Connections	Least Connections Weight	Host Range	Source NAT	Remote	
Web1	172.26.25.61	1000000	0	1	No	No	Delete Modify
Web 2	172.26.25.62	1000000	0	1	No	No	Delete Modify
Web 3	172.26.25.63	1000000	0	1	No	No	Delete Modify
Web 4	172.26.25.64	1000000	0	1	No	No	Delete Modify

The interface also shows a taskbar at the bottom with the Start button, several open applications (CAPÍTULO IV - Mi..., Adobe Reader, Foundry Network...), and the system tray showing the time as 11:27 a.m.

Foundry Networks Device Management - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Dirección

Foundry Networks

- Internet
  - QOS
  - VLAN
    - Port
    - Protocol
  - STP
  - Trunk
  - Static Station
  - SLB
    - General
    - Backup
    - Bind
    - Real Server
    - Real Server Port
    - Router Interface
    - Source IP
    - TCP/UDP Port
    - Virtual Server
    - Virtual Server Port
  - TCS
  - FWLB
  - NAT

### Bind

Virtual Server Name	Virtual TCP/UDP Port	Real Server Name	Real TCP/UDP Port	
IAS	HTTP	web1	HTTP	Unbind
IAS	HTTP	web2	HTTP	Unbind
Virtual Server Name	Virtual TCP/UDP Port	Real Server Name	Real TCP/UDP Port	

[Add Bind]

[Virtual Server][Virtual Server Port][Real Server][Real Server Port]

[Home][Site Map][Logout][Save][Frame Enable/Disable][TELNET]

Listo Internet

Inicio CAPÍTULO IV - Mi... Adobe Reader - [...] Foundry Network... ES 11:27 a.m.

Foundry Networks Device Management - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Dirección

Foundry Networks

- Internet
  - QOS
  - VLAN
    - Port
    - Protocol
  - STP
  - Trunk
  - Static Station
  - SLB
    - General
    - Backup
    - Bind
    - Real Server
    - Real Server Port
    - Router Interface
    - Source IP
    - TCP/UDP Port
    - Virtual Server
    - Virtual Server Port
  - TCS
  - FWLB
  - NAT

### Real Server

Server Name	Server IP	Maximum Connections	Least Connections Weight	Host Range	Source NAT	Remote	
Web1	172.26.25.61	1000000	0	1	No	No	Delete Modify
Web 2	172.26.25.62	1000000	0	1	No	No	Delete Modify
Web 3	172.26.25.63	1000000	0	1	No	No	Delete Modify
Web 4	172.26.25.64	1000000	0	1	No	No	Delete Modify
Server Name	Server IP	Maximum Connections	Least Connections Weight	Host Range	Source NAT	Remote	

Listo Internet

Inicio CAPÍTULO IV - Mi... Adobe Reader - [...] Foundry Network... ES 11:27 a.m.

Las sesiones activas en cada servidor ser pueden ver aquí.

The screenshot shows the Foundry Networks Device Management web interface in Microsoft Internet Explorer. The browser address bar shows the URL `http://172.26.24.2 /Home`. The left sidebar contains a tree view of network configuration options, with 'Real Server' selected. The main content area displays a table titled 'Real Server' with columns for Server Name, IP, State, Current Session, Connection (Current, Peak, Total), Pkts (Rx, Tx), and Bytes (Rx, Tx). Below the table, there are navigation links for statistics and management actions.

Real Server										
Server		State	Current Session	Connection			Pkts		Bytes	
Name	IP			Current	Peak	Total	Rx	Tx	Rx	Tx
web1	172.26.25.61	active	150	74	1477	15292072	203845356	176319644	171344344074	331
web2	172.26.25.62	active	170	84	3027	18819275	0	0	0	0
web3	172.26.25.63	active	0	0	1537	207569	0	0	0	0
web4	172.26.25.64	active	0	0	61	1353	8419	8178	1417230	12

Statistics:General|Virtual Server|Virtual Server Port|Real Server|Real Server Port

[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

La configuración para el balanceo de carga se puede apreciar aquí, mediante el método de Round Robin:

The screenshot shows the Foundry Networks Device Management interface in Microsoft Internet Explorer. The left sidebar displays a tree view of configuration options, with 'Virtual Server' selected under the 'SLB' (Server Load Balancing) section. The main content area displays the configuration for a Virtual Server named 'IAS' with IP '172.26.25.50'. The configuration is summarized in the following table:

Server		Metrics	Symmetric						Connection	
Name	IP		Group	State	Priority	Keep	Activates	Inactive	Current	Total
IAS	172.26.25.50	Default (Round_Robin)	1	1	0	0	0	0	103	0

Below the table, there are navigation links: [\[Home\]](#), [\[Site Map\]](#), [\[Logout\]](#), [\[Save\]](#), [\[Frame Enable/Disable\]](#), and [\[TELNET\]](#). The status bar at the bottom indicates the time as 02:20 p.m.

#### **IV.10.- Configuración de los Enlaces VPN**

En la solución implantada se utilizaron configuraciones basadas en políticas que básicamente se fundamenta en lo siguiente:

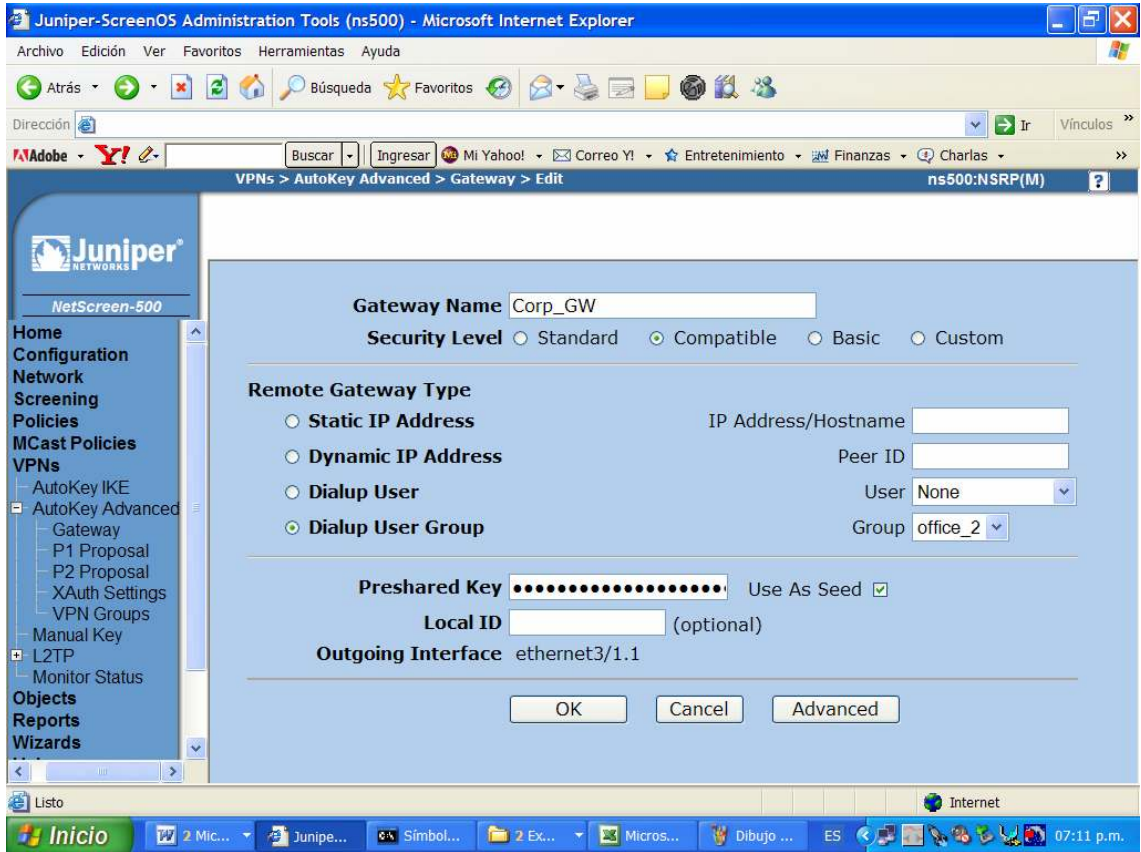
**10.1- VPN (Basadas en Políticas):** Una Policy lookup determina cual tráfico debe ser encapsulado, es decir cuándo la política es ejecutada entonces la acción a ejecutar es establecer el túnel VPN.

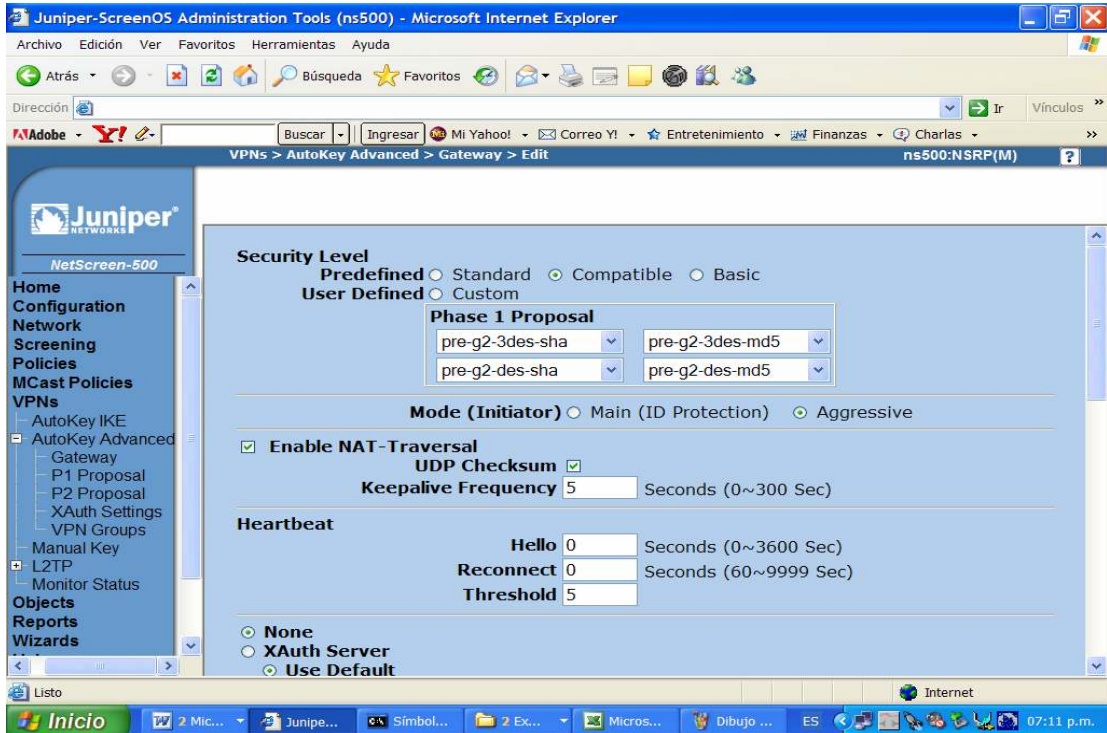
Las VPN se utilizarán para establecer canales de comunicación seguros, con los aliados de negocio y el personal de la empresa que por razones de trabajo necesiten movilidad dentro del territorio nacional o desde cualquier parte del mundo.

Aquí se pueden apreciar las pantallas de configuración.

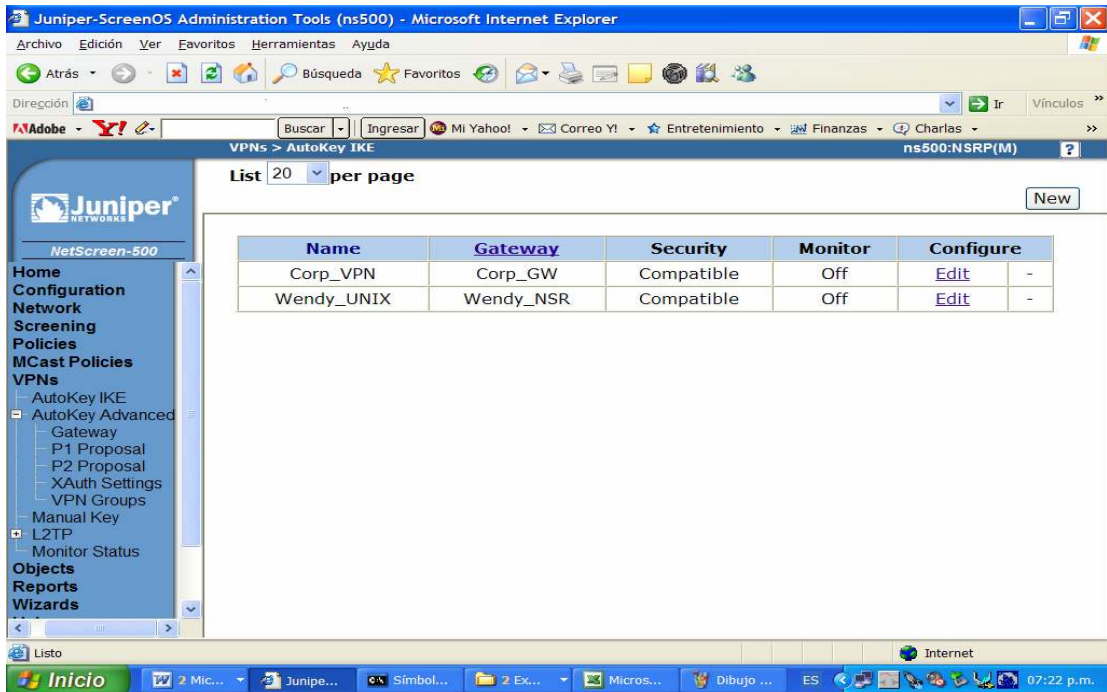
Primero se configuran los Gateway y en ellos se establecen los parámetros siguientes:

- Algoritmos de hash y encriptación para la fase 1 y fase 2
- Niveles de seguridad
- En el caso de utilizar una clave predefinida, se debe configurar en esta sección
- Nombre, interfaz mediante la cual se establecerá el VPN.

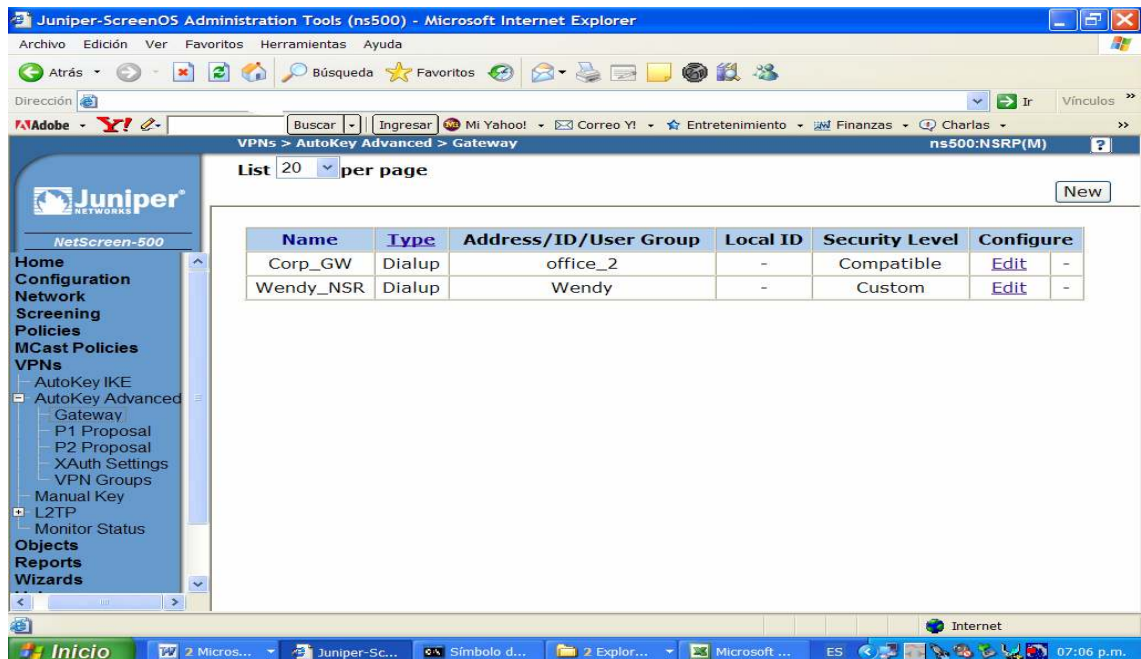
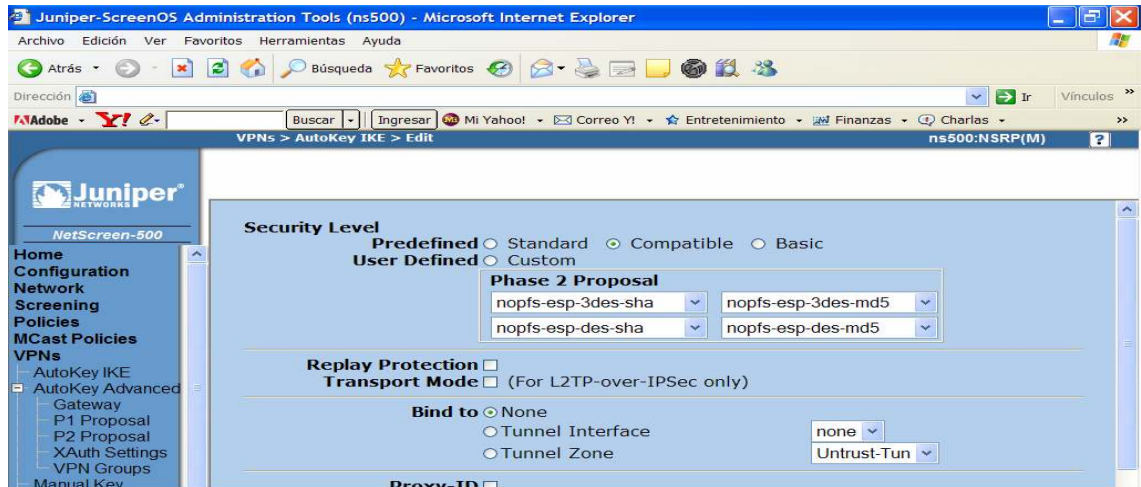




Luego se configuran el AutoKey IKE

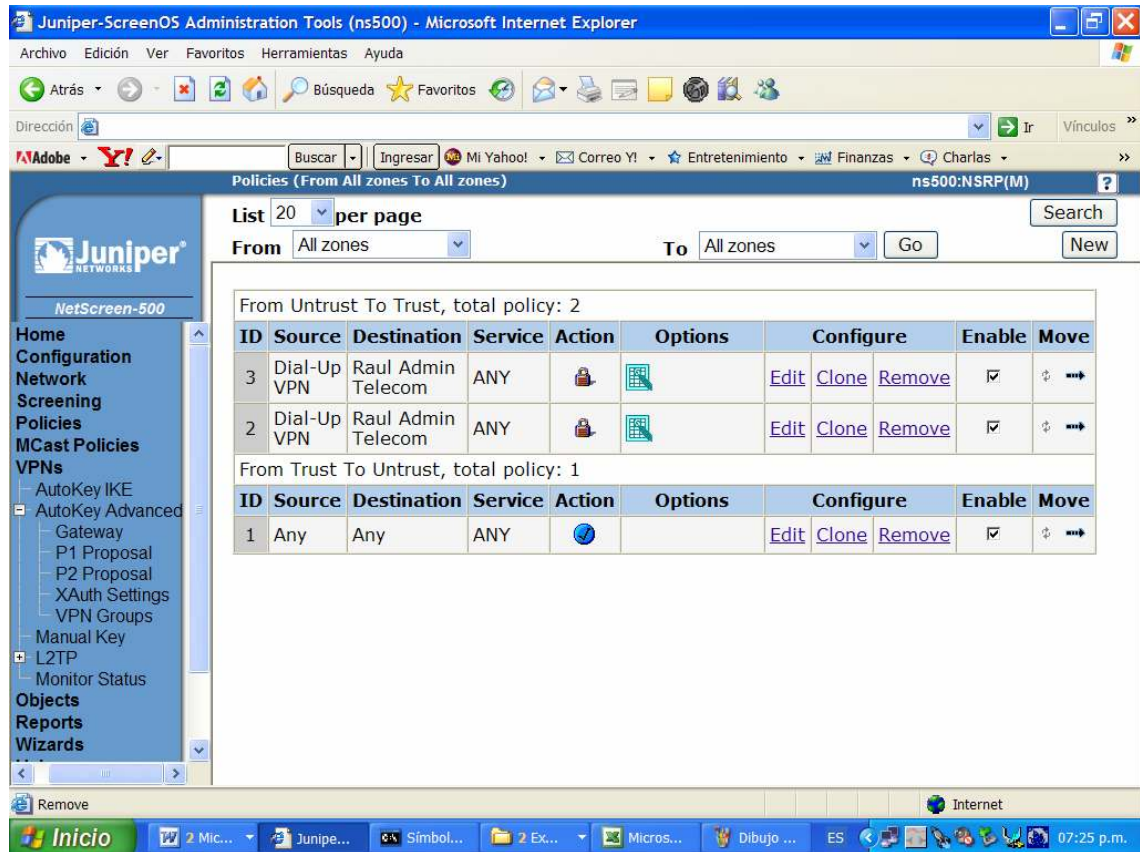


Aquí se configuran los algoritmos de fase 2





Luego como etapa final se configuran las políticas, mediante las cuales se establecerán los túneles VPN.



#### IV.11.- Alta Disponibilidad de los Equipos Firewall

La solución contempla el funcionamiento de los equipos de seguridad firewall, en configuraciones activo pasivo, en la cual todas las sesiones, configuraciones, políticas, alarmas, eventos, etc. Son replicados desde el master al esclavo, permitiendo que si ocurre cualquier falla, el dispositivo en estado pasivo pueda tomar el control, de manera totalmente transparente para la red.

### **11.1- Confiabilidad**

Los equipos utilizados en la implantación de la solución tiene categoría Carrier Class, para garantizar niveles de disponibilidad del orden de 99.999%. Por último, se implementará un sistema de redundancia con las especificaciones que son descritas en el siguiente punto.

### **11.2- Escalabilidad**

Esto implica que los dispositivos y equipos involucrados en la implantación de la solución deben ser fácilmente modificables para proporcionar anchos de bandas mayores, mayor poder de procesamiento con esquemas de cluster, activo o activo pasivo, y adaptarse a las tecnologías emergentes que puedan garantizar el soporte de requerimientos futuros y de mayor funcionalidad.

En concordancia con esto, la solución planteada proporciona una base adecuada para la futura migración hacia nuevas tecnologías, manteniendo en un alto grado de seguridad en el esquema actual de seguridad y dejando paso para un proceso de cambios lo menos traumático posible, tanto en el aspecto tecnológico como en lo económico.

### **11.3- Sistema de Monitoreo, Control y Gestión de Fallas**

Como mecanismo de gestión y administración de los dispositivos, la solución plantea centralizar este proceso apoyándose en la capacidad de los equipos de generar y transmitir información en referencia a su estado actual, tráfico,

sesiones, ataques, alarmas, alertas y mucha más información importante para la gestión de la seguridad. Dicha información será procesada por una aplicación de manera gráfica, mediante la cual se puede observar y monitorear el estado actual de todas las comunicaciones cursadas a través de todas las zonas de seguridad del los firewall. De esta forma el monitoreo y administración de estos dispositivos se simplifica y se hace más proactivo, en lugar de reactivo. También permitirá realizar esquemas de correlación de eventos de manera de detectar ataques complejos a la infraestructura.

A su vez un esquema de monitoreo compartido con las dos empresas ISP permitirá llevar un control, monitoreo y administración de todo el ancho de banda disponible para la plataforma del Portal Web, el cual es el eje principal en toda la modernización tecnológica de la empresa.

#### **IV.12.- Plan de Implantación**

##### **12.1.-Migración**

En esta etapa se contemplaron una serie de actividades destinadas a coordinar la migración paulatina desde el esquema actual de zonas de seguridad hacia la nueva arquitectura de 9 zonas de seguridad.

Entre estas actividades se encuentran las siguientes:

- Se ejecutó el control de cambios para cada servicio, para ubicarlo en su respectiva zona de seguridad, cambio de direccionamiento IP, incorporación de los nuevos servicios, servidores y protocolos utilizados.

- Se realizó un levantamiento de información y control de cambios con el personal del área de redes, para determinar los cambios exactos necesarios en el direccionamiento IP y configuraciones de los equipos de comunicaciones, Ras, Concentradores de VPN, y sus respectiva reubicación física según el nuevo esquema de seguridad.
- Se realizó la migración en forma paralela, de cada servicio en horario no laboral de tal forma de no impactar la continuidad operativa de las aplicaciones de la empresa. Para esto se hicieron migraciones semanales de los servicios uno a uno en conjunto con las áreas involucradas, es decir la banca nacional, aliados de negocios, clientes extranet, etc, así como también las áreas internas de la empresa.
- Pruebas de funcionamiento y entonación de la solución.
- Pruebas integrales junto con el personal de los aplicativos.
- Pruebas de Failover.
- Pruebas de Penetración por parte del personal interno de seguridad de la empresa.

## **12.1.- Asignación de Recursos**

Para la ejecución de este plan de implantación se requirió de la conformación de un grupo de trabajo multidisciplinario integrado por cinco grupos especializados en diversas áreas de la empresa. También se necesitó la colaboración y asesoría de la empresa integradora de soluciones y el proveedor de la tecnología de seguridad adquirida. El Gerente de Seguridad de la empresa será el encargado de la coordinación general del proyecto en sí.

***Aplicativos de Negocio:*** El primero de ellos está formado por especialistas en las aplicaciones de negocio utilizadas actualmente para el manejo de las operaciones inherentes a la gestión de negocio de la empresa. Las responsabilidades de este grupo están enfocadas a mantener el correcto funcionamiento de las aplicaciones en el proceso de integración con la nueva plataforma de seguridad.

***Redes:*** El segundo grupo lo conforman especialistas en arquitecturas de redes WAN y LAN y protocolos TCP/IP. Este grupo velará por el debido funcionamiento de los equipos que conforman estas plataformas, así como por la interconexión con los equipos existentes y su interoperabilidad.

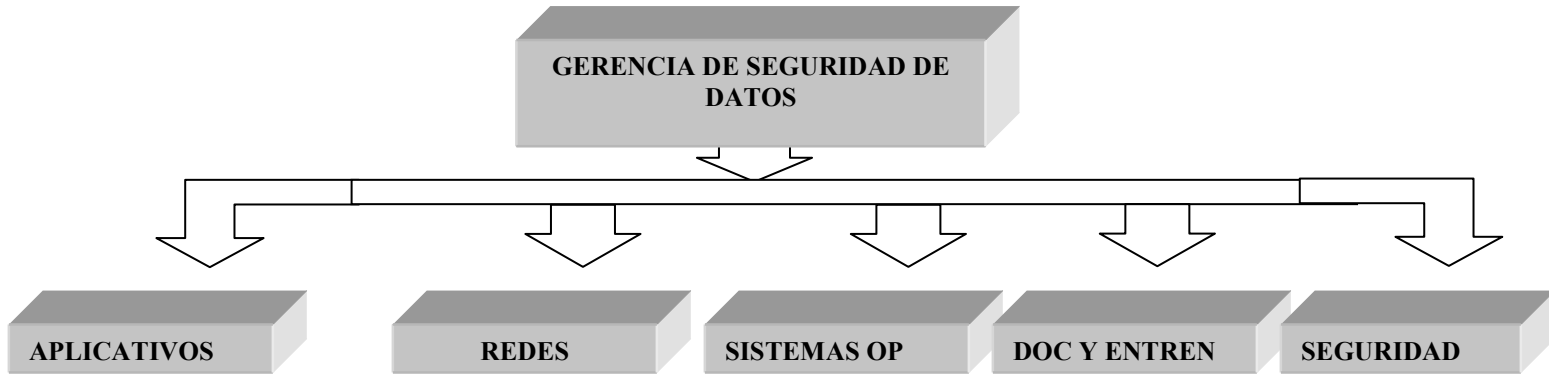
***Sistemas Operativos:*** El tercer grupo estará formado por especialistas en el área de sistemas operativos, y tendrá como responsabilidad principal todo lo referente a la configuración y puesta a punto de todos los sistemas operativos de los servidores donde van a correr las aplicaciones de negocio de la empresa.

**Documentación de Aplicaciones y Entrenamiento:** El cuarto grupo estará compuesto por especialistas en el área de entrenamiento, aplicaciones y

documentación de sistemas. Entre sus responsabilidades principales está la de actualizar y generar la documentación de las aplicaciones y herramientas de oficina. Proporcionar entrenamiento para la utilización de las nuevas funcionalidades de los sistemas a ser implantados.

**Seguridad:** Finalmente el quinto grupo formado por los especialistas en el área de seguridad de datos y seguridad de redes.

En el siguiente diagrama se puede ver la conformación del grupo multidisciplinario.



## **CAPITULO V**

### **CONCLUSIONES Y RECOMENDACIONES**

#### **V.1.- Conclusiones**

La seguridad perimetral como estrategia para controlar el acceso a todos los recursos y sistemas de negocio en las empresas se ha convertido en un tema prioritario y de vital importancia ya que involucra el uso de nuevas plataformas tecnológicas, lo que implica muchas veces una gran inversión de recursos económicos, y recursos humanos, todo con un mismo fin de proteger la integridad, autenticidad y confidencialidad de la información. Esta inversión debe estar acompañada de un estudio y un análisis técnico económico, previamente a la definición de un plan estratégico migración o implantación de un esquema de seguridad perimetral.

La implantación de la nueva plataforma de seguridad para la protección de todos los activos informáticos de la organización y de sus sistemas de negocio, ha permitido actualizar toda la plataforma de seguridad perimetral de redes. A través de esta nueva arquitectura la empresa podrá garantizar niveles de protección adecuados, en todas las zonas de seguridad, utilizando para tal efecto un arreglo en alta disponibilidad de firewalls de alto desempeño, con categoría carrier class.

Esta nueva plataforma de seguridad es la columna vertebral sobre la cual se sustenta todo el sistema de comunicaciones y la protección de todos los sistemas de negocio informáticos de la empresa.

En la evaluación y selección de la solución final de firewall y su implantación como corazón de la nueva arquitectura de seguridad en la red de datos de la empresa, es importante destacar varios aspectos y criterios que se tomaron en cuenta, partiendo como base las necesidades de la organización. Entre otros tenemos:

- Robustez, confiabilidad y desempeño, se necesitaban equipos con categoría Carrier Class, debido al tamaño de la red de la empresa y al gran volumen de información que se maneja.
- Soporte y garantía de la solución por parte del representante de la empresa fabricante en el país.
- Costos de adquisición

Para la organización el mayor peso en la matriz de evaluación, no lo tenía el factor costo, si no las bondades tecnológicas, factor seguridad, alto desempeño y demás ventajas que le brindaría a la organización la utilización de tecnología de punta escalable con respaldo en el país.

Adicionalmente a la implantación de las zonas de seguridad, cabe destacar la utilización de enlaces VPN utilizando como medio de comunicación el acceso de Internet, ofreciendo la gran ventaja de permitirles a los usuarios una conexión segura y estable a través de un túnel en donde la información viajará encriptada entre la red privada interna y la red pública (Internet). También se activaron servicios de balanceo de carga para el portal de servicios Web de la corporación, mediante la utilización de equipos Server Iron Capa 7, mediante la cual todo el tráfico Web dirigido hacia la granja de servidores Web, es balanceado, garantizando un excelente tiempo de respuesta y alta disponibilidad del servicio.



Se puede concluir que la seguridad de una red no se basa en una única técnica exclusiva de adquisición e instalación de un firewall, sino que debe venir complementada con la definición estratégica de políticas de seguridad que permitan gestionar cada uno de los aspectos críticos de la red. Pero sobre todo debe haber voluntad desde lo más altos estratos de tren gerencial para hacer cumplir las normas y políticas de seguridad en el resto de la organización.

## **V.2.-Recomendaciones**

La seguridad no depende única y exclusivamente de la implantación de esta nueva plataforma de seguridad perimetral, ya que es indispensable mantener un óptimo nivel de protección de la información en todos sus niveles, actualizando las normas, procedimientos y políticas de acuerdo a la dinámica en que vayan surgiendo nuevas estrategias de ataque contra las redes y sus activos de información. El compromiso de la alta gerencia para el cumplimiento de todos estos factores de seguridad es vital.

Para lograr blindar aun más la seguridad en la organización se debe tomar en cuenta los siguientes factores de suma importancia:

- Implantación de un sistema de detección y prevención de intrusos, mediante el cual se pueda realizar de manera automatizada, el control y monitoreo periódico de toda la actividad generada a través de la red de la empresa.
  
- Pruebas de penetración frecuentes: ejecución de pruebas externas que simulen posibles ataques hacia la red privada, logrando identificar de manera precisa los huecos de seguridad que puedan existir.

- La definición de un conjunto de planes de seguridad que minimicen los riesgos y brinden protección ante cualquier contingencia.
- Ejecución del contrato de soporte, mediante el cual se garantiza que todos los equipos cuenten con actualizaciones de sus sistemas operativos, cada vez que el fabricante realice mejoras de software.

## BIBLIOGRAFIAS CONSULTADAS

Manual “**Formulación y Gestión de Proyectos**”.  
Banco Interamericano de Desarrollo. 2002.

Manual “**Swith Foundry**”.

ALDEGANI, Gustavo. Miguel. (1997). *Seguridad Informática*. Argentina MP Ediciones.

AMOROSO, Edward. (1994). *Fundamentals Of Computer Security Technology*. Estados Unidos, Prentice Hall. CISCO Systems. *CISCO Networking Academies*. Curriculum Online Versión 1.1.

Chiavenato, I. (1997). *Administración de Recursos Humanos*. México: Mc Graw Hill.

ELLIS, Juanita; SPEED, Timothy. (2001). *The Internet Security Guidebook, From Planning To Development*. Estados Unidos. Academic Press.

ESSINGER, James. (2001). *Internet Trust & Security*. Gran Bretaña. Addison-Wesley.

HERNADEZ, R., FERNÁNDEZ, C., BAPTISTA, P. (1991). *Metodología de la Investigación*. México. McGraw Hill

MENDEZ, C. (1990). *Metodología*. Colombia. McGraw Hill

MENDEZ, A. (1993). *Metodología*. Colombia. Mc Graw Hill.

SCHNEIER, Bruce. *Secrets & Lies, Digital Security in a Networked World*. Wiley Computer Publishing. 1ª Edición. Estados Unidos 2000.

## INTERNET

Manual. “**Firewall Netscreen Serie 5000**

[http://www.juniper.net/techpubs/hardware/netscreen-systems/netscreen-systems50/ug\\_5000.pdf](http://www.juniper.net/techpubs/hardware/netscreen-systems/netscreen-systems50/ug_5000.pdf)

Netscree VPN Guide

[http://www.juniper.net/techpubs/hardware/netscreen-remote/nsr\\_vpn\\_installation\\_guide\\_v8\\_0.pdf](http://www.juniper.net/techpubs/hardware/netscreen-remote/nsr_vpn_installation_guide_v8_0.pdf)

<http://www.cert.org>

HUERTA, Antonio Villalón. *Seguridad en Unix y Redes*. Versión 1.2 Digital – Open Publication License v.10, 2 de Octubre de 2000. <http://www.kriptopolis.com>

[http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html)

<http://www.commoncriteria.org/docs/origins.htm>

