UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SISTEMA DE SEGURIDAD PERIMETRAL EN UNA RED EN ALTA DISPONIBILIDAD.

INFORME DE COMPETENCIA PROFESIONAL

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

ROBERT MANUEL SOTO MANRIQUE

PROMOCIÓN
2006- II

LIMA – PERÚ
2011

SISTEMAS DE SEGURIDAD PERIMETRAL EN UNA RED EN ALTA DISPONIBILIDAD.

Agradezco en primer lugar a Dios, a mis padres, a mi esposa por el apoyo constante y mi hija quien es el incentivo para seguir adelante.

SUMARIO

El presente informe trata sobre los Sistemas de Seguridad Perimetral para una red en alta disponibilidad. Se revisa los tipos de vulnerabilidades que existen, luego realizamos la clasificación en cuanto al riesgo que representa dichos ataques, puntos en las redes donde son menos seguros y sitios donde los hackers concentran sus ataques.

Habiendo identificado lo que necesitamos, se realiza el estudio del equipo que se utilizará para superar esas vulnerabilidades.

Se trabaja con equipos Firewall que nos proporcionan seguridad de acceso a los puertos, direcciones IP origen o destino que llegan hasta la capa de transporte pero se podría habilitar para que se inspeccione a un mayor nivel de seguridad. Por buenas prácticas se recomienda utilizar otro equipo para realizar esa función.

La inspección entonces llega hasta la capa de aplicación; monitoreando el trafico que pasa por la red, identificando los tipos de vulnerabilidades y categorizándolo para tener mayor consideración, además nos muestra hacia quien va el ataque (servidor, host, equipos).

Los servidores VPN son utilizados mayormente para el acceso hacia los equipos en producción, desde internet o desde la misma intranet.

Se complementa con políticas de seguridad que nos ayudan en la administración de los equipos de seguridad concientizando a los usuarios para mantenerla. Una correcta política de seguridad de eventos nos brindara el camino correcto para la gestión de incidencias.

Los servidores Proxy y antivirus son necesarios para mantener limpia la intranet de virus, troyanos, spyware, etc.

Los sistemas de monitoreo son analizados en el informe, ya que son de gran importancia para las empresas suministrar evidencias o registros que generan cada equipo.

Los equipos de monitoreo proporcionan los datos suficientes para poder prevenir las incidencias o saber porque se ha presentado.

Finalmente se detalla las diferentes topologías de red que se pueden utilizar en una solución de Seguridad Perimetral (Topología Física y Topología Lógica).

INDICE

PRÓLOGO

La falta de conocimientos y capacitación es una de las fuentes principales de riesgos de Seguridad a los que se exponen las organizaciones. La seguridad no es solamente el implementar usuarios y contraseñas, es implementar políticas que garanticen la seguridad tanto física como lógica de la información.

El activo más importante en las organizaciones públicas, privadas y de cualquier índole, es la información que se posee, entre más grande es la organización más grande es el interés de mantener la seguridad en la red, por lo tanto, es de suma importancia el asegurar la seguridad de la información, de proteger las operaciones de daños no intencionados como deliberados.

Por esta razón, el presente informe, nos revela como un activo o recurso relacionado al sistema de información, manejado de la forma eficaz, facilita las tareas de todos aquellos que se encuentran involucrados en las decisiones con respecto a la seguridad de las redes o sistemas de información y sus modos de administración. De igual manera resaltar la importancia en detectar y alertar la vulnerabilidad de un activo. Un adecuado tratamiento de esta problemática resulta absolutamente vital, ya que las amenazas cada vez son mayores a las que la información se encuentra expuesta.

Saber utilizar las ventajas del uso de la tecnología, como herramientas de auditoría de seguridad y saber cual aplicar para cada necesidad, nos ayudará a salvaguardar la información, en consecuencia reducir los riesgos de nuestra organización.

Describiremos las principales herramientas que nos permitan asegurar el perímetro de nuestra red para los accesos de nuestra intranet hacia internet y de internet hacia los servidores mediante conexiones seguras, tener monitoreado el trafico tanto entrante como saliente mediante equipos que nos brinden inspección y análisis como son los IPS, los filtros de web que nos brindarán un nivel de seguridad mayor a nuestras redes brindándonos el control de páginas que podrán visitar los usuarios de acuerdo a las políticas que se implanten en las empresas.

CAPITULO I
ANTECEDENTES

1.1 Situación inicial

El crecimiento tecnológico en el Perú y el desarrollo económico sostenido ha traído la necesidad para muchas empresas de contar con más equipos de networking que provean conectividad a nuevas áreas, nuevas sucursales o simplemente la ampliación de red en las oficinas principales. Los sistemas de protección perimetral por lo general no son tomados en cuenta para proteger a las estaciones de trabajo y servidores, los cuales llegan a ser puntos perfectos para todo tipo de ataque. En la mayoría de los casos la protección está enfocada en el acceso de puerto más no en la inspección de tráfico de red.

Por ello, en el presente informe se toma como situación inicial la topología de una empresa donde no posee un adecuado sistema de seguridad perimetral implementada.

Se cuenta con un firewall que da seguridad por puerto, más no con un equipo que brinde seguridad contra ataques hacia los aplicativos o ataques de denegación de servicios que llegan hasta la capa de aplicación según modelo OSI.

No hay un segundo dispositivo firewall como contingencia, es decir si el equipo sufre cualquier problema de hardware o software la seguridad queda vulnerable y los accesos y servicios sufren un tiempo de inactividad.

No se cuenta con un servidor correlacionador de eventos, donde nos puede mostrar en tiempo real que sucede en la red o un sistema de monitoreo que nos ayude a verificar el estatus de cada dispositivo.

En el siguiente grafico se muestra la topología que se describe en esta situación inicial. Ver Fig. 1.1

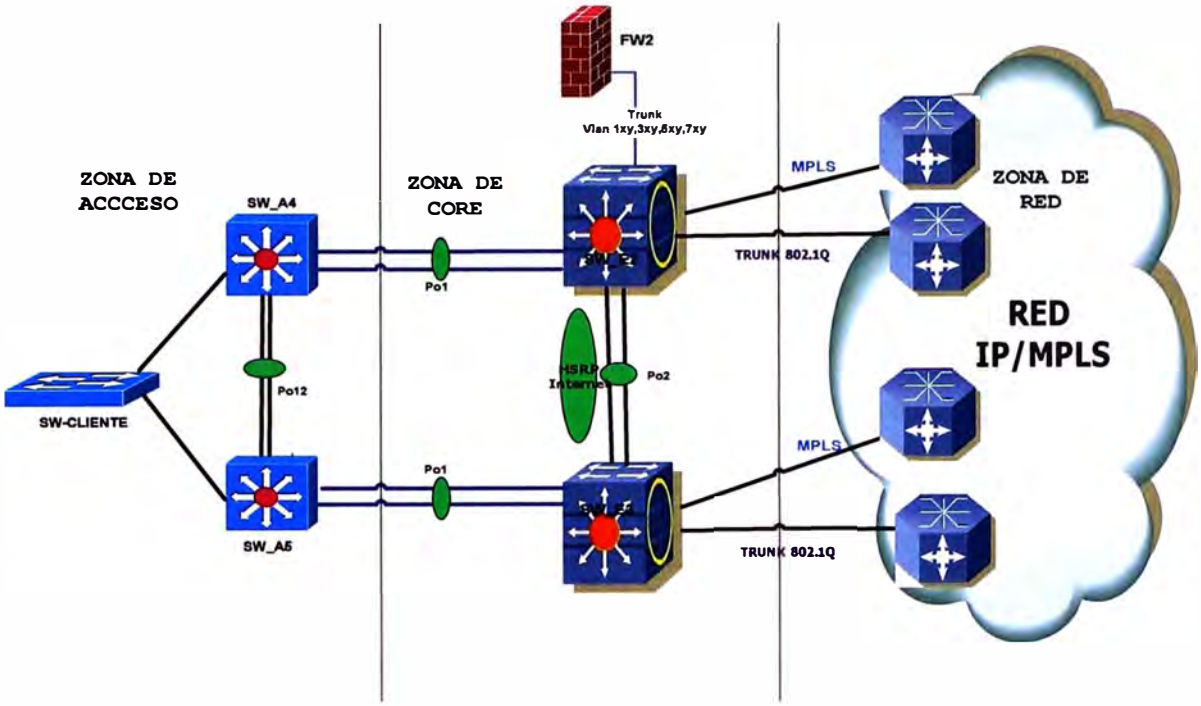

Fig. 1.1 Topología Inicial

1.2 Objetivos

a) Establecer los criterios para conseguir estabilidad y disponibilidad de redes garantizando el correcto funcionamiento de los sistemas de información y el acceso a los servicios que toda empresa necesita para su normal operatividad, manteniendo el perímetro de la red segura implantando políticas de seguridad que ayudará a contrarrestar cualquier ataque o vulnerabilidad.

b) Determinar las políticas para centralizar el control de acceso en dispositivos de red y mantener una administración gestionable de las políticas que se brinda a cada usuario.

c) Identificar las herramientas de monitoreo para las redes seguras que nos permitan saber que está pasando en la red mediante registros claros y detallados, para la detección inteligente de equipos o usuarios que pudieran ocasionar intencionalmente o no, daños a la empresa.

d) Brindar una guía de ayuda para las empresas que deseen implementar seguridad perimetral en sus redes, teniendo como modelo las topologías utilizadas en este informe.

1.3 Alcances

Se propone un sistema de seguridad perimetral con alta disponibilidad para redes empresariales. El tema se centra en la importancia de mantener segura la información y los servicios estables, brindando el acceso a los equipos de acuerdo a las funciones en la

empresa.

Los tipos de vulnerabilidades de la empresa que se producen por los accesos a internet y los que se generan desde la misma red local, podremos conocerlos y clasificarlos de acuerdo a los niveles de riesgos y amenazas. El nivel que alcanzará el sistema de seguridad perimetral, sería hasta la capa de aplicación del modelo OSI, con equipos como: Sistemas de Prevención de Intrusos (IPS), Sistemas de Detección de Intrusos (IDS) o Stateful Firewall.

La estabilidad de los servicios en el sistema de seguridad desarrollado, propone la alta disponibilidad en dispositivos de redes, mediante el cual el servicio no presentará tiempo de inactividad muy prolongado.

1.4 Estructura del Informe

En el primer capítulo presentamos la topología de una empresa, con inadecuada sistema de seguridad, esta vulnerabilidad se indica en la Situación Inicial, una vez encontrado los puntos a resolver nos proponemos los Objetivo del Informe. En el segundo capítulo daremos a conocer la "Administración de Riesgos en Redes Empresariales LAN", en el tercer capítulo ampliaremos el concepto de seguridad perimetral en redes LAN, el cuarto capítulo "Gestión y Administración de eventos en una Red Segura". El ultimo capitulo es la "Ingeniería del Proyecto" donde graficamos los diferentes tipos de topologías de la red.

Se agregan anexos de reportes de continuidad del servicio, descripción de los dispositivos a utilizar y los tipos de Organizaciones Internacionales de seguridad.
Finalmente se lista el material utilizado dentro de la bibliografía.

CAPITULO II
ADMINISTRACION DE RIESGOS EN REDES EMPRESARIALES LAN.

2.1 Valor y Clasificación de la Información en Redes.

El principal bien de las empresas es la información y por lo tanto es el principal bien a proteger en medida que su pérdida afecte a la empresa u organización.

La clasificación de la información define el diseño del sistema de seguridad al poner en orden de prioridades los bienes a proteger, y por lo tanto, el nivel de inversión sobre cada parte del sistema. La clasificación define incluso el nivel de prioridad que tiene en la organización.

De esta manera, el valor de la información entra a tallar el flujo de la misma. Si el bien fluye de un lado a otro, el camino que recorre también debe ser protegido y el medio de transporte lógico debe ser seguro.

Krutz y Vines[1] describen el tipo de información para las empresas de la siguiente manera:

a) Pública.- Cualquier información no incluida en las categorías de sensible, privada y confidencial, y cuya obtención o divulgación no afecta a la organización.

b) Sensible.- Información que requiere un mayor nivel de clasificación que el normal. relacionado con la confidencialidad.

c) Privada.- Información que es considerada de una persona natural y para uso de la compañía solamente. Por ejemplo, encuestas, evaluaciones de trabajo, etc.

d) Confidencial.- Información muy sensible y de uso interno únicamente. Por ejemplo, campañas comerciales, base de datos de clientes, etc.

2.2 Amenazas, Vulnerabilidades y Riesgos

La información y otros componentes del sistema están siempre bajo la amenaza de ser atacados por agentes tanto externos como internos quienes tratarán de aprovecharse de las vulnerabilidades del sistema y por ello siempre existirá un nivel de riesgo. El nivel de riesgo mide el grado de seguridad de una organización basado en las vulnerabilidades, el valor de la información y la probabilidad de ser atacados (amenazas) al momento de

efectuar el análisis

Este factor define el nivel de fortaleza y debilidad de cada uno de los componentes de todo el sistema, por ello es importante establecer políticas de seguridad que van desde el monitoreo de la infraestructura de red, hasta el reconocimiento de las propias necesidades de seguridad.

2.2.1 Amenazas

Cualquier evento que ocasione incidencias, produciendo daños materiales o inmateriales sobre un activo de la organización. Se suelen dividir las amenazas que existen sobre los sistemas informáticos en tres grandes grupos:

a) Desastres del entorno: Se han de tener en cuenta desastres naturales (terremotos, inundaciones), cortes de fluido eléctrico, y peligros relacionados con operadores, programadores o usuarios del sistema.

b) Amenazas en el sistema: Bajo esta denominación se contemplan todas las vulnerabilidades de los equipos y software que pueden acarrear amenazas a la seguridad, como fallos en el sistema operativo, fallos en los programas, etc.

La figura 2.1 muestra la cantidad de amenazas que se pueden producir en la red local de una empresa en el periodo de un mes. Las amenazas que se analizan son: virus, malware, troyanos, etc.

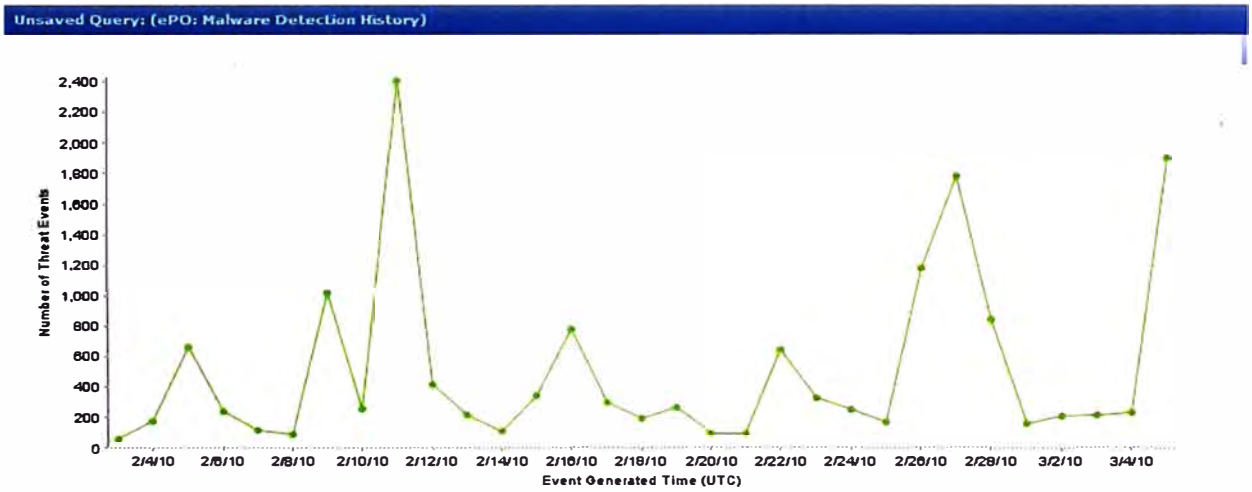

Fig 2.1 Eventos de virus VS Tiempo

c) Amenazas en la red: Cada día es menos común que una máquina trabaje aislada de todas las demás; se tiende a comunicar equipos mediante redes locales, intranets o el propio internet, por ejemplo, es necesario analizar aspectos relativos al cifrado de los datos en tránsito por la red o instalar sistemas de autenticación de usuarios remotos.

2.2.2 Vulnerabilidades

En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

Las vulnerabilidades se descubren muy seguidas en grandes sistemas, y el hecho de que se publiquen rápidamente por todo internet (mucho antes de que exista una solución al problema), es motivo de debate. Mientras más conocida se haga una vulnerabilidad, más probabilidades de que existan piratas informáticos que quieren aprovecharse de ellas.

2.2.2.1 Definición de niveles de Vulnerabilidad.

a) Extremadamente crítico: Son aquello que pueden comprometer el sistema. Y son activamente explotadas (o los "exploits" están disponibles públicamente).

b) crítico: En este caso no hay "exploits" conocidos disponibles en el momento de su divulgación.

c) Moderadamente crítico: Son de tipo denegación de servicio (DoS) que comprometen al sistema y requieren interacción con el usuario. En redes LAN servicios como SMB, RPC, NFS, etc. (no diseñados para Internet).

d) Menos crítico: Tenemos los "cross-site scripting" y de privilegios escalables. Permiten la exposición de información sensible a usuarios locales (sin privilegios).

e) No crítico: Se caracterizan por tener privilegios muy limitados y denegación de servicios localmente explotables.

La figura 2.2 muestra la evolución de vulnerabilidades en los sistemas operativos de Microsoft (Windows XP y Vista) tomando como muestra los 50 software más utilizados por Windows [2].

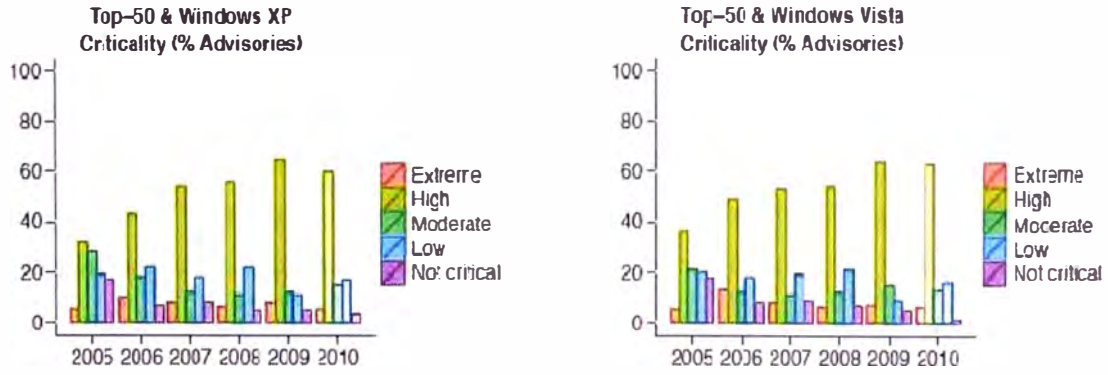

Fig 2.2 Evolución de las vulnerabilidades en S.O. Microsoft Fuente: secunia.com

2.2.3 Riesgos

Es la posibilidad de que se produzca un impacto determinado en la organización. En el área de informática existen varios riesgos tales como: ataque de virus, códigos maliciosos, gusanos, caballos de Troya y hackers; no obstante, con la adopción de internet como instrumento de comunicación y colaboración, los riesgos han evolucionado, ahora las empresas deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

De los informes semanales y reportes de amenazas realizados en DataCenter se obtuvo un reporte estadístico de los riesgos más comunes que se presentan en las desktop de los usuarios. (Véase la Fig. 2.3)

45%	Threat Type not available
31%	app_puocookie
14%	Virus
8%	Trojan
2%	Malware

Fig2.3 Top de Riesgos

2.3 Metodología y Tipos de Ataques en Redes.

Hay muchos tipos de ataques de red que no son virus, gusanos y troyanos. Para conocer los ataques, es conveniente saber los distintos tipos de ataques por categorías y su funcionamiento. Definiendo las vulnerabilidades, es posible hacerle frente para contrarrestarlo, más cuando se da en ataques individuales. No hay una forma estándar de categorización de los ataques de red, por lo que describiremos en tres formas:

a) Ataques de Reconocimiento.

b) Ataques de Acceso.

c) Denegación del Servicio.

2.3.1 Ataque de Reconocimiento.

Los ataques de reconocimiento implican el descubrimiento no autorizado y la cartografía de los sistemas, servicios o vulnerabilidades. Reconocimiento de los ataques a menudo emplean el uso de packet sniffers o port scanners, que están ampliamente disponibles como descargas gratuitas en Internet.

En un ataque de reconocimiento, el intruso malintencionado suele comenzar por la realización de un ping sweep de la red de destino para determinar qué direcciones IP están habilitadas.

Nmap es la aplicación más popular para la realización de los escaneos de puertos. De la información obtenida, el intruso consulta los puertos para determinar el tipo, versión de la aplicación y el sistema operativo que se ejecuta en el host destino. En muchos casos, los intrusos buscan servicios vulnerables que pueden ser explotados más tarde, cuando hay menos probabilidad de ser descubierto [3].

Nombramos los tipos de Ataques de Reconocimientos:

a) Packet sniffers

b) Ping sweeps

c) Port scans

a) Packet Sniffers.- Ataque que logra el descubrimiento de contraseñas y usuarios enviados en texto plano, además de información no autorizada. Se utiliza como herramienta para análisis de fallos para descubrir problemas en la red, por ejemplo cuando un ordenador A no puede establecer comunicación con el ordenador B.

b) Ping Sweeps.- Es un tipo de ataque que se utiliza para realiza un escaneo de red básica y descubrir que host están activos. Un ping sweep consiste de ICMP eco requests enviadas a varios host. Si una dirección dada esta activa, la dirección devuelve una respuesta de ICMP eco reply . Los ping sweep están entre los métodos más antiguos y lentos utilizados para escanear una red.

c) Port Scans.- Es un ataque típico de reconocimiento que es utilizado para escanear puertos, direcciones IP y activos en la red. Además de mostrar qué puertos están abiertos también sirve para obtener información sobre servicios HTTP, FTP, SMTP, SNMP y SMB. La fig. 2.4 muestra los tipos de ataques de reconocimiento, tomando como ejemplo el ataque Port Scans con un software para escaneo de puertos llamado NMAP que está disponible tanto en software libre como Windows.

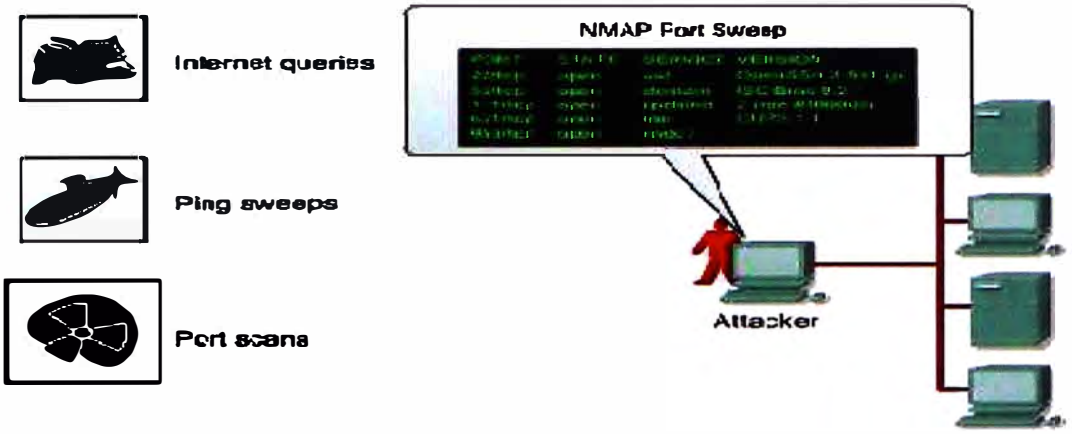

Fig 2.4 Tipos de ataque de Reconocimiento Fuente: www.cisco.com

2.3.2 Ataques de Acceso.

Los hackers usan ataques de acceso en las redes o sistemas por tres razones: recuperar datos, tener acceso y escalar privilegios de acceso.

Los ataques de acceso a menudo emplean ataques de contraseña para adivinar los password de los sistemas. Los ataques de contraseña pueden ser puestos en práctica usando varios métodos, incluso ataques de fuerza bruta, programas de Caballo de Troya, IP spoofing. Sin embargo, la mayor parte de ataques de contraseña se refieren a ataques de fuerza bruta, que implican tentativas repetidas basadas en un diccionario incorporado para identificar una cuenta de usuario o password[3].

Los tipos de ataques de acceso son:

a) Fuerza Bruta.- Ataque que logra obtener acceso a recursos mediante el rompimiento de la clave de acceso a ese recurso. A través del ensayo de prueba y error se ingresan los datos de una cuenta y una clave de acceso en texto claro. Un ataque típico es identificar la clave de una cuenta de algún servicio.

b) Main-in-the-middle.- Ubicación de un usuario o programa en medio de una sesión tomando control de ésta y haciéndoles creer a los usuarios que ellos están conectados directamente con los recursos y/o servicios.

Para evitar este tipo de ataques hay que monitorear constantemente los sistemas para evitar el uso de herramientas hostiles.

c) Port Redirection.- Un sistema comprometido es usado como un punto de partida para ataques contra otros objetivos. Una herramienta de intrusión se instala en el sistema comprometido para el re direccionamiento de la sesión.

d) Trust Exploitation.- Un atacante utiliza los privilegios concedidos a un sistema en una

forma no autorizada, que posiblemente lleve a comprometer el objetivo.

e) Buffer OverFlow.- Un programa escribe datos más allá de la memoria búfer asignado. Desbordamientos de búfer suclen surgir como consecuencia de un error en un programa en C o C + +. Un resultado de la inundación es que los datos válidos se sobrescribe o a fin de permitir la ejecución de código malicioso

La figura 2.5 muestra un ejemplo de ataque buffer overflow errores de RTD (Real Time Distributor), producido hacia un equipo de telefonía.

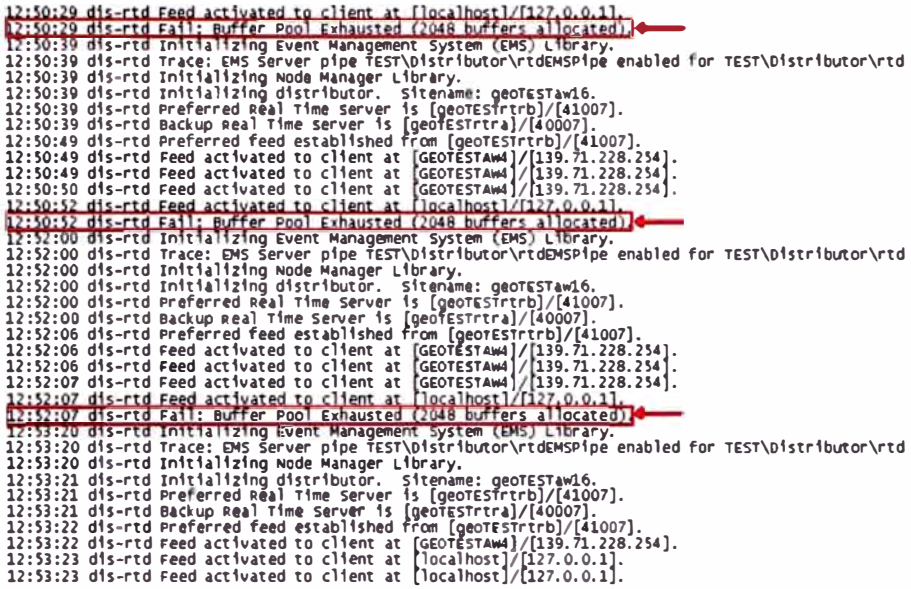

Fig 2.5 Ataque de Acceso Buffer OverFlow

2.3.3 Denegación de Servicio.

Los ataques de tipo DOS se dan con el objetivo de dejar fuera de acceso a determinados servidores, estaciones o incluso al mismo switch.

Los ataques de DOS intentan comprometer la disponibilidad de una red, hosts, o aplicación. Ellos son considerados un riesgo principal porque pueden interrumpir fácilmente un proceso comercial y causar una pérdida significativa. Estos ataques son relativamente simples de realizar, hasta por un atacante no calificado.

Tenemos 3 tipo de Denial of Service:

a) Ping of Death.- En un ataque ping de la muerte, un hacker envía una solicitud de eco en un paquete IP más grande que el tamaño máximo de paquete de 65.535 bytes. El envío de un ping de este tamaño puede hacer que el equipo de destino se reinicie o colapse.

b) Smurf Attack .- Este ataque toma ventaja de la capacidad que tiene ICMP de enviar mensajes a direcciones broadcast, lo cual es utilizado para iniciar ataques de inundación. Intervienen 3 partes: la estación atacante, la víctima y redes cómplices.

La estación atacante genera un paquete ICMP echo-request con origen falso de la estación víctima y con destino a un rango de IPs, las estaciones reciben el mensaje ping con dirección falsa y responden a la víctima. Como el número de host que responde es alto el enlace de la víctima se satura.

c) TCP SYN Flood .- En un ataque de inundación SYN TCP, una inundación de paquetes es enviado, a menudo con una dirección de remitente falso. Cada paquete es tratado como una solicitud de conexión, haciendo que el servidor genere un medio de conexión abierta enviando un paquete TCP SYN-ACK y esperando una bolsa en la respuesta de la dirección del remitente. Sin embargo, como se forja la dirección del remitente, nunca llega la respuesta. Estas conexiones a medio abrir satura el número de conexiones disponibles en el servidor, evitando que responder a las peticiones legítimas hasta después del ataque final. (Véase **Fig 2.6**)

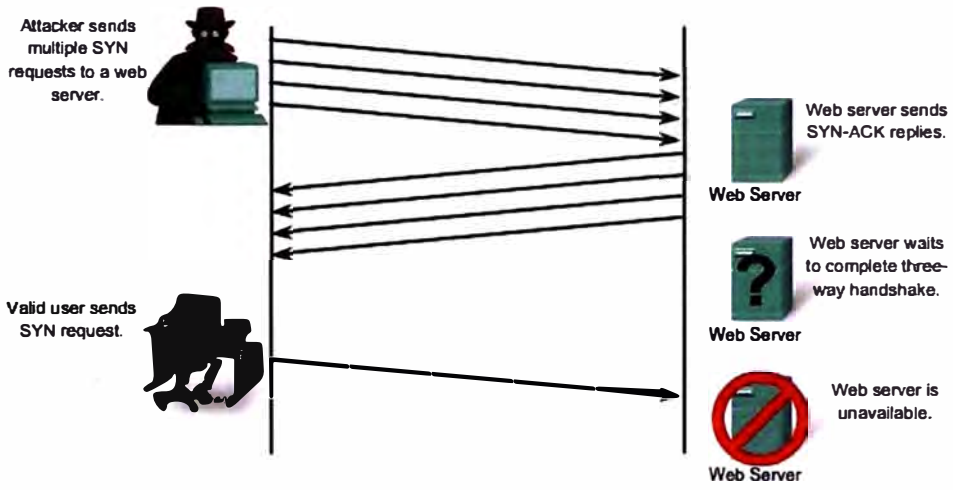

Fig 2.6 Ataque DoS TCP SYN Flood

Fuente: www.cisco.com

2.4. Estadísticas sobre vulnerabilidades y riesgos.

Los datos incluyen alrededor de 12186 aplicaciones web con 97554 vulnerabilidades detectadas de diferentes niveles de riesgo [4]. El análisis muestra que más de un 13% de todos los sitios revisados pueden ser atacados. Cerca del 39% son Cross-Site Scripting, SQL Injection en un porcentaje de 15% del total de páginas escaneadas el 7% son vulnerabilidades, de un porcentaje del 30% de las paginas solo el 4% se encontró vulnerabilidades del tipo Fingerprinter.

Los gráficos y la tabla que se muestran detallan los porcentajes encontrados luego de realizar el escaneo de las páginas con sus respectivas vulnerabilidades. Véase (Fig. 2.7, Fig. 2.8 y Tabla 2.1).

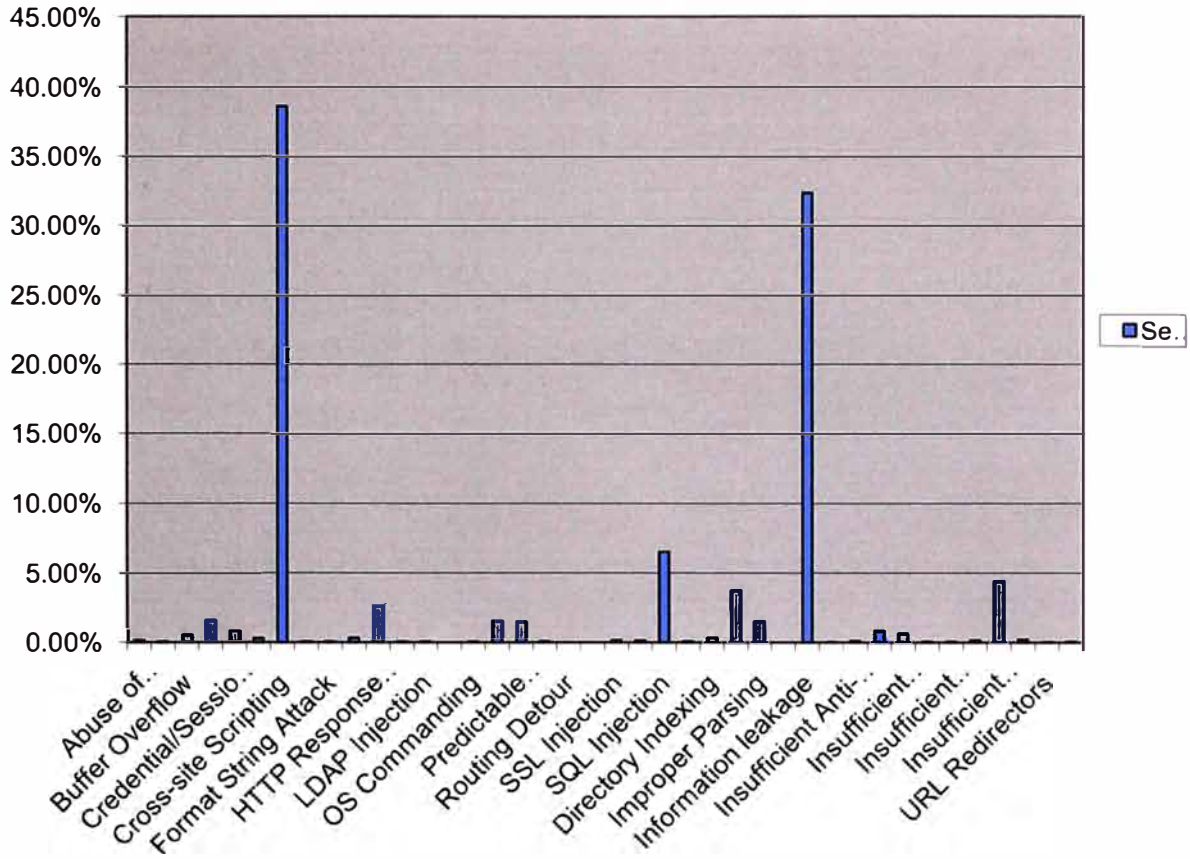

Fig. 2.7 Porcentaje de Vulnerabilidades Fuente: www.webappsec.org

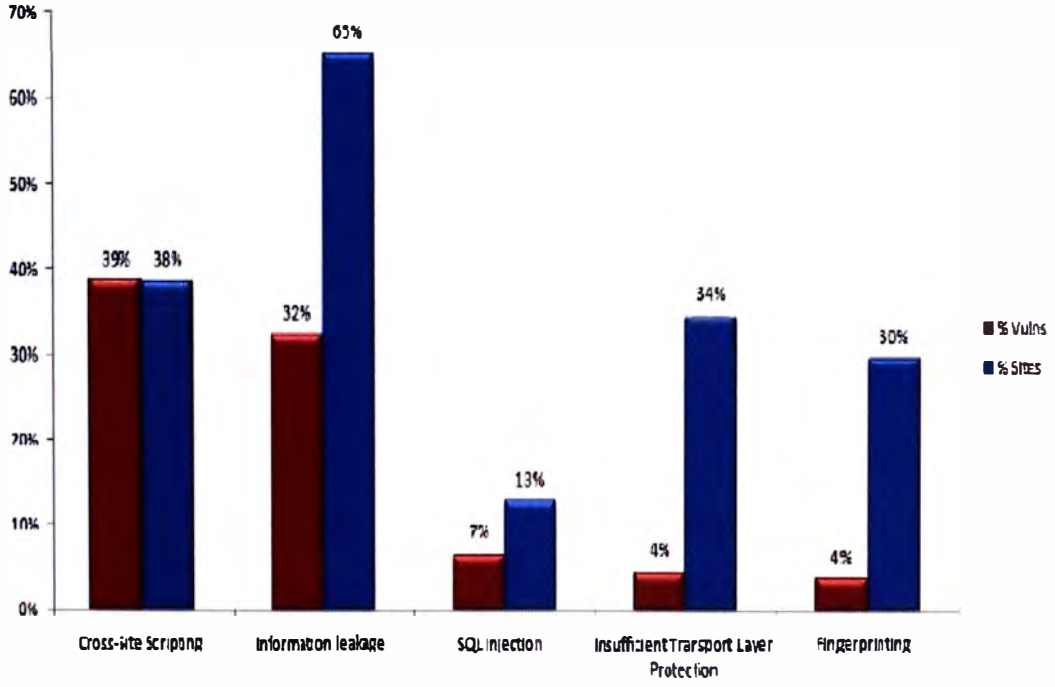

Fig. 2.8 Vulnerabilidades encontradas en aplicaciones web Fuente: www.webappsec.org

Tabla 2.1

Threat Clasification	N of Vulns	N of Sites	% Vulns	% Sites
Abuse of Functionality	153	83	0.16%	0.68%
Brute Force Attack	79	51	0.08%	0.42%
Buffer Overflow	537	84	0.55%	0.69%
Content Spoofing	1564	304	1.60%	2.49%
Credential/Session Prediction	794	147	0.81%	1.21%
Cross-site request forgery	285	161	0.29%	1.32%
Cross-site Scripting	37624	4686	38.57%	38.45%
Denial of Service	42	36	0.04%	0.30%
Format String Attack	52	43	0.05%	0.35%
HTTP Request Splitting	311	162	0.32%	1.33%
HTTP Response Splitting	2592	161	2.66%	1.32%
Integer Overflow	79	46	0.08%	0.38%
LDAP Injection	41	16	0.04%	0.13%
Mail Command Injection	1	1	0.00%	0.01%
OS Commanding	76	30	0.08%	0.25%
Path Traversal	1563	139	1.60%	1.14%
Predictable Resource Location	1507	295	1.54%	2.42%
Remote File Inclusion	99	44	0.10%	0.36%
SOAP Array Abuse	2	1	0.00%	0.01%
SSL Injection	157	33	0.16%	0.27%
Session Fixation	137	123	0.14%	1.01%
SQL Injection	6345	1555	6.50%	12.76%
Application Misconfiguration	85	60	0.09%	0.49%
Directory Indexing	370	184	0.38%	1.51%
Fingerprinting	3663	3604	3.75%	29.57%
Improper Parsing	1464	524	1.50%	4.30%
Improper Permissions	4	4	0.00%	0.03%
Information leakage	31527	7942	32.32%	65.17%
Insecure Indexing	8	7	0.01%	0.06%
Insufficient Anti-automation	108	36	0.11%	0.30%
Insufficient Authentication	806	304	0.83%	2.49%
Insufficient Authorization	615	286	0.63%	2.35%
Insufficient Data Protection	64	21	0.07%	0.17%
Insufficient Process Validation	52	34	0.05%	0.28%
Insufficient Session Expiration	169	71	0.17%	0.58%
Insufficient Transport Layer Protection	4317	4195	4.43%	34.42%
Server Misconfiguration	193	113	0.20%	0.93%
URL Redirectors	5	4	0.01%	0.03%
Xpath Injection	64	19	0.07%	0.16%
Total	97554	12186		

Sumario.

En el capítulo II, presenta una revisión del valor y clasificación de la información en redes, para entender la importancia de los datos (información) que se manejan en una empresa y el grado de nivel que pueden alcanzar de acuerdo al contenido.

Toda información se encuentra expuesta a Amenazas, riesgos y vulnerabilidades estos conceptos con abordados en este capítulo, teniendo en cuenta el grado de riesgo se logra clasificar las vulnerabilidades y los distintos tipos de amenazas que la información puede estar siendo afectada.

Los tipos de ataques que pueden sufrir un dispositivo de red o un servidor desde internet o dentro de una red local son estudiados en este capítulo mediante la categorización de los ataques. Finalmente se recoge un análisis de vulnerabilidades realizadas a 12186 aplicaciones web donde Site-Cross Scripting se presenta en mayor cantidad.

CAPITULO III
FUNDAMENTO TEORICO.

3.1. Seguridad Perimetral en redes LAN

La seguridad de los datos y transacciones es de vital importancia en esta época de rápida expansión de las redes informáticas, y de la nueva economía basada en internet. Por ello la seguridad perimetral basa su filosofía en la protección de todo el sistema informático de una empresa desde "fuera" es decir componer una coraza que proteja todos los elementos sensibles de ser atacados dentro de un sistema.

Los retos que se derivan de la seguridad se han convertido en los más importantes en todas aquellas compañías que hacen uso de las tecnologías de la información. Hace que la seguridad ocupe un primer lugar para los directivos de las empresas, por tal motivo cada vez más están usando aplicaciones que son determinantes para el funcionamiento y productividad de sus negocios.

El éxito de las compañías y su supervivencia, dependen de estas aplicaciones y de la productividad que puedan obtener implementándolas. De esta manera, la disponibilidad, la confiabilidad, la integridad y la autenticación de los datos, son fundamentales para el negocio.

Sin una protección adecuada y efectiva la plataforma de tecnología informática es vulnerable a actividades no autorizadas de hackers, competidores o empleados.

Es por eso; cuando hablamos de seguridad perimetral en las redes, debemos mencionar "Políticas de Seguridad" de una organización. Sin una política de seguridad, la seguridad perimetral no sirve, ya que es la realización práctica. Este punto lo tocaremos más adelante para mejor detalle.

Las acciones que realiza la seguridad perimetral son:

a). Rechaza conexiones a servicios comprometidos, permitiendo sólo ciertos tipos de tráfico (por ejemplo correo electrónico, http, https etc.) a usuarios finales o administradores.

b) Proporcionar un único punto de interconexión con el exterior, por lo que es posible auditar el tráfico entre la zona interna (inside) y la externa (outside).

c) Redirigir el tráfico entrante a los sistemas adecuados dentro de la red local, ocultando nombre de sistemas, topologías, tipos de dispositivos usados, cuentas de usuarios internos, sistemas o servicios vulnerables que no son fáciles de proteger desde Internet

d) Poder mantener controlado y monitoreado los tipos de ataques; hackers, virus, malware que toman como punto cualquier DMZ, con lo que la empresa gana confianza y estabilidad para conseguir un rendimiento mayor en cuanto a la información que puedan compartir con sus demás colaboradores.

La seguridad en un entorno corporativo se puede considerar organizada por capas, siendo la capa de seguridad perimetral la más externa de todas, por lo que la protección es más temprana. El hecho de disponer de una capa de seguridad no elimina la necesidad de las demás, sino que las complementa para mejorar la seguridad global, como se muestra en la fig. 3.1

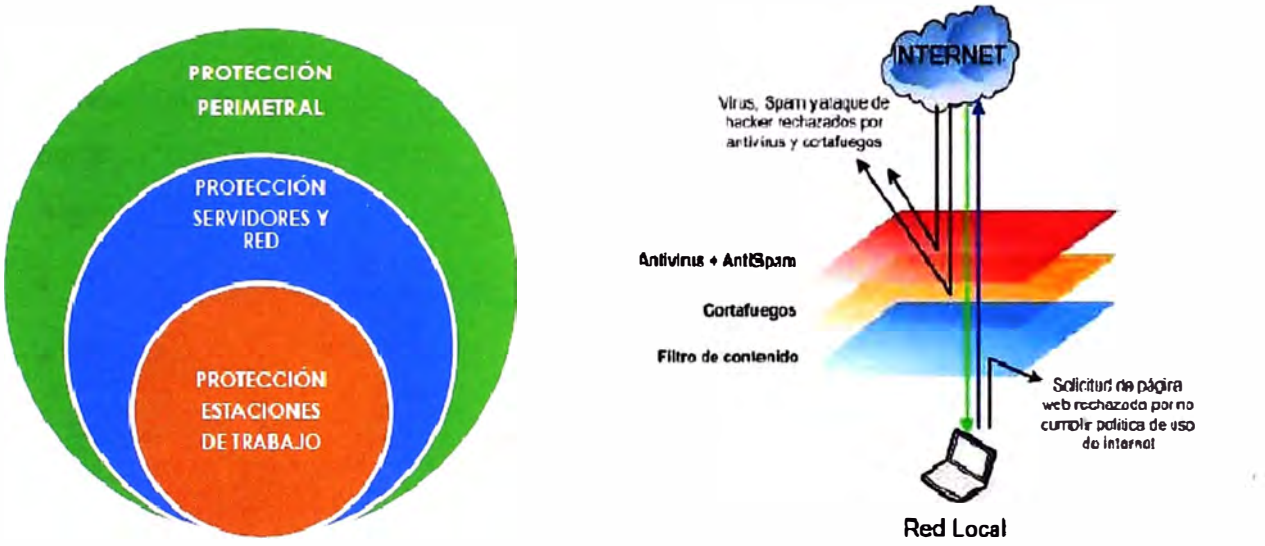

Fig. 3.1 Capas de Seguridad en una red Empresarial.

3.2. Perímetro sobre la Red LAN.

El perímetro es por lo general el primer punto de acceso a toda red, por ésta razón debe asegurarse debidamente para evitar que los ataques externos puedan dañarla, es decir es la frontera fortificada de nuestra red. Debido a que son la primera barrera entre internet y nuestra organización, los servidores de perímetro, o de borde, han de contar con las técnicas de protección más sofisticadas, ya que por lo general en caso de que sean comprometidos, un atacante tendría acceso a los servidores más importantes de la empresa. En el lado del perímetro se incluyen las estructuras, métodos de transmisión, formatos de transporte y medidas de seguridad que son utilizadas para proveer confidencialidad,

integridad, disponibilidad y autenticación para transmisiones de datos sobre redes de comunicación pública y privada.

a) Confidencialidad: Asegura la liberación intencional o no de información no autorizada de la organización. La perdida de confidencialidad puede ocurrir de diversas formas. Por ejemplo por una liberación intencional de información privada de la organización, configuración errónea de parámetros de red de los dispositivos, etc.

Algunos de los elementos utilizados para asegurar la confidencialidad son:

a) Protocolos de seguridad de red.

b) Servicios de autenticación de red.

c) Servicios de encriptación de datos.

b) Integridad: Asegura que el mensaje enviado es el mensaje recibido y que el mensaje no fue intencionalmente modificado. Por ejemplo, la pérdida de integridad puede ocurrir cuando se modifica el contenido de una página Web. El concepto de integridad el de no repudiación, lo que significa que se tiene evidencia confiable de las actividades realizadas por una fuente especifica.

Algunos de los elementos empleados para asegurar integridad son:

- Servicios de Firewall
- Administración de comunicaciones.
- Servicios de detección de intrusos (IPS).

c) Disponibilidad: Se refiere a los elementos que crean fiabilidad y estabilidad en una red y en los sistemas. La disponibilidad asegura que los sistemas sean accesibles cuando sea requerido permitiendo a los usuarios autorizados acceder a la red o al sistema.

d) Autenticación: Se refiere a que los elementos deben validarse entre sí, antes de iniciar una sesión. La autenticación evita que elementos no autorizados para comunicarse en la red puedan establecer sesiones.

El siguiente grafico muestra los dispositivos que delimitan la seguridad perimetral de una red: router, firewall, prevención de intrusos y acceso remoto. Garantizando la disponibilidad de los servicios, integridad, confidencialidad de la información, acceso seguro desde internet hacia los distintos aplicativos y autenticación de los usuarios para ingresar a gestionar los dispositivos y servicios. En los puntos tocados mas adelante se detallara el funcionamiento de cada dispositivo mencionado. Véase Fig. 3.2.

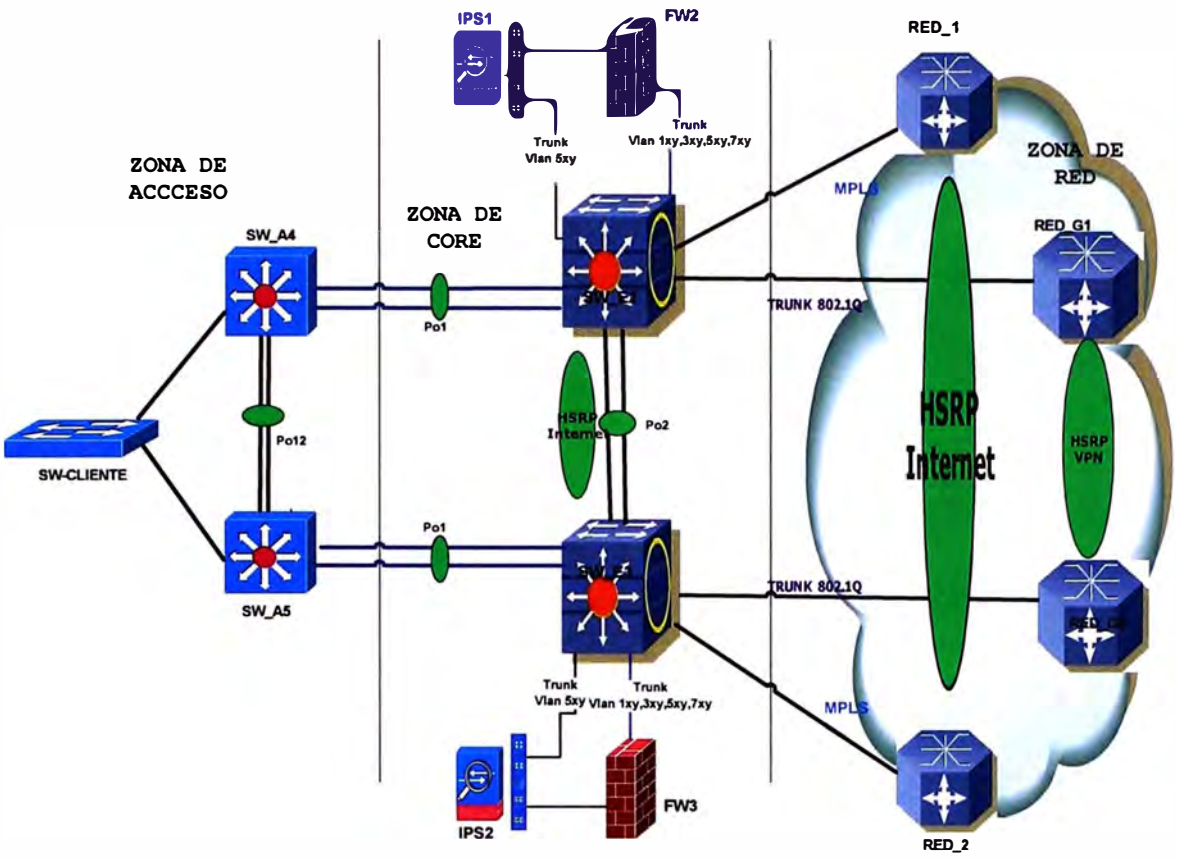

Fig. 3.2 Topología Perimetral de una Red Empresarial.

3.3 Análisis Perimetral

El análisis perimetral es la manera en la que se analizan las áreas a proteger, teniendo políticas de seguridad dentro de las empresas, para evitar el daño de la información.

En el desarrollo del análisis, varias preguntas se deben contestar:

a) La necesidad del negocio:

¿Qué es lo que la organización quiere hacer con la red?, ¿Cuáles son las necesidades de la organización? .Independiente de la implementación de seguridad, las necesidades del negocio es lo primordial.

b) La identificación de amenazas:

¿Cuáles son los tipos más probables de amenazas para una organización?, ¿Cuáles son las áreas más vulnerables de la red dentro de la empresa?

c) El análisis de riesgo:

¿Cuál es el costo versus beneficio de implementar diversas tecnologías de seguridad?

d) Practicas recomendadas.

¿Qué es lo fiable, lo recomendado y las buenas prácticas de seguridad que actualmente se emplean?

3.3.1 Técnica para delimitar áreas a proteger.

La técnica que se utiliza para delimitar las áreas es a través de Redes Autodefensivas; es decir, la red tiene la habilidad de identificar, prevenir y adaptarse a las amenazas de seguridad.

No se puede depender de dispositivos puntuales que estén en la periferia sino que la red en sí misma debe defenderse.

El primer elemento es la "integración"; la seguridad de la red debe estar integrada a nivel del sistema, todos los componentes de la red tienen que ser un punto de defensa e interactuar entre sí mismos. Los routers tienen que hablar y trabajar con los switches, los firewalls, los sistemas de prevención de intrusos, servidores, PCs, etc. Todo debe trabajar como un sistema unificado y cada punto de la red debe tener la posibilidad de actuar como agente de seguridad.

La "Colaboración"; es el segundo de los elementos. La empresa Cisco lanzó la iniciativa Control de Admisión de la Red (NAC, por sus siglas en inglés) a la cual se han sumado los principales proveedores de seguridad (Trend Micro, IBM, Microsoft, Symantec), para crear una plataforma donde convergen todas las tecnologías que hacen que las redes sean más seguras, de esta manera se obtiene dispositivos que trabajen en coordinación para mitigar los ataques.

Como tercer y último elemento está la "Adaptabilidad"; la seguridad debe tener un enfoque proactivo y no reactivo, donde la red se adapta a la evolución de los nuevos ataques, de esta manera la red puede identificar comportamientos sospechosos de los distintos dispositivos conectados a una red, independientemente de que el ataque sea conocido o no.

La Red Autodefensiva consta de tres pilares para responder a las nuevas amenazas [6].

a) El primer pilar, Seguridad integrada, se incorporan elementos de seguridad en componentes de la red como switches y routers.

b) El segundo pilar, Seguridad Colaborativa, se construyen vínculos entre los elementos de seguridad de la red y se entiende la presencia de la red hasta los puntos terminales que se conectan a ella.

c) El tercer pilar, introduce funciones de adaptabilidad, las cuales incrementan la capacidad de la red para responder a amenazas tanto conocidas como desconocidas sobre la base de un conjunto de nuevas tecnologías.

En el diagrama topológico muestra las diferentes zonas de seguridad (DMZ, Internet,

Usuarios), accesos a servidores, control de internet, etc. Teniendo como finalidad mejorar la adaptabilidad e integración con otros dispositivos de seguridad dentro de la red. Véase Fig. 3.3.

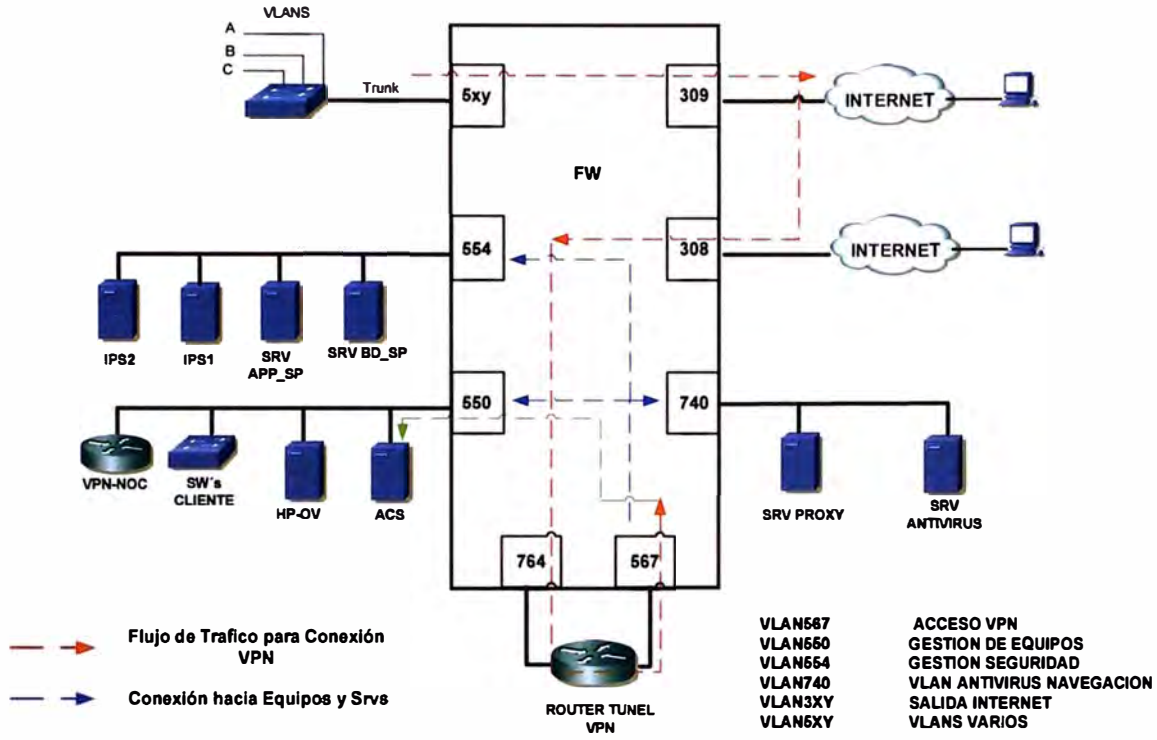

Fig. 3.3 Topología Lógica de una Red Empresarial.

3.3.2 Políticas de Seguridad.

Una política de seguridad es un conjunto de objetivos de una empresa, son normas de conducta para los usuarios, administradores y requisitos del sistema. Estos objetivos, normas y requisitos de forma colectiva garantizan la seguridad de una red y los sistemas informáticos en una organización. Al igual que un plan de continuidad, una política de seguridad es un documento en constante evolución sobre la base de los cambios en la tecnología, los negocios, y las necesidades de los empleados.

Una política de seguridad tiene una serie de ventajas:

a) Demuestra el compromiso de la seguridad para la organización

b) Establece las normas para el comportamiento esperado.

c) Garantiza la coherencia en las operaciones del sistema, software y hardware de adquisición, el uso y mantenimiento.

d) Define las consecuencias jurídicas de violaciones.

e) Se le brinda al personal de seguridad el apoyo de la gestión.

Las políticas de seguridad se utilizan para informar a los usuarios, el personal y los

gerentes de las necesidades de una organización para la protección de la tecnología y los activos de información. Una política de seguridad también especifica los mecanismos que sean necesarios para atender las necesidades de seguridad y proporciona una línea de base que para adoptar, configurar y auditar sistemas informáticos y redes para su cumplimiento.

Componentes principales de una política de seguridad:

a) Políticas de Identificación y Autorización.- Especificar los usuarios autorizados que pueden tener acceso a los recursos de la red y verificar sus privilegios. Esto también incluye acceso físico hacia los recursos como switches, routers, servers, etc.

b) Políticas de Password.- Asegurara un mínimo de 6 caracteres alfanumérico más un carácter, cada 2 meses se estima cambiar el password.

c) Políticas de Acceso Remoto.- Identificar como los usuarios van a acceder a la red y con qué tecnología. Saber los privilegios con lo que van a acceder a los recursos de la red.

d) Procedimientos para Soporte de Redes.- Especificar los procedimientos para realizar updates, upgrades, etc. hacia servidores, switches, router, firewall, etc.

e) Procedimientos contra incidencias.- Realizar procedimientos contra disaster recovery, incidencia de seguridad o fallas en puntos importantes para la red.

3.4 Alta Disponibilidad para Redes de Datos.

Alta disponibilidad es un protocolo de diseño del sistema y su implementación asociada que asegura un cierto grado absoluto de continuidad operacional durante un período de medición dado.

3.4.1 Cluster de alta disponibilidad.

El término "cluster" se aplica a los conjuntos o conglomerados de computadoras construidos mediante la utilización de componentes de hardware comunes y que se comportan como si fuesen una única computadora.

La tecnología de clusters ha evolucionado en apoyo de actividades que van desde aplicaciones, servidores web, comercio electrónico y bases de datos de alto rendimiento, entre otros usos.

Los clusters son usualmente empleados para mejorar el rendimiento y/o la disponibilidad por encima de la que es provista por un solo computador típicamente siendo más económico que computadores individuales de rapidez y disponibilidad comparables.

3.4.1.1 Tipos de Cluster de alta disponibilidad

a) Alta disponibilidad de Infraestructura.-También llamado Redundancia de Hardware.

Si se produce un fallo de hardware en alguna de las máquinas del cluster, el software de alta disponibilidad es capaz de arrancar automáticamente los servicios en cualquiera de las otras máquinas del cluster (Failover). Y cuando la máquina que ha fallado se recupera, los servicios son nuevamente migrados a la máquina original (failback). Esta capacidad de recuperación automática de servicios nos garantiza la alta disponibilidad de los servicios ofrecidos por el cluster, minimizando así la percepción del fallo por parte de los usuarios.

b) Alta disponibilidad de Aplicaciones.- Si se produce un fallo de las aplicaciones de alguna de las máquinas del clúster, el software de alta disponibilidad es capaz de re arrancar automáticamente los servicios que han fallado en cualquiera de las otras máquinas del clúster. Y cuando la máquina que ha fallado se recupera, los servicios son nuevamente migrados a la máquina original. Esta capacidad de recuperación automática.

3.4.2 Redundancia.

Los sistemas redundantes en ingeniería de computadores, son aquellos en los que se repiten aquellos datos o hardware de carácter crítico que queramos asegurar ante los posibles fallos que puedan surgir por el uso continuado.

Se presenta como una solución a los problemas de protección y confiabilidad. Este tipo de sistemas se encarga de realizar el mismo proceso en más de una estación, ya que si por algún motivo alguna dejara de funcionar o se colapsara, inmediatamente otro tendría que ocupar su lugar y realizar las tareas del anterior.

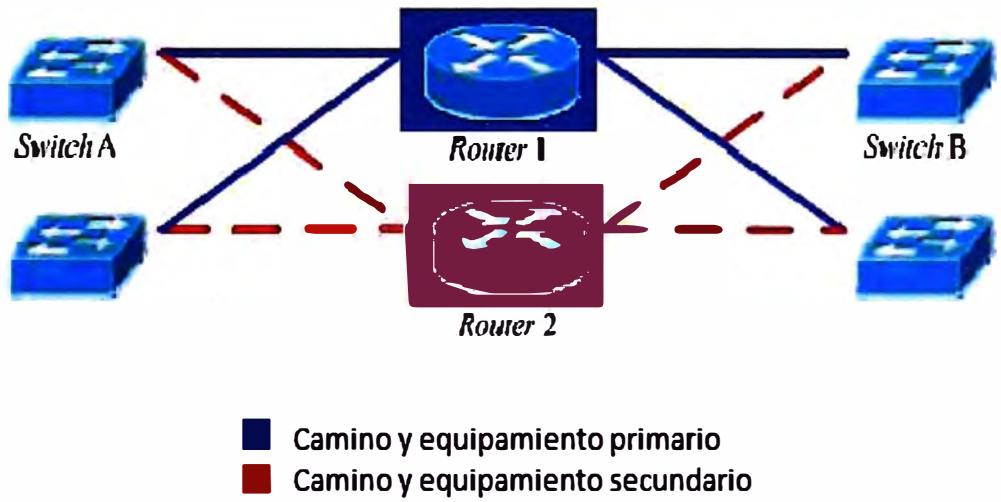

Fig. 3.4 Red genérica Redundante. Fuente: www.cisco.com

Los dispositivos en redes (como hubs, switches y routers) son actualmente diseñados para cubrir soluciones con redundancia, por ejemplo tarjetas que tienen 2 Uplink, fuentes de

alimentación duales, las figuras 3.5 y 3.6 son ejemplos de hardware redundante.

Fig. 3.5 Uplink Redundante. Fuente: www.cisco.com

Fig. 3.6 Routers con múltiples fuentes de alimentación.

3.4.3 Disponibilidad

La importancia de la disponibilidad de un servicio es visible en tareas tan simples como reservar una plaza en un avión o la recaudación de dinero en un cajero automático que sería difícil de lograr sin el apoyo de un sistema informático. A veces, esta disponibilidad es tan importante que puede llegar a ser la clave para la prosperidad de un negocio o su fracaso total.

El concepto de disponibilidad en una red se refiere al período en que los servicios están disponibles o el tiempo que se asume como razonable para que el sistema responda a una petición de usuario.

La disponibilidad de un servicio se calcula en función del porcentaje que aumenta la probabilidad de encontrar el servicio operativo en un momento dado. Este porcentaje se asocia con el tiempo de funcionamiento del servicio y con el término; "número de nueves de disponibilidad", donde una solución de "cinco nueves" tiene un tiempo de actividad del 99,999%. El documento presenta dos formas de calcular la disponibilidad de un servicio.

a) Disponibilidad operacional: Es un período de tiempo que incluye todas las fuentes de tiempo de inactividad, tales como: tiempo de inactividad administrativa, tiempo de inactividad logística, etc. Se basa en la división de disponibilidad del sistema y el tiempo total. Matemáticamente, es igual a:

$$Ao = \frac{Uptime}{Operating\ Cycle}$$ Fórmula. 2.1

Por ejemplo: Una red que se encuentra disponible 165 horas por semana, el máximo valor seria 24 horas/día x 7 días/semana. El porcentaje de disponibilidad, en este caso es 165/168 = 98.21%.

b) Disponibilidad inherente: Es el porcentaje de tiempo cuando el sistema esté en funcionamiento. La disponibilidad inherente puede ser obtenida por la fórmula que figura a continuación

$$A = \frac{E[Uptime]}{E[Uptime]+E[Downtime]}$$ Fórmula. 2.2

$$A_I = \frac{MTBF}{MTBF+MTTR}$$ Fórmula. 2.3

Donde:

MTBF: como su nombre indica, es el tiempo medio entre fallos de los módulos de hardware. MTBF de módulos de hardware se puede obtener del proveedor para la plataforma-módulos de hardware-off.

MTTR: es el tiempo necesario para reparar un módulo hardware que ha fallado.

Ejemplo: Se está usando un equipo que tiene el tiempo medio entre fallos (MTFB) de 81,5 años y el tiempo medio de recuperación (MTTR) de 1 hora:

MTBF en horas = 81,5 * 365 * 24 = 713940

Disponibilidad = MTBF / (MTBF + MTTR) = 713940 / 713941 = 99,999859%

Indisponibilidad = 0.000141%.

3.4.3.1 Tiempo de Inactividad

Son periodos de tiempo introducidos, durante el cual las operaciones dejan de funcionar, por lo general como resultado de problemas mecánicos o falta de material.

El tiempo de inactividad es una forma más intuitiva de entender la disponibilidad. La tabla 3.1 compara la disponibilidad y el tiempo de inactividad correspondiente [7].

	Uptime	Downtime	Downtime por Año	Downtime por Semana
1	90%	10%	36.5 dias	16 horas y 15 minutos
2	98%	2%	7.3 dias	3 horas y 22 minutos

3	99%	1%	3.65 dias	1 hora y 41 minutos
4	99.80%	0.20%	17 horas y 30 minutos	20 minutos y 10 segundos
5	99.90%	0.10%	8 horas y 45 minutos	10 minutos y 5 segundos
6	99.99%	0.01%	52.5 minutos	1 minuto
7	99.999%	0.001%	5.25 minutos	6 segundos
8	99.9999%	0.0001%	31.5 minutos	0.6 segundos

Tabla 3.1 Valores de Disponibilidad.

Algunos valores de la tabla pueden asociarse con determinados servicios:

(1) Computadoras personales y equipos experimentales.

(3) Sistemas de acceso.

(5) Servidores de Internet.

(6) Sistemas de Negocio.

(7) Sistemas de Telecomunicaciones, Bancos y Salud.

(8) Sistemas Militares.

3.4.3.2 Costos de Disponibilidad.

Cuando se implementan opciones más sofisticadas para mejorar la disponibilidad de la implementación, los costos pueden aumentar drásticamente en función exponencial.
La fig 3.7 muestra al curva Costo vs Niveles de Disponibilidad.

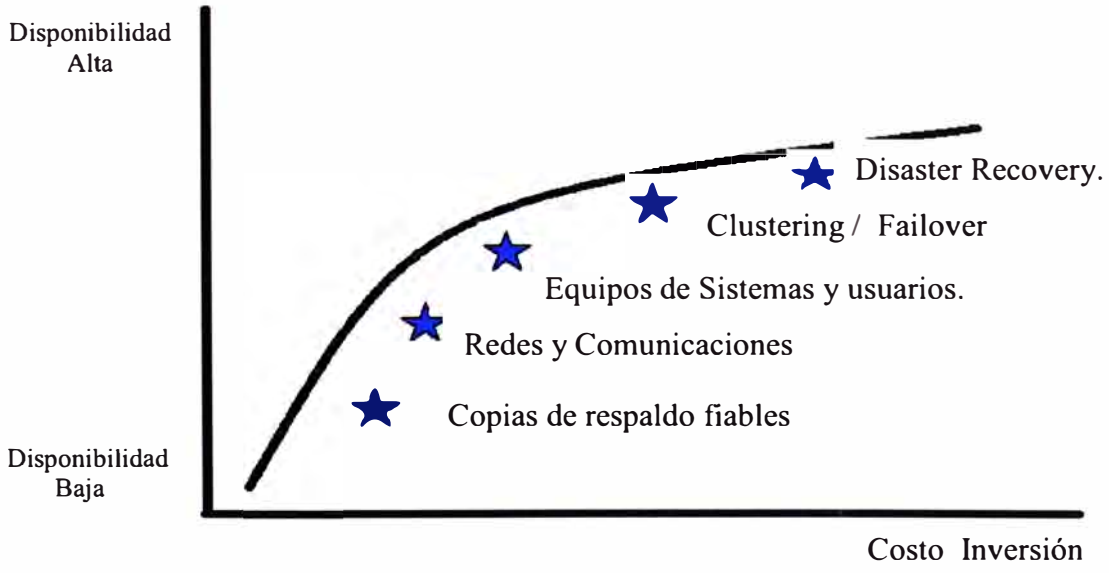

Fig. 3.7 Niveles de Disponibilidad.

Por lo tanto, la regla fundamental para alcanzar un alto nivel de disponibilidad es una base sólida técnica y la aplicación de un sistema de gestión estricta. Si no se aplica la estrategia

correcta, la inversión realizada en la compra de hardware y software puede ser en vano.

3.4.4 Tecnologías para Alta Disponibilidad

Algunas soluciones para efectuar alta disponibilidad a nivel de red (capa 3) son mencionados en esta sección:

3.4.4.1 Hot Standby Router Protocol (HSRP)

El Hot Standby Router Protocol es un protocolo propiedad de CISCO que permite el despliegue de routers redundantes tolerantes a fallos en una red, definido en la RFC 2281 [10] en donde entre los dos equipos se crea una IP virtual que puede ser usada como default gateway de los cliente. Véase Fig. 3.8

Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los Routers.

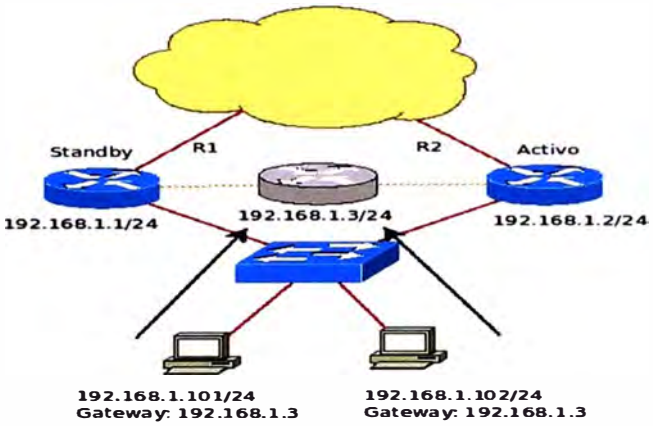

Fig. 3.8 Diagrama de una Red HSRP Básica. Fuente: www.cisco.com

El funcionamiento del protocolo HSRP es el siguiente: Se crea un grupo (también conocido por el término inglés Clúster) de routers en el que uno de ellos actúa como maestro, enrutando el tráfico, y los demás actúan como respaldo a la espera de que se produzca un fallo en el maestro.

HSRP es un protocolo que actúa en la capa 3 del modelo OSI administrando las direcciones virtuales que identifican al router que actúa como maestro en un momento dado.

Este protocolo se configura por interface, por lo que podemos tener varios grupos en cada una de las interfaces para brindar redundancia simultánea a varios segmentos de la red.

Si el router que está en el rol de Activo pierde conectividad o queda fuera de servicio, el vecino que está en modo Standby automáticamente toma su lugar (se asocia con la MAC y la IP virtual) haciendo que el cambio sea transparente a los clientes de la red involucrada,

como muestra la fig. 3.9

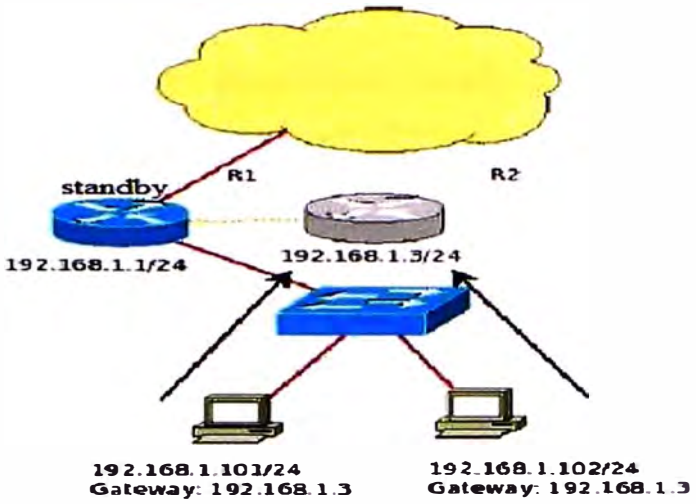

Fig. 3.9 Failover Del Cluster HSRP. Fuente: www.cisco.com

3.4.4.2 Heartbeat

Heartbeat es un "demonio" que proporciona servicio de clúster a la infraestructura de los clientes. Esto les permite saber acerca de la presencia (o desaparición) de procesos entre dos máquinas e intercambiar mensajes fácilmente entre ellos.

Con el fin de ser útiles a los usuarios, Heartbeat tiene que ser combinado con un administrador de recursos de clúster (CRM), que tiene la tarea de iniciar y detener los servicios (direcciones IP, servidores Web, firewall, etc.) agrupados hacen la alta disponibilidad.

El modulo de comunicaciones Heartbeat provee mensajeria multicast fuertemente autenticada y localmente ordenada básicamente sobre cualquier medio basado en IP o no. Heartbeat soporta comunicaciones en cluster sobre los siguientes enlaces redes:

- Unicast UDP sobre IPv4;
- Broadcast UDP sobre IPv4;
- Multicast UDP sobre IPv4;
- Serial Link Communications.

Heartbeat puede detectar fallas en el nodo de forma fiable en menos de medio segundo. Se registra en el temporizador de vigilancia del sistema y el demonio está listo para hacerlo.

3.5 Alternativa de Solución para el Sistema de Seguridad Perimetral

La topología que se trabajara está planteada en el capítulo I, desde ese punto se parte para realizar las mejoras en cuanto a la seguridad.

A) La primera mejora se tendría que realizar en los dispositivos firewall, la redundancia de

este dispositivo es importante para la continuidad del servicio y el buen funcionamiento de los aplicativos.

De la gran variedad de firewall (Fortinet, Cisco, CheckPoint, Lucent, etc.) que se tienen en el mercado, la topología inicial se presenta un firewall ya instalado y funcionando por lo que el segundo tiene que ser del mismo modelo y capacidad para realizar la Alta Disponibilidad entre ellos.

El modo que irían a trabajar estos equipos serian: Active – Standby, es decir el trafico pasaría siempre por el firewall activo mientras que el otro siempre estará en modo de escucha, para cuando ocurra cualquier problema con el activo, el segundo firewall de inmediato tome el control del flujo de trafico asumiendo la labor del activo.

La figura 3.9 se observa la topología al momento de adicionar el segundo firewall y el estado en que trabajarían cada uno de ellos.

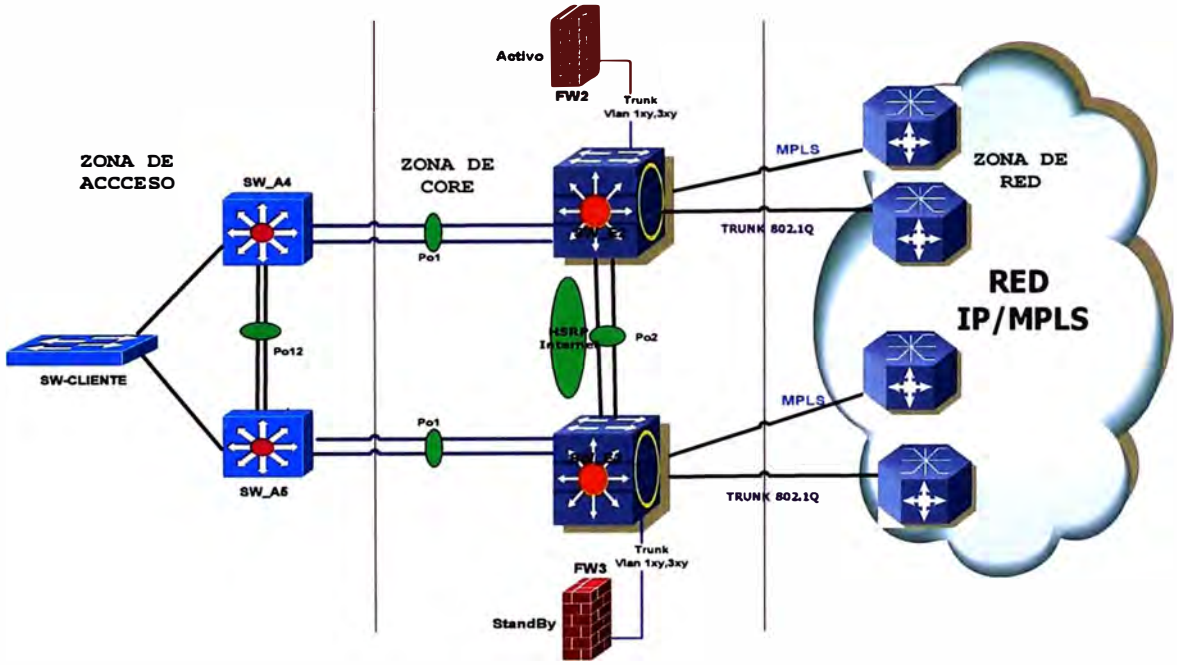

Fig. 3.10 Topología de Solución para Firewall.

B) Al ver que la seguridad era insuficiente por el constante cambio y aumento de vulnerabilidades en internet como: ataques del día cero, gusanos, virus, etc. que no pueden ser mitigados por el firewall, se presento la solución de una tecnología que permitía la inspección de tráfico en la red, es decir analizaba el trafico que pasaba pero no tomaba ninguna acción.

Estos equipos son llamados "Sistemas de Detección de Intrusos (IDS)", los IDS trabajan en "modo promiscuo" similar a un Sniffer que se pone en la red, copea el tráfico hacia una consola de administración donde se puede monitorear y verificar en que firmas esta

coincidiendo.

Como el IDS es un dispositivo pasivo en la red, apareció un dispositivo que podía estar en "modo de escucha" al tráfico de red en primer momento; pero cuando se presenta algún evento muy reiterativo podía bloquear y proteger, este dispositivo tiene el nombre de "Sistema de Prevención de Intrusos" (IPS), el IPS no solo realiza el análisis del trafico sino que puede realizar una defensa de la red, en modo inline.

En el capitulo V se detallara mas las funcionalidades del IPS.

El sistema de seguridad perimetral con el IPS era un punto que se tenía pendiente, de acuerdo a la topología el IPS puede estar delante o atrás del firewall. Por buenas prácticas de diseño de redes, el IPS tendría que ir atrás de firewall por las siguientes razones:

1.- El firewall podría asegurar hasta capa cuatro según modelo OSI.

2.- Delay de tráfico seria menor.

3.- Favorecería el análisis, si se presenta un problema de conectividad.

4.- El tráfico monitoreado seria tráfico valido.

5.- Hubiera menos falsos positivos al momento de realizar el análisis de la inspección de tráfico.

El grafico 3.10 muestra la ubicación del IPS dentro del sistema de seguridad perimetral planteado, por lo que tendrían que ser dos appliance para tener equipos redundantes tanto de firewall como IPS.

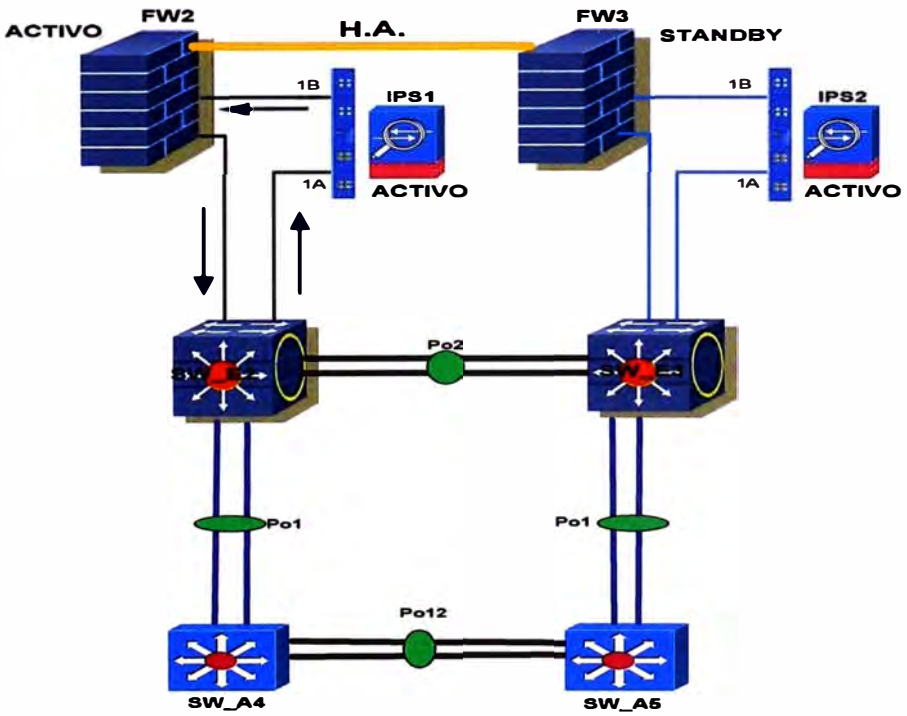

Fig.3.11 Topología con los IPS

C) La seguridad perimetral no puede tener un correcto funcionamiento dentro de una empresa si es que no se tiene una adecuada administración de los eventos (logs), los equipos de seguridad y conectividad generar registros que ayudan a realizar un diagnostico certero cuando se presenta algún problema o intermitencia en los servicios.

Por eso la importancia de contar con un servidor correlacionador de eventos, que centralice esos log´s que envían los distintos dispositivos. Se toma como opción para esa función el HP-OpenView que es un correlacionador muy estructurado que nos muestra a detalle los diferentes registros y log enviados, (ver fig. 3.11), también podemos trabajar con otras marcar como el Syslog´s que es OpenSource, además de otras marcas como: el MARS de Cisco o Accelops que son tecnologías muy fuertes en el mercado en este campo. En el capítulo IV se detalla el tema de registros.

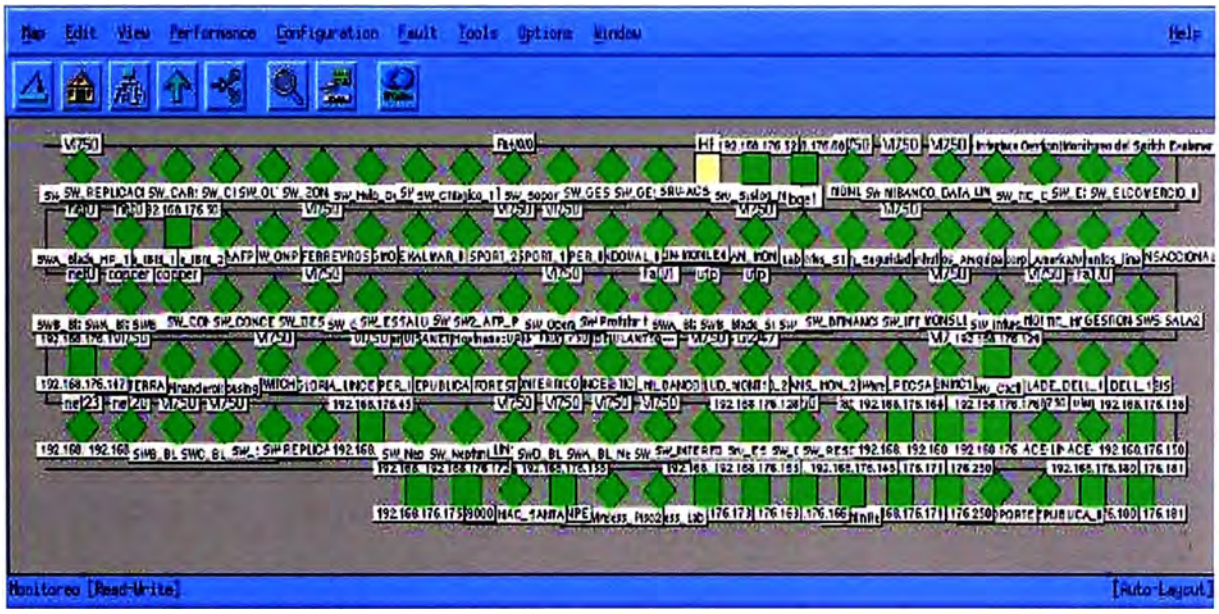

Fig. 3.12 Pantalla del HP-OpenView.

Sumario

El capitulo III, se reviso el concepto de seguridad perimetral y perímetro sobre una red Lan como puntos iniciales, resaltando la importancia que tienen las empresas de contar con seguridad y respaldo para sus aplicativos, la seguridad de la Red lo podemos dividir en capas siendo la seguridad perimetral la capa mas saliente y toma el nombre de perímetro. El perímetro de la red analiza que dispositivos son los adecuados para alcanzar altos niveles de confiabilidad, integridad y disponibilidad de los servicios.

El procedimiento del análisis perimetral nos permite conocer puntos vulnerables de la red, servidores o servicios que tienen mayor prioridad o data sensible de la empresa. Definimos técnicas para contrarrestar las vulnerabilidades y tener políticas que ayuden a sobrellevar la seguridad perimetral.

La alta disponibilidad para redes se trabajo en este capitulo reforzando conceptos como cluster, redundancia y disponibilidad.

En vulnerabilidad se toco la forma de cómo calcularlo matemáticamente en el caso de redes, tiempos de inactividad y costos de disponibilidad.

En tecnologías de alta disponibilidad mencionamos dos: HSRP que es una tecnología propietaria de Cisco y va de acuerdo al RFC 2281 y Heartbeat que es un servicio desarrollado en OpenSource.

Como último punto se reviso las alternativas de solución para el sistema de seguridad perimetral que se está desarrollando en el informe.

CAPITULO IV
GESTION Y ADMINISTRACION DE EVENTOS EN UNA RED SEGURA.

4.1 Control de Acceso para Redes LAN Seguras.

Los accesos deben darse de manera que durante el proceso de acceso a la información este no debe interrumpirse. El proceso debe ser capaz de ser auditado y los permisos de acceso deben darse de tal manera que se debe prevenir la modificación:

a) De datos por parte de usuarios no autorizados.

b) No autorizada de datos por usuarios autorizados.

Además se debe asegurar la preservación de la consistencia interna (los datos publicados internamente deben ser datos reales) y de la consistencia externa (los datos publicados externamente deben guardar consistencia con la información que maneja la empresa).

4.1.1 Restricciones de Acceso.

La estrategia de control de acceso debe darse por capas:

a) Acceso perimetral.- Restricciones de acceso a determinados protocolos y/o servicios desde el lado externo. Uso de ACL a determinados puertos, dominios, etc.

b) Acceso de Red.- Restricciones de acceso a determinados protocolos y/o servicios a los sistemas en la red interna. Uso de ACL a determinados puertos, servidores, etc.

c) Acceso al host.- Los sistemas operativos permiten el filtrado de acceso de usuarios y/o estaciones por medio de políticas de acceso.

d) Acceso a la aplicación.- Las aplicaciones permiten la identificación de usuarios o restricciones de acceso a determinados servicios de manera independiente por parte del sistema operativo donde es instalado.

e) Acceso a los datos o recursos.- Sobre los datos se pueden definir permisos para que sólo determinados usuarios o servicios puedan tener acceso a ellos. Acceso definidos por permisos y con derechos de acción sobre ellos.

Todos los accesos tienen la capacidad de monitoreo y registro de actividades para verificar que sólo se efectúen las acciones permitidas.

4.1.2 Modelos de Control de Acceso.

Existen tres modelos de control de acceso:

a) Control de Acceso Mandatorio.- La autorización de acceso a un sujeto depende de una etiqueta, la cual indica edición y la clasificación de sensibilidad del obejto.

b) Control de Acceso Discrecional.- El sujeto tiene autoridad con ciertas limitaciones para especificar que dispositivos pueden ser asequibles.

c) Control de Acceso No Discrecional.- Una autoridad central determina que sujetos pueden tener acceso a ciertos dispositivos basados en la politica de seguridad de la organización.

4.1.3 Identificación y Autenticación.

Los procesos de identificación y autenticación van juntos en un sistema donde se desea el control de acceso para redes seguras y la forma en que son manejados, definen el acceso a los recursos:

La parte inicial del proceso es la autorización de acceso a los recursos, que vienen a ser los privilegios que se les da a los usuarios. Una vez autorizado, el usuario procede a indentificarse ante el recurso o servicio mostrando sus credenciales: usuario y clave, smart card o señales biometricas. Luego el sistema procede a verificar, autenticar, las credenciales para ver si corresponden a los que dicen pertenecer. Estos procesos deben ser monitoreados y registrados cada evento que no corresponde a los permitidos para detectar cualquier actividad hostil, proceso conocido como "accounting".

4.1.3.1 Factores de Autenticación.

Los factores de autenticación son:

a) ¿Qué conoces?. Es algo que sólo "conoce" el usuario autorizado. Ejm: una clave, etc.

b) ¿Qué tienes?. Adicional a lo que uno ya "conoce", debe contar con algún dispositivo externo que complemente lo primero. Ejm: Smart Cards. Token, etc.

c) ¿Quién erés?. Características intrínsicas referentes al usuario.

Ejm: iris, huellas digitales.

La Fig. 4.1 muestra un ejemplo de autenticación de usuarios, como es un tarjeta de credito.

Fig. 4.1 Smart Card. Lo Que Tienes

4.1.3.2 Tecnologías de Autenticación.

Dentro de las tecnologias de autenticación existentes, las más importantes son: Claves y Token, Biometricas, Kerberos, CHAP (Challenge Handshake Autentication Protocol).

4.1.3.2.1 Claves y Tokens

Las claves son un conjunto de caracteres utilizados por un cliente a través de los cuales se valida en un sistema para acceder a sus recursos. Pueden ser tipo estatico; siempre el mismo para validarse y de tipo dinamico, uno nuevo cada vez que se valida.

Una "passphrase" es una secuencia de caracteres que usualmente es mayor que el número permitido para una clave.

Los tokens son tarjetas de memoria del tamaño de una tarjeta de credito que son empleados para suministrar claves estaticas o dinamicas. Exiten los siguientes tipo de smart cards:

A) Static password tokens.

- **a)** El propietario se autentica asi mismo al token.
- **b)** El token autentica al propietario.

B) Synchronous Dynamic password token.

- **a)** El token genera un nuevo valor de clave único en períodos de tiempo fijos.
- **b)** La clave única es ingresada al sistema junto con el PIN del propietario.

C) Asynchronous dynamic password tokens.

- **a)** Esquema similar al anterior con la excepción de que la clave es generada asincrónicamente y el cliente no tiene que autenticarse en la ventana de tiempo permitida.

D) Challenge-reponse tokens.

- **a)** Un sistema genera un cadena de desafio aleatorio y el propietario ingresa la cadena en el token junto con el PIN adecuado.
- **b)** El token genera una respuesta que es ingresada al sistema.
- **c)** El mecanismo de autenticación en el sistema determina si el propietrario debe ser autenticado.

La Fig. 4.2 muestra un modelo de token, que es utilizado como medio de autenticación .

Fig. 4.2 Token Modelo Semilla Fuente: www.vasco.com

4.2 Rol y Responsabilidad en la Gestión de Red.

Todas las personas en una organización, desde el director ejecutivo, a la nueva persona contratada, se consideran usuarios finales de la red y debe cumplir con la política de seguridad de la organización.

Desarrollar y mantener la política de seguridad delega a las funciones específicas dentro del departamento de TI.

La administración a nivel ejecutivo siempre debe ser consultada durante la creación de políticas de seguridad para garantizar que la política sea integral, coherente y jurídicamente vinculante.

Las organizaciones más pequeñas pueden tener un cargo ejecutivo único que supervisa todos los aspectos de la operación, incluidas las operaciones de la red. Las organizaciones más grandes podrían romper el grupo de trabajo ejecutivo en varias posiciones.

El negocio y la estructura de informes de una organización dependen del tamaño de la organización y la industria.

Algunos de los títulos ejecutivos más comunes:

a) Director de la Unidad.- Autorizar actividades propuestas por el oficial de seguridad que involucre implementación en infraestructura, organización, entretenimiento, aprobación de políticas de seguridad.

b) Líder de Operaciones.- Evaluar y recomendar implementaciones y mejoras recomendadas por el oficial de seguridad, analizar y definir un plan de acción sobre una vulnerabilidad o incidente.

c) Oficial de Seguridad.- Velar por el cumplimiento de las normas y políticas de seguridad de información, así como los procedimientos implantados.

d) Líder Técnico de Seguridad.- Asegura el cumplimiento de los controles lógicos de la seguridad, detecta y reporta fallas de red, identificación de vulnerabilidades.

e) Responsable Técnico de Ingeniería.- Sugerir mejoras de ingeniería en la seguridad TI, evalúa, selecciona y prueba equipos para SI.

f) Promotores de Seguridad.- Asegurar que las aéreas tomen conciencia de las políticas, procesos y procedimientos y guías de seguridad establecida.

g) Procesos y Auditorias.- Generación, Supervisión y cumplimiento de procesos y procedimientos implantados del SGSI, ejecutar de auditorías internas.

Verificar acciones tomadas por los promotores de seguridad para resolver incidentes.

La estructura organizativa de una empresa para la gestión de seguridad en redes, tomando

como referencia el Standard ISO 27001. Véase (Fig. 4.3)

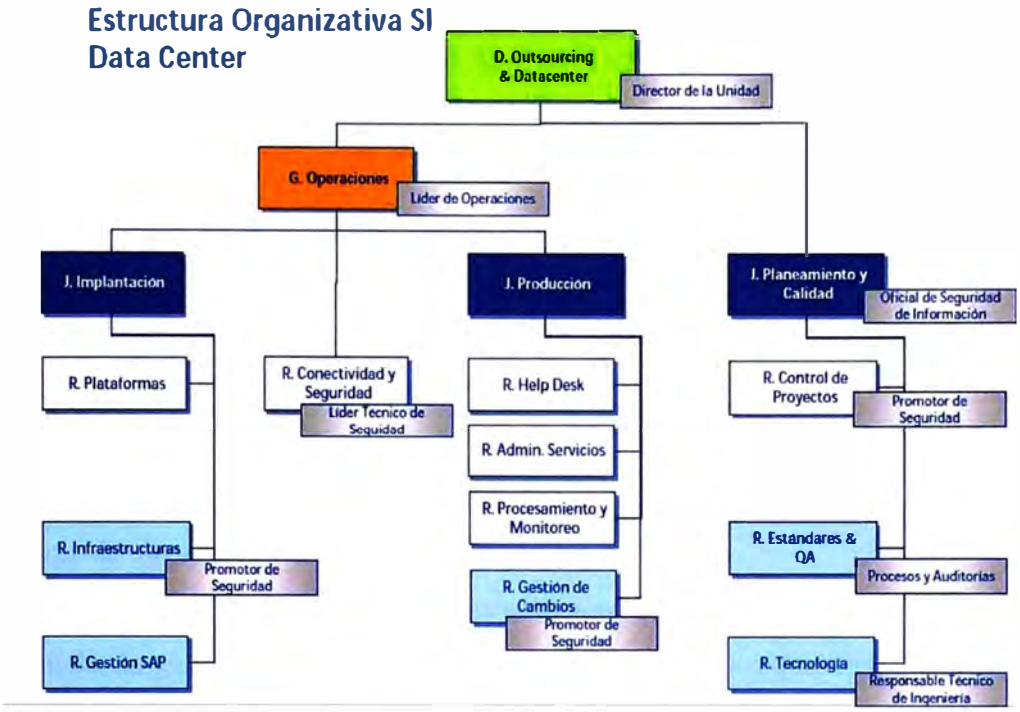

Fig. 4.3 Diagrama Estructural de Gestión en Seguridad

En el Anexo A se detalla los diferentes tipos de organizaciones internacionales de seguridad (CERT, SANS, ISC^2) y el Standard IOS 27001.

4.3 Establecimiento de Políticas de Registro.

Los requisitos deben incluir todas las leyes aplicables, regulaciones y políticas de organización existentes, como las políticas de retención de datos. Las metas deben basarse en el equilibrio de la reducción de Organización de riesgo con el tiempo y los recursos necesarios para realizar las funciones de gestión de registro. Los requisitos y metas entonces se deben utilizar como base para establecer una organización en toda la capacidad de gestión de registro.

Las organizaciones deben desarrollar políticas que definen claramente los requisitos obligatorios, sugerencias y recomendaciones para varios aspectos de la gestión de registro, incluyendo los siguientes [11]:

A) Generación de registros:

a) Cuales host y dispositivos deben o pueden realizar registros de acuerdo al tipo de eventos que realizan, por ejemplo security events, conexiones de red, intentos de autenticación, username, intentos de IP source, etc.

b) Frecuencia con la que debería registrarse cada evento, por ejemplo: cada ocurrencia,

cada vez que pase alguna ocurrencia, etc.

B) Transmisión de Registros.

a) Cuales host y dispositivos deberían transferir registros de acuerdo al tipo de evento que realizan para la administración de datos, por ejemplo: protocolos y servicios que están permitidos.

b) Frecuencia con la que deberían transferir los host o los servidores al syslog, por ejemplo: tiempo real, cada 5 minutos, cada hora, etc.

c) La confidencialidad, integridad y disponibilidad de cada registro de datos deben ser protegidas mientras esta en tránsito, incluso otra red es utilizada para transferir los registros.

C) Almacenamiento y Eliminación de Registros.

a) Tiempo de almacenamiento de registros en los servidores.

b) La confidencialidad, integridad y disponibilidad de registros deben estar presentes al momento de guardarlos en una habitación que cumpla los requisitos.

c) Espacio de almacenamiento que debería tener los registros en los Server.

d) Los datos innecesarios como deberían eliminarse.

e) Requerimientos de registros y preservación de acuerdo a un formato que nos indique cualquier movimiento, para que no puedan sufrir modificación ni alteración.

D) Análisis de Registros.

a) Frecuencia que los registros deben o deberían ser analizados. (tanto a nivel servidor como infraestructura).

b) ¿Quién debe o debería tener acceso a los registros y como se registrara esos acceso (tanto a nivel servidor como infraestructura)?.

c) ¿Que debería realizarse cuando se encuentra una actividad sospechosa o es identificado una anomalía?

d) ¿Como los datos sensibles de la empresa se muestran en los logs?, como passwords o contenidos de e-mails, estos deben ser tratados para salvaguardar cualquier fuga de información.

Las organizaciones deben asegurarse que sus otros procedimientos, directrices guarden relación con sus políticas que tienen implantadas para darle el soporte y funcionalidad.

4.4 Centralización y Análisis de Registros.

Los registros e informes incluyen flujo de contenido, cambios de configuración o instalación de nuevo software, por nombrar algunos nombres. Para identificar las

prioridades de información y seguimiento, es importante obtener el aporte de la gestión de red, administradores y seguridad de equipos. La política de seguridad también debe desempeñar un papel importante en responder a las cuestiones de qué tipo de información para los registros e informes.

Desde un punto de vista de la presentación de informes, la mayoría de dispositivos de red puede enviar datos syslog que puede ser muy valiosa la hora de solucionar problemas de red o de amenazas de seguridad. Los datos de cualquier dispositivo pueden ser enviados a una serie de análisis de syslog para su visualización. Estos datos se pueden consultar en tiempo real, en la demanda, y en los informes programados. Hay varios niveles de registro para asegurar que la cantidad correcta de los datos se envían, basada en el dispositivo envía los datos. También es posible a los datos de registro de marca del dispositivo en el software de análisis para permitir la visualización y presentación de informes granulares. Por ejemplo, durante un ataque, los datos de registro que es proporcionada por conmutadores de nivel 2 podrían no ser tan interesantes como los datos proporcionados por el sistema de prevención de intrusiones (IPS).

Muchas aplicaciones y protocolos también están disponibles, tales como SNMP, que se utiliza en los sistemas de gestión de red para supervisar y realizar cambios de configuración para dispositivos de forma remota.

4.4.1 Software Centralizadores de Registro.

4.4.1.1 Syslogs.

En una infraestructura de registro basado en el protocolo syslog, cada generador de registro utiliza el mismo formato de alto nivel para sus registros y el mismo mecanismo básico para la transferencia de sus entradas de registro a un servidor syslog corriendo en otro host. Syslog proporciona un marco sencillo para la generación de registro de entrada, almacenamiento y transferencia, que cualquier sistema operativo, software de seguridad, o una aplicación que puede utilizarse si ha sido diseñado para ello. Muchas fuentes de registro usan a syslog como su formato de registro nativo y ofrecen características que permiten que sus formatos puedan ser convertidos a formatos syslog.

Para su implementación se tiene dos tipos de sistemas:

a) Syslog Server.- Dichos sistemas son los que aceptan y procesan los diferentes tipos de eventos que envían los Syslog Clientes.

b) Syslog Cliente.- Dispositivos de red o Server que envían los mensajes de logs hacia los Syslog Server.

El Servidor Syslog muestra distintos tipos de mensajes y puede clasificarlos en diferentes niveles de acuerdo al riesgo que pueda estar ocurriendo, una organización establece los niveles que desea para monitorear de acuerdo a sus políticas implantadas, la siguiente figura muestra los niveles y tipos de mensajes que pueden presentarse. Véase Fig. 4.4

Level	Keyword	Description	Definition
0	emergencies	System is unusable.	LOG_EMERG
1	alerts	Immediate action is needed.	LOG_ALERT
2	critical	Critical conditions exist.	LOG_CRIT
3	errors	Error conditions exist.	LOG_ERR
4	warnings	Warning conditions exist.	LOG_WARNING
5	notification	Normal but significant condition.	LOG_NOTICE
6	informational	Informational messages only.	LOG_INFO
7	debugging	Debugging messages.	LOG_DEBUG

Fig. 4.4 Nivel de Mensajes del Servidor Syslog Fuente: www.cisco.com

4.4.1.2 HP Openview Network Node Manager (NNM)

Es un administrador de información para el protocolo SNMP (Simple Network Management Protocol), posee funciones de monitorización de dispositivos, recolección, almacenamiento y procesamiento de información SNMP, también permite descubrir y configurar mapas de red a nivel de enrutamiento (nivel 3 del modelo OSI).

HP OpenView es un conjunto de soluciones de software, amplio y modular para gerenciar y optimizar los servicios de TI e infraestructura de voz y datos, estas soluciones permiten ofrecer:

a) Autodescubrimiento de la red.
b) Visualización topológica de la red descubierta.
c) Gestión de eventos.
d) Servicio de correlación de eventos.
e) Actualización automática de estados en el mapa.
f) Colecciones de datos SNMP.
g) Visualización grafica de datos SNMP.
h) Consolas de gestión.
i) Interfaz Web de usuario.

A) SNMP

SNMP (Simple Network Management Protocol) es un protocolo para la gestión de red desarrollado por el IETF (RFC 3410) para proveer una gestión estándar, simplificada, y extensible de una red que tiene diferentes equipos de interconexión. El SNMP fue diseñado para facilitar la gestión de la red sin hacerla muy compleja.

La arquitectura del SNMP se basa en la interrelación de tres componentes básicos: un gestor, un agente, y una base de datos o MIB (Management Information Base). El gestor SNMP representa un programa como, por ejemplo, el HP OpenView de la plataforma de gestión de Hewlett-Packard. El agente constituye un software residente en los dispositivos gestionados de la red, tales como un conmutador, un enrutador, o una computadora. Cada agente almacena datos de gestión y responde a las preguntas del gestor SNMP. El tercer elemento, la base de datos, es referenciado como la Base de Información de Gestión y contiene los objetos gestionados.

4.5 Evidencia de Registro en Dispositivos de Redes Seguras.

a) Registros del Syslog.

El grafico muestra los eventos que envían los dispositivos de una red empresarial, el servidor syslog es un concentrador de registro que brinda disponibilidad, integración e integridad. Véase Fig. 4.5

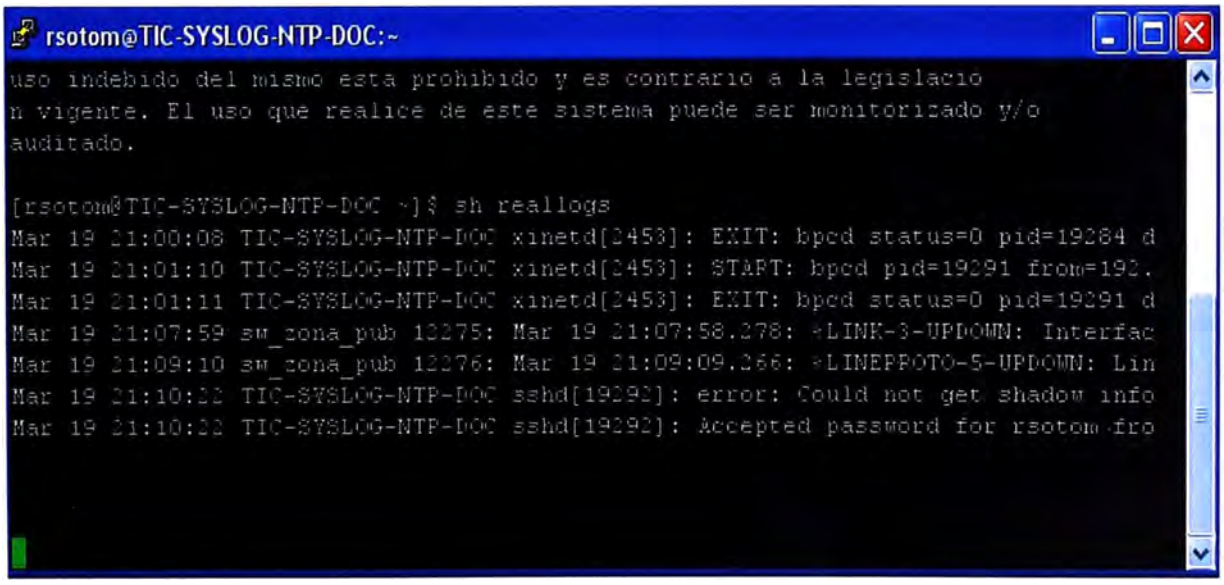

Fig. 4.5 Registros del Servidor Syslog.

b) HP-OpenView Registros.

La Fig. 4.6 muestra los eventos de los dispositivos que están monitoreados en el HP OpenView por ejemplo: switch, router, firewall.

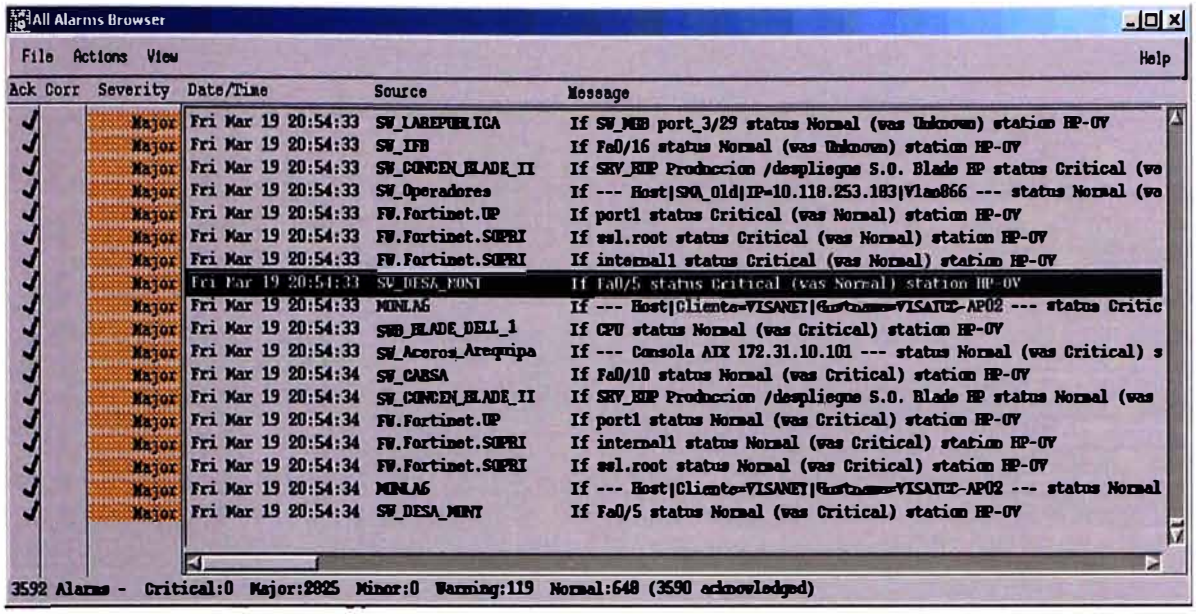

Fig. 4.6 All Alarm Browser.

La Fig. 4.7 muestra todos los dispositivos monitoreados por el Hp Openview en forma grafica. Los dispositivos se encuentran ordenados y en estado normal.

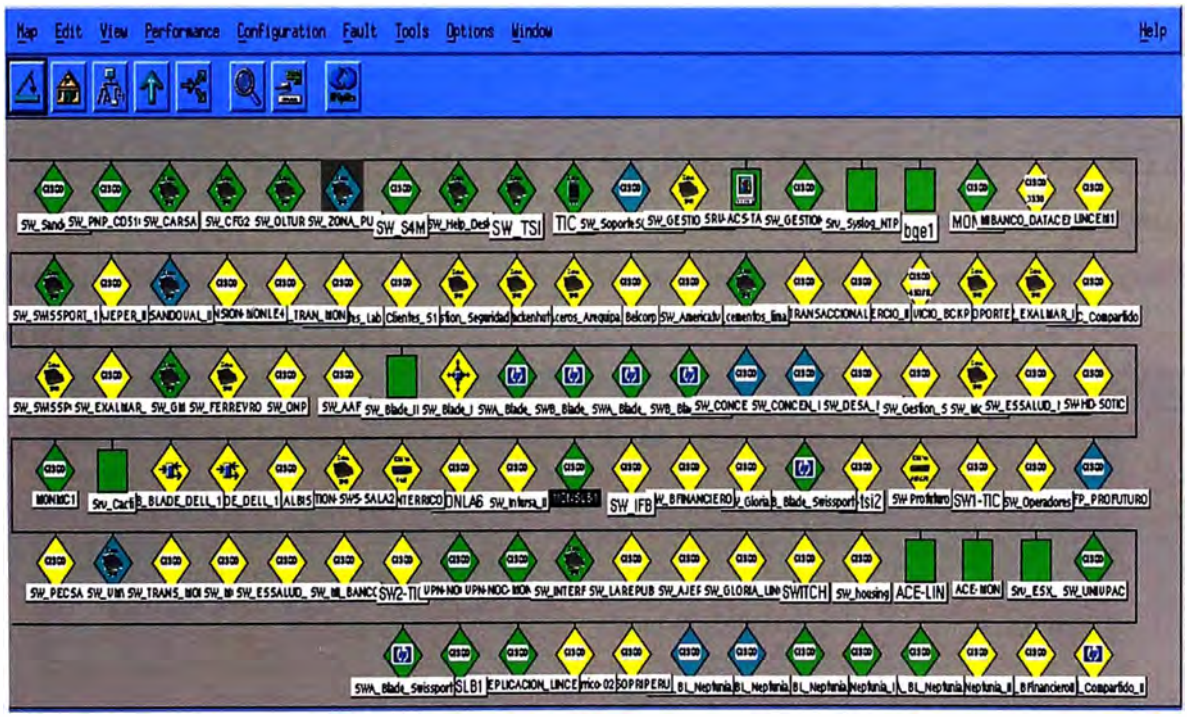

Fig. 4.7 Pantalla Dispositivos Monitoreados.

En el HP Openview se puede observar gráficos de toda una red que estén interconectados sus dispositivos, mostrando una topología de manera referencial mediante el comando "show cdp neigbord" que es propio de los equipos de marca Cisco , en el siguiente grafico se muestra un Switch Core con varios switches de acceso conectados directamente a el, (Véase Fig. 4.8).

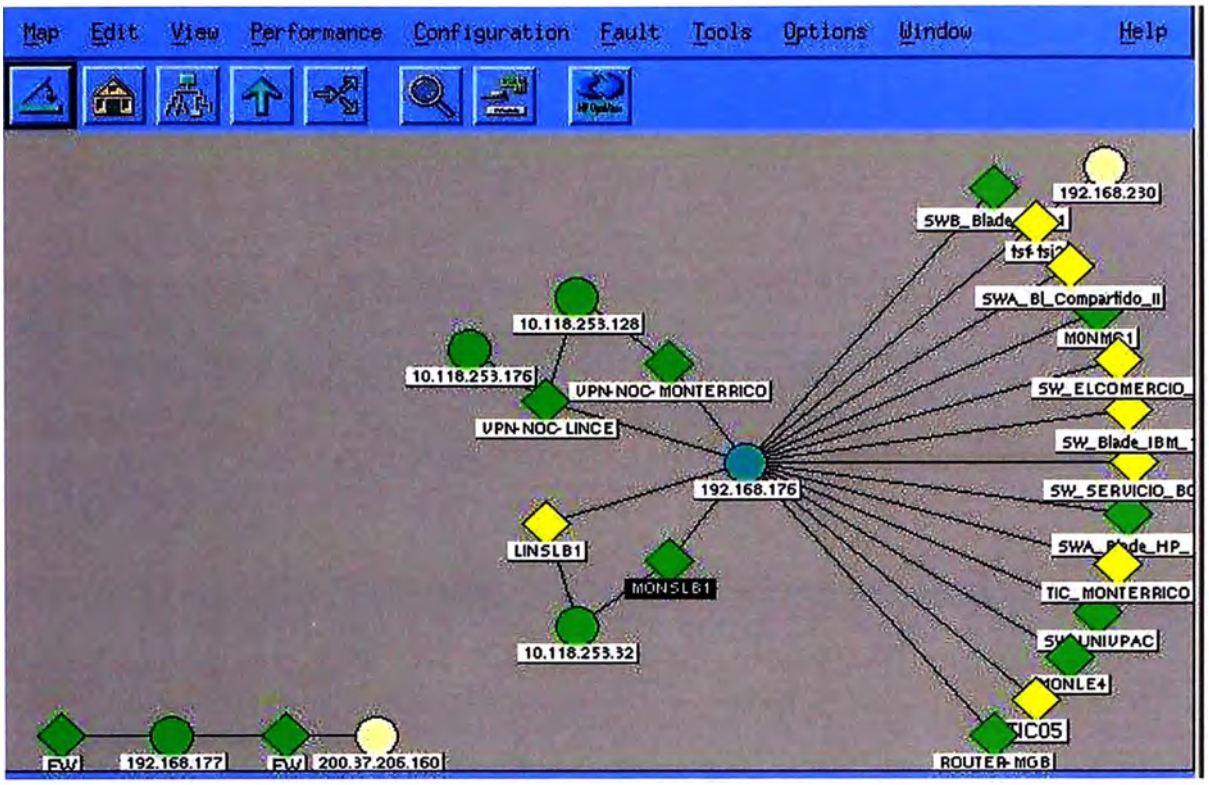

Fig. 4.8 Red de Dispositivos Monitoreados.

c) IPS: Registro de eventos.

Los registros que se muestran en la Fig.4.9 son eventos producidos por el comando ping hacia un servidor. La firma ICMP Echo Reply es visualizado en el software de monitoreo propio para los IPS de marca Cisco, IME nos ayuda a visualizar dichos eventos que se activan y produce el registro.

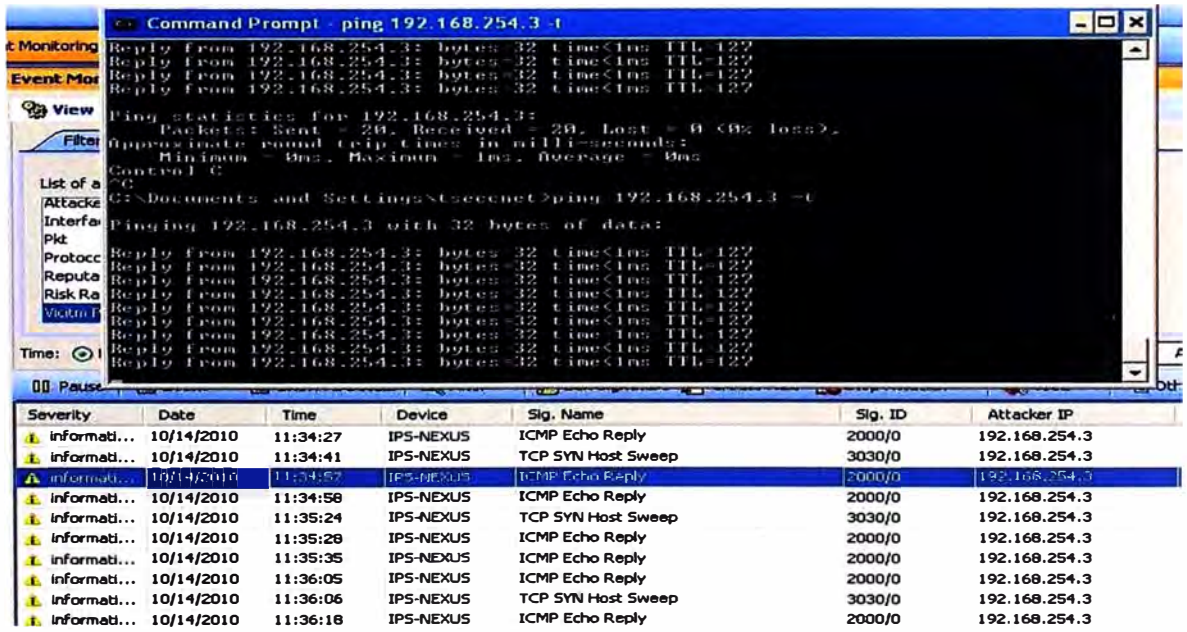

Fig. 4.9 Registros del IPS.

Sumario.

En el capítulo IV se revisó el concepto de control de acceso para los usuarios de una red empresarial, estos accesos se dan mediante dispositivos que brindan restricciones o permisos de acuerdo al tipo de trabajo que va realizar el usuario. Los Token son dispositivos que aumentan el nivel de seguridad en el acceso, ya que "no solo es algo que conoces" (password) sino "algo que tú tienes".

Toda empresa que tiene implantado un sistema de seguridad perimetral tiene un orden jerárquico de rol y responsabilidades para la gestión de una red, esto se desarrolló tomando en cuenta las recomendaciones del ISO 27001.

Los registros dentro de un sistema de seguridad perimetral toman importancia para evidenciar cualquier intermitencia o ataque en la red, por lo que se ha incluido en este capítulo políticas de registro además de las tecnologías que permiten concentrar los diferentes tipos de eventos que producen los dispositivos de seguridad y tenerlos de forma ordenada y clasificada cuando se necesiten. Como último punto se detalla mediante grafico los diferentes tipos de registros y del software concentrador (HP Openview).

CAPITULO V
INGENIERIA DEL PROYECTO.

5.1 Ubicación de los dispositivos de Seguridad.

a) Routers.- Un router es un tipo de dispositivo que pasa paquetes de datos entre redes basándose en direcciones de capa 3. Puede tomar decisiones acerca de la mejor ruta para la distribución de datos por la red, trabajar en capa 3 permite al router tomar decisiones basándose en las direcciones de red, en lugar de las direcciones MAC individuales de la capa 2.

Los routers que se colocan en los límites de la red, también se le conoce como routers firewall. Estos proporcionan una seguridad básica dentro de una zona más privada. Frente a la red exterior o frente a un área menos controlada, puede crearse ACL para cada protocolo de red configurado.

b) Sistemas de Prevención de Intrusos.- Los IPS deben ser colocados según el tipo de arquitectura de red implementada. Por ejemplo, si la organización tiene acceso a internet y tiene servidores públicos que proveen servicios, entonces debe haber un IPS en la red externa (pública) y uno en la red privada (interna) para monitorear ataques en ambos lados de la red, como recomendación de buenas prácticas. Así mismo debe haber HIDS (Host Intrusion Detection System) en los servidores públicos protegiendo los datos más importantes en cada servidor.

En el Capítulo III, se reviso que el IPS va estar situado detrás del firewall para inspeccionar el tráfico que entra desde internet y el tráfico interno generado por los servidores.

c) Firewall.- El firewall es un equipo diseñado para trabajar en el perímetro principalmente, pero si es necesario se puede colocar para proteger el acceso a determinados servidores y estaciones en la red interna.

Por buenas prácticas la mejor ubicación de estos dispositivos es atrás de los equipos que dan la salida a internet, es decir es la primera barrera antes de ingresar a la red interna. Por tal motivo; el firewall está ubicado de acuerdo a la topología que se muestro en el capítulo

III y se detallara más en este capítulo.

d) Dispositivos VPN.- Los dispositivos para VPN pueden estar ubicados en los Firewall, routers firewall o crearlos entre dos routers o dos firewall para brindar una capa más de seguridad a la conectividad. Las conexiones VPN se crean para encriptar la comunicación entre dos redes (LAN), o para el acceso seguro hacia servicios en producción.

En el Anexo B se describe las características técnicas de los equipos de seguridad que se utilizarán en el Sistema de Seguridad Perimetral.

5.1.1 Diagrama de inspección de tráfico.

La Fig. 5.1 nos muestra el flujo de tráfico que tiene el paquete al momento de ingresar a los dispositivos de seguridad [12].

a) El paquete ingresa a la interfaz del dispositivo (2).

b) El firewall verifica si la conexión existe (3), si es existente lo envía para la inspección de secuencia (6), si no existente sigue la secuencia y el paquete es analizado por los ACL.

c) (4) Si hay un ACL que permita la conexión, el paquete es enviado, caso contrario "lo deniega".

d) El primer paquete del flujo debe coincidir con una regla de traslación por defecto, se realiza una búsqueda rápida para determinar una interfaz de salida. Las reglas de traslación indican si se puede realizar NAT o no. Una regla de translación es exitosa entonces la conexión es creada. (5).

e) Las inspecciones se aplican para garantizar el cumplimiento del protocolo. Función de NAT incorporada sobre el paquete IP (6).

f) Traslación de la dirección IP en la cabecera IP o puerto si esta utilizando PAT (7).

g) El tráfico es desviado hacia el IPS para su análisis.

h) El paquete es enviado hacia la interfaz de salida, dicha interfaz es determinada primero por las reglas de traslación (8).

i) Cuando no se determina la interfaz de salida por las reglas de traslación, los resultados del global route encuentran la interfaz de salida adecuada para el paquete (9), una vez que la ruta del siguiente salto es encontrada, la capa 2 comienza a realizar la búsqueda y reescribe la cabecera de la direcciones MAC (10).

j) Los contadores se incrementarán en la interfaz de salida y el paquete es transmitido hacia el destino (11).

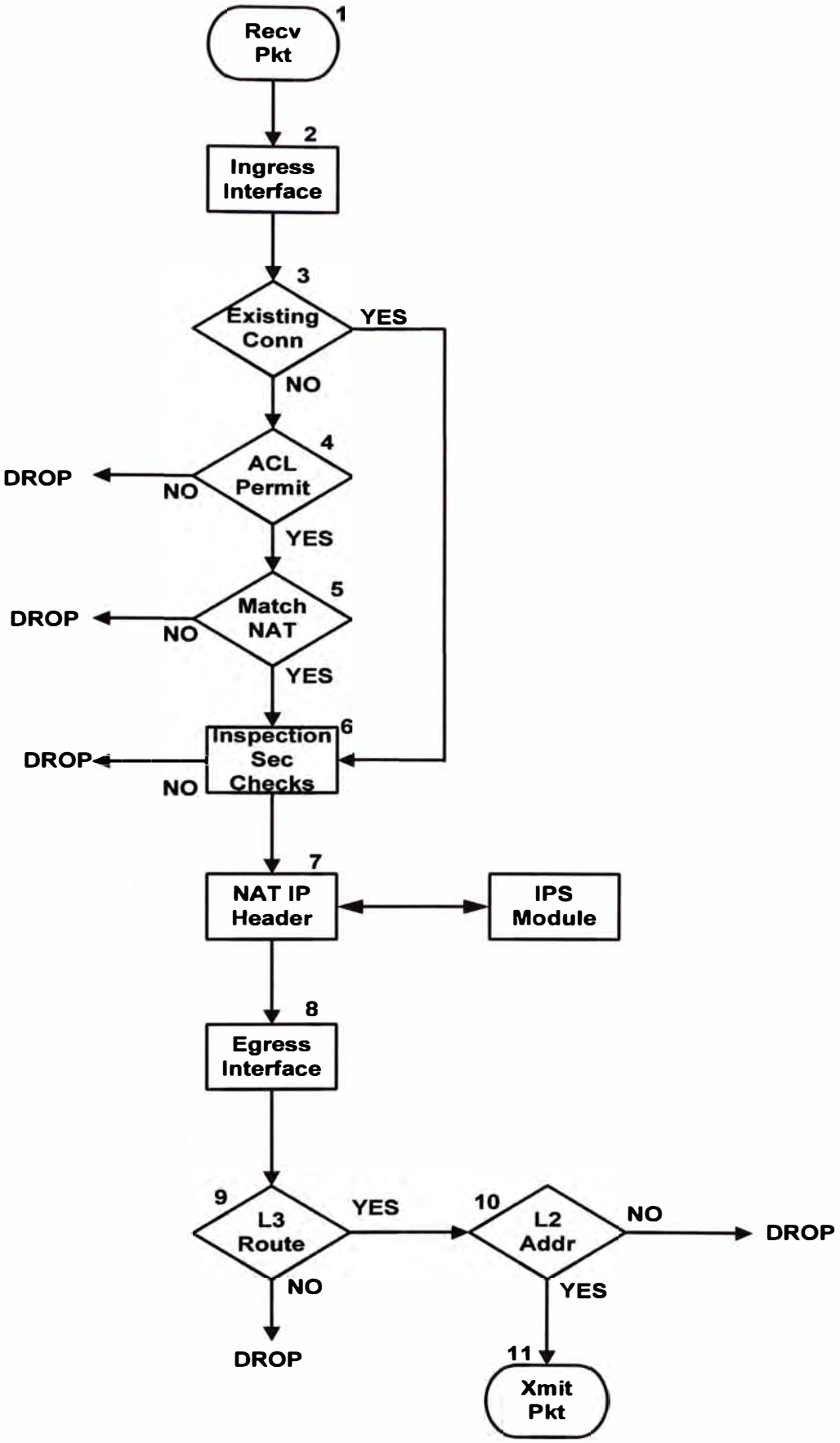

Fig. 5.1 Diagrama de Flujo de Tráfico IP.

5.1.2 Sistemas de Prevención de Intrusos (IPS)

Los gusanos de Internet y los virus pueden propagarse en todo el mundo en cuestión de minutos. Una red de inmediato debe reconocer y mitigar las amenazas de virus y gusanos.

Los firewalls no pueden hacer mucho y no puede proteger contra malware o ataques de día cero. Un ataque de día Cero es un ataque informático que intenta explotar las vulnerabilidades del software que se desconoce o no han sido divulgadas por el proveedor de software. El termino de las cero horas se describe en el momento en que el exploit es descubierto Durante el tiempo que tarda el proveedor de software para desarrollar y lanzar un parche, la red es vulnerable a estos exploit.

Un método para impedir que los gusanos y los virus penetren en la red es que un administrador supervise continuamente la red y analicé los archivos de registro generados por los dispositivos de red. Esta solución no es muy escalable. Analizar manualmente la información de los archivo de registro es una tarea que consume tiempo y proporciona una visión limitada de los ataques que se lanza contra una red. En el momento en que se analizan los registros, el ataque ha comenzado ya.

Los Sistemas de Detección de Intrusión (IDSs) fueron puestos en práctica para monitorear pasivamente el tráfico sobre una red. Un dispositivo IDS-HABILITADO copia la corriente del tráfico, y analiza el tráfico monitoreando más bien los paquetes reales reenviados. Compara el tráfico capturado con firmas desconocidas (maliciosas) en una forma Offline (Fuera de línea) de una manera similar al software de chequeo de virus (antivirus). Esta implementación de IDS offline se conoce como modo promiscuo.
Es mejor implementar una solución que detecta y actué de inmediato frente a un problema de red cuando sea necesario.

Un sistema de prevención de intrusiones (IPS) se basa en la tecnología IDS. A diferencia de IDS, IPS es un dispositivo aplicado en modo online. Esto significa que todo el tráfico de entrada y salida debe fluir a través de él para su procesamiento. El IPS no permite que los paquetes entren en la zona de confianza de la red sin que sea analizado.
Un IPS monitorea el tráfico de la capa 3 y capa 4, analiza el contenido y la carga útil de los paquetes que contendría los ataques más sofisticados y podría incluir datos maliciosos en las capas 2 hasta la 7. La plataforma del fabricante CISCO para IPS utilizan una mezcla de tecnologías de detección, basadas en firmas, perfiles y análisis de protocolo de detección de intrusos [12]. Este análisis profundo permite que el IPS identifique, detenga y bloquee los ataques que normalmente pasan a través de un dispositivo de seguridad tradicional.

Cuando llega un paquete a través de una interfaz en un IPS, el paquete no se envía a la interfaz de salida o de confianza hasta que el paquete ha sido analizado. Ver Fig.5.2

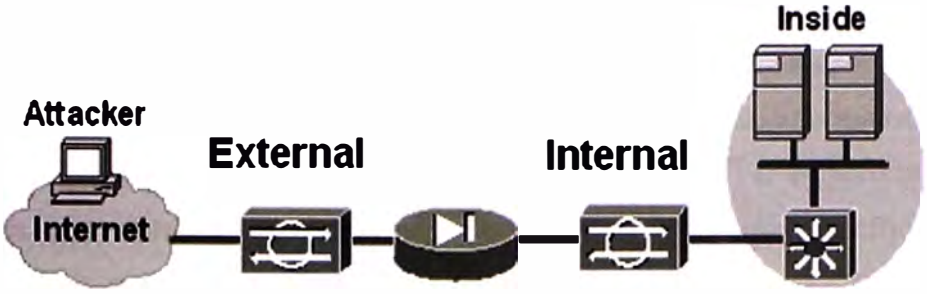

Figura 5.2 Despliegue de sensores IPS Fuente: www.cisco.com

5.1.2.1 Ventajas y Desventajas del IPS vs IDS

La ventaja de operar con el IDS es que no afecta negativamente el flujo de paquetes reales del tráfico transmitido. La desventaja de operar en una copia del tráfico es que el IDS no puede detener el tráfico malicioso, un solo paquete de los ataques, puede alcanzar el sistema de destino antes de que pueda aplicar una respuesta para detener el ataque. Un IDS a menudo requiere la asistencia de otros dispositivos de red, como routers y firewalls, para responder a un ataque.

La ventaja de operar en modo inline con un IPS es que este puede detener los ataques de un simple paquete antes de alcanzar el sistema destino. La desventaja es que un IPS mal configurado o una solución IPS inadecuada pueden afectar negativamente el flujo de paquetes del tráfico transmitido.

5.1.2.2 Sistema de Arquitectura del IPS.

A). Reputation filtering

"Reputation filtering" es una de las nuevas funcionalidades que resulta de la utilización del nuevo servicio Cisco SensorBase.

"Reputation filtering" comprueba la reputación de una IP antes de que siquiera los paquetes enviados por dicha IP sean procesados por el IPS. De esta manera se obtiene una funcionalidad proactiva. Además, al no procesar dichos paquetes se consigue un ahorro muy significativo en el uso de los recursos del IPS.

La funcionalidad "Reputation filtering" es bloquear todo tráfico originado por una IP sólo si detecta que dicha IP tiene la reputación absolutamente más baja de la escala.

En caso contrario, el "Reputation filtering" dará su conformidad para que el tráfico prosiga y siga siendo analizado por otra funcionalidad de los IPS: las firmas o "signatures".

B). Firmas (Signatures)

Una firma es un conjunto de reglas que un IDS y un IPS utilizan para detectar actividad maliciosa, tales como los ataques DoS. Estas firmas les dan una identificación exclusiva a gusanos específicos, virus, malware, ataques maliciosos. Los sensores IPS están sintonizados para buscar concordancia con firmas patrones de tráfico anormales.

Las Firmas IPS son conceptualmente similares a los "virus.dat" el archivo utilizado por los antivirus. Los virus.dat son archivos que contienen información específica acerca de los virus y esto le permite identificar a los software maliciosos, para McAFee el archivo es .DAT, para el antivirus Sophos .IDE.

Un Sensor IDS o IPS examina el flujo de datos usando muchas firmas diferentes, cuando un sensor coincide con una firma de un flujo de datos, el toma una acción, tal como un registro de eventos o se envía una alarma hacia un software administrativo del IDS o IPS.

LA Fig. 5.3 muestra los elementos de la Firma: Active Directory Failed

SignatureID : 5726

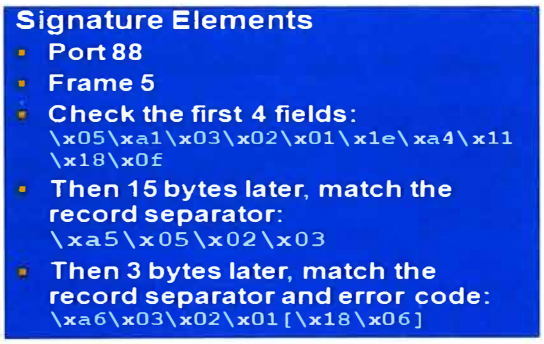

Fig. 5.3 Elementos de la Firma Fuente: www.cisco.com

La figura 5.4 muestra la definición de la firma, rango de riesgo, credibilidad y el tipo de vulnerabilidad que protege.

Fig. 5.4 Boletín de Seguridad. Fuente: www.microsoft.com

C). Global Correlation

"Global Correlation" averigua el valor de la reputación de las direcciones IP que quieran enviar tráfico y utiliza dicho valor para influenciar el "Risk Rating" de las firmas del IPS, de tal manera que una IP con mala reputación obtendrá un "Risk Rating" mucho más alto que una IP con buena reputación.

La información de los atacantes con su reputación es enviada a una base de datos que se encuentra en internet (Cisco SensorBase) que recolecta la información de todos los IPS que lo tienen activado.

D). Updates

Las funcionalidades que utilizan SensorBase necesitan actualizarse constantemente cada día. Por otro lado, la funcionalidad de "firmas" se actualiza cada semana. Por ambos motivos se debe tener conectividad web hacia los servidores de actualización de Cisco en Internet. La figura 5.5 muestra como se realiza el update para el caso del SensorBase (Global Correlation).

1.-IPS inicializa la petición de actualización de datos de Reputación.

2.- EL sensor recibe información que contiene el nombre DNS de un servidor para conseguir los datos de las IP y su Reputación.

3.- Akamaized DNS le brinda el servidor más cercano.

4.- Se inicia el proceso de Download.

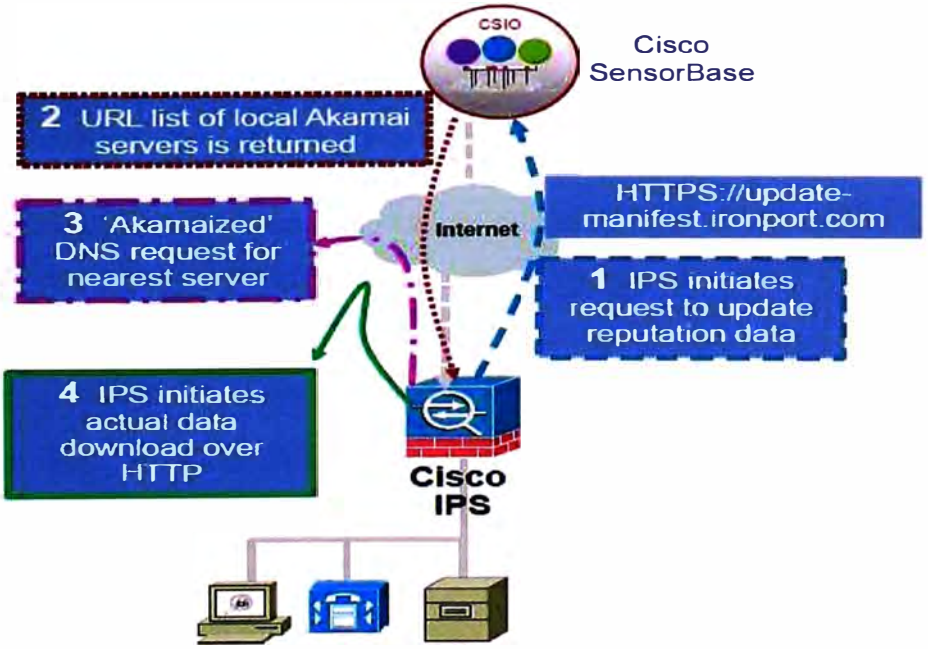

Fig. 5.5 Update por Medio del SensorBase Fuente: www.cisco.com

5.1.2.3 Información del Entorno.

Es necesario brindar al IPS información sobre el entorno en el cual se despliega, para que de esta manera el IPS sea más preciso al momento de diferenciar el tráfico legítimo del tráfico malicioso.

A) Risk Ratings (RR) y Target Value Ratings (TVR)

Risk Rating (RR): es un valor que indica el grado de riesgo de los eventos detectados por el IPS. Este valor es calculado automáticamente y el resultado es un valor entre 0 y 100.

Target Value Rating (TVR): es un valor configurable por el usuario y que refleja la importancia de los equipos a proteger por el IPS.

El TVR es un multiplicador del RR y puede tomar los siguientes valores:

Low : multiplicador por 0.75

Medium : multiplicador por 1 (éste es el valor por defecto)

High : multiplicador por 1.5

Mission Critical: multiplicador por 2

Digamos que cierto evento tiene por defecto un RR = 40 y que queremos proteger la IP 10.10.10.10 a la cual asociamos un TVR=Mission Critical.

Esto quiere decir que el RR del evento será 40 x 2 = 80 si es que dicho evento está relacionado a la IP 10.10.10.10.

Sin embargo, si un evento similar es detectado para cualquier otra IP entonces el RR será simplemente 40, ya que las demás IPs tienen configurado por defecto un TVR=medium, el cual es un multiplicador x 1.

B) OS Mappings y Passive OS Fingerprinting

Muchos ataques son relevantes sólo para ciertos sistemas operativos. Por ello, si supiéramos cuáles son los sistemas operativos que se utilizan en los equipos a los cuales protegemos, entonces obtendríamos menor cantidad de falsos positivos.

La funcionalidad "OS Mappings" permite configurar manualmente la IP y el sistema operativo de cada equipo que protegemos.

Por otro lado, la funcionalidad "Passive OS Fingerprinting" permite descubrir automáticamente las IPs y los sistemas operativos que no hemos declarado con la funcionalidad anterior.

A continuación se muestran los "OS-Mappings" y "TVRs" de las IPs a proteger.

Tabla 5.1 Lista de Servidores

IPS-1			
Equipo	***IP***	***Sist. Operativo***	***Target Value Rating***
Servidor de Correo	IP_Address	Solaris 10	Mission Critical
Ironport C160	IP_Address	AsyncOS (basado en FreeBSD)	Mission Critical

C) SensorBase – Reputación dinámica de direcciones IP

SensorBase es el servicio de reputación de direcciones IPs que Cisco creó a partir del servicio Ironport Senderbase.

Originalmente, IronPort Senderbase se retroalimentaba de la base instalada de equipos Ironport, la cual cubre más del 25% del tráfico mundial de correo electrónico y tráfico web.

Con la adquisición por parte de Cisco, se hizo una reingeniería para utilizar la tecnología de Senderbase en los equipos Cisco, lo cual resultó en la nueva base de datos SensorBase, lo cual se retroalimenta de una base instalada de equipos mucho más grande.

Los Cisco IPS pueden beneficiarse de SensorBase a partir del sistema operativo 7.0. Las nuevas funcionalidades del IPS son "Reputation Filtering" y "Global Correlation", las cuales se mencionan en la sección "5.1.2.2".

Para que dichas funcionalidades trabajen adecuadamente, es necesario que se permita acceso a los puertos 80/443 y además al servicio DNS.

D) Detección de Falsas Alarmas.

La activación de mecanismos que pueden generar alarmas que son falsos positivos o falsos negativos. Estas alarmas deben abordarse en la implementación de un IPS.

Una alarma del tipo falso positivo es un resultado esperado, pero no deseado. Una alarma de falso positivo se produce cuando un sistema genera una alarma de intrusión después de procesar el tráfico de un usuario normal que no debería haber dado lugar al disparo de la alarma. El análisis de los falsos positivos limita el tiempo que un analista de seguridad ha de examinar la actividad intrusiva real en una red. Si esto ocurre, el administrador debe asegurarse de ajustar el IPS a cambio del tipo de alarma verdaderos negativos.

Un verdadero negativo es el resultado que describe una situación en la que el tráfico normal de la red no genera una alarma.

Un falso negativo es cuando un sistema de intrusión falla al no generar una alarma después del procesamiento del tráfico del ataque para el cual el sistema de intrusión está configurado para detectar. Es imperativo que el sistema de intrusión no genere falsos negativos, ya que significaría que los ataques no se detectan. El objetivo es hacer que este

tipo de alarma sea del tipo verdadero positiva.

Un verdadero positivo describe una situación en la que un sistema genera una alarma de intrusión en respuesta al tráfico de ataques conocidos.

Tabla 5.2 Tipos de Alarmas

Tipo de Alarma	Actividad en la Red	Actividad del IPS	Resultado
Falso Positivo	Tráfico Normal Usuario	Genera Alarma	Verificar
Falso Negativo	Tráfico Malicioso	No genera Alarma	Verificar
Verdadero Positivo	Tráfico Malicioso	Genera Alarma	Correcto
Verdadero Negativo	Tráfico Normal Usuario	No genera Alarma	Correcto

5.1.2.4 Funcionamiento en conjunto

Cuando el tráfico es recibido por el Cisco IPS es analizado por los siguientes módulos:

a) Reputation Filter, si el valor de reputación es el más bajo posible, entonces el tráfico será denegado inmediatamente, de no ser así se continúa el análisis en el siguiente módulo

b) Signature Inspection, se verifica cuál es el valor de riesgo (Risk Rating) para decidir si el tráfico es denegado o permitido. En cualquiera de los casos el tráfico es enviado al siguiente módulo "global correlation"

c) Global correlation, aquí el valor de riesgo (Risk Rating) puede ser influenciado por la reputación de la IP y con ello finalmente se decide si se bloquea o permite el tráfico, la información del atacante es enviada al Cisco "SensorBase" con su reputación.

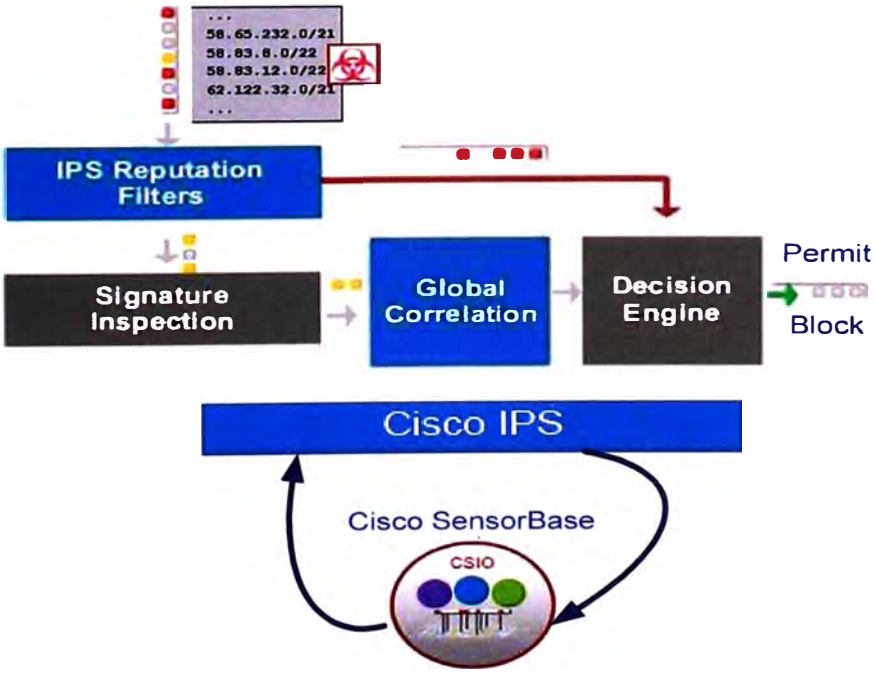

Fig. 5.6 Funcionamiento del Cisco IPS en su conjunto Fuente: www.cisco.com

5.2 Presupuesto de Equipos.

En la tabla 5.2 se muestra el presupuesto de los equipos principales del Sistema de Seguridad Perimetral.

Tabla 5.2 Precios de equipos

Cantidad	Producto	Descripción	Precio Unitario	Total
1	Lucent VPN Firewall Brick 700	Firewall	$ 14,727.90	$ 14,727.90
2	IPS 4240	IPS	$ 7,242	$14,484

5.3 Topología Física de RED

El siguiente grafico muestra como estaba la red al inicio, contaba con disponibilidad de conectividad pero la parte de seguridad estaba limitada porque solo existía un solo Firewall. Véase Fig. 5.7

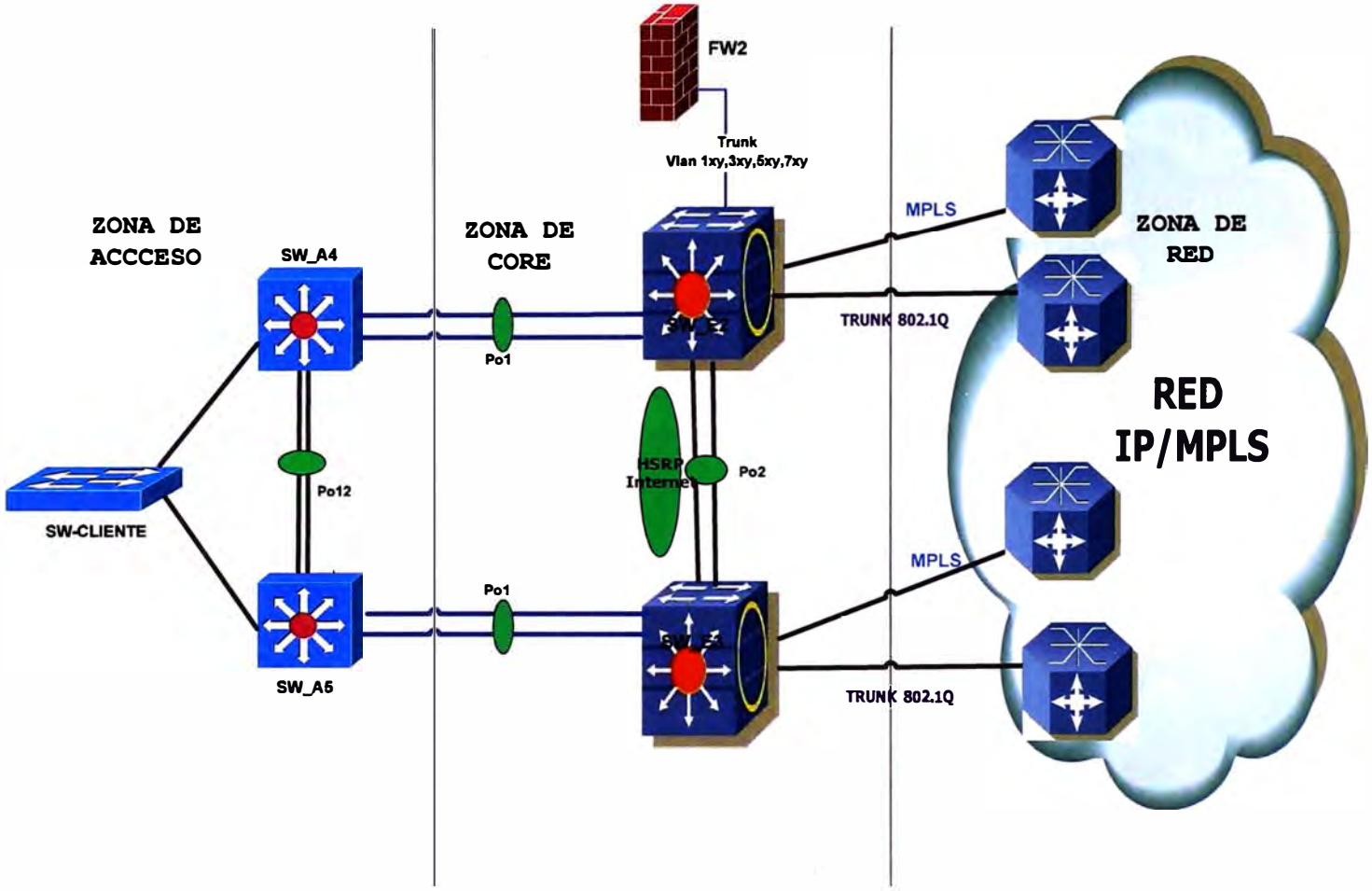

Fig. 5.7 Topología de Red Inicial.

5.3.1 Topología física de los FIREWALL

a) La fig. 5.8 muestra la ubicación física de los dispositivos de seguridad perimetral: Firewall, IPS y la redundancia en equipos de conectividad, llegando al SW-Cliente. Al momento de producirse la pérdida de conectividad en el SW conectado al FW activo, todo el tráfico es desviado al segundo SW (SW-E3). En el anexo C muestra el tráfico producido durante una intermitencia.

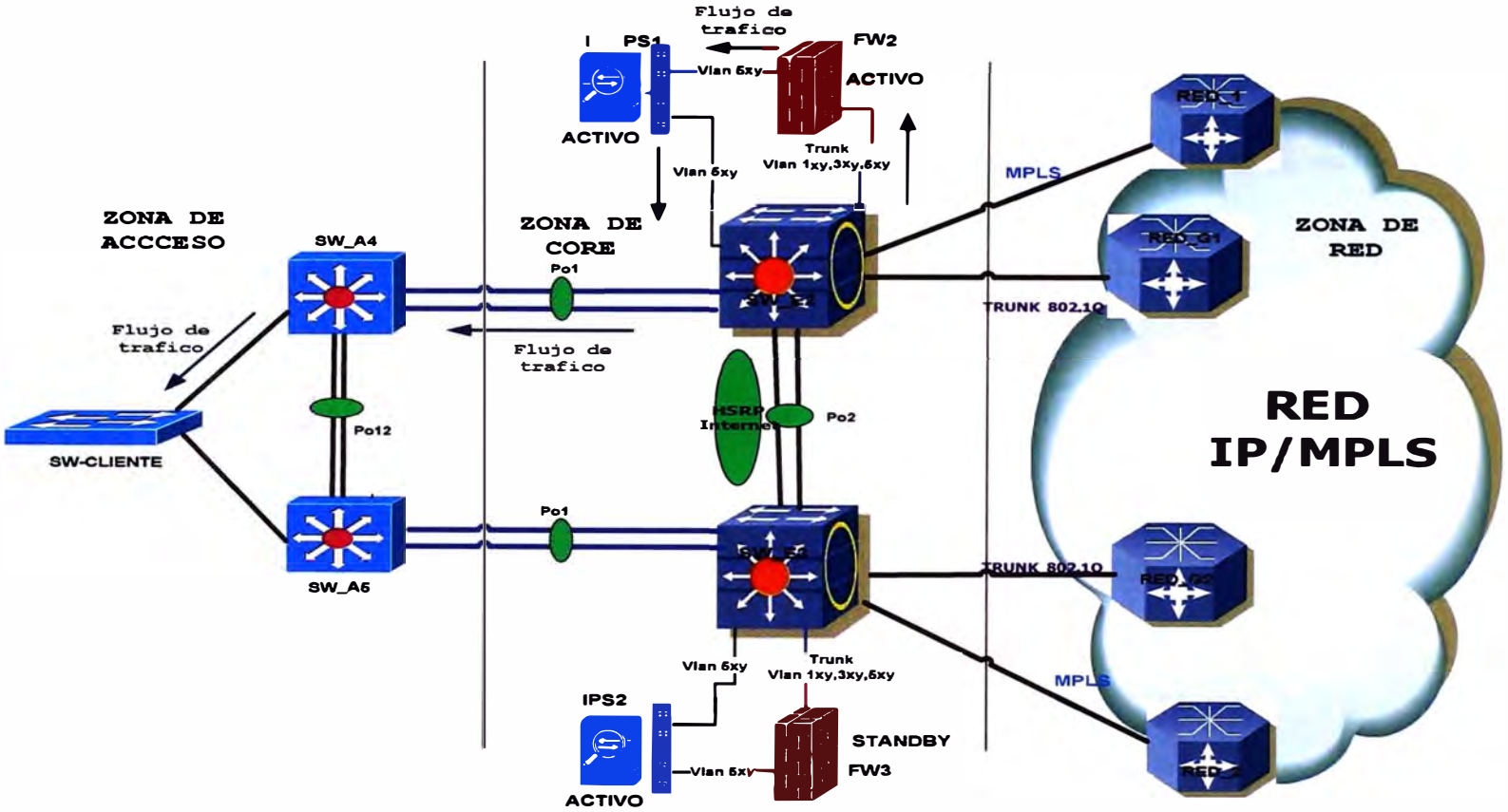

Fig. 5.8 Topología Física del Firewall

b) La alta disponibilidad del Firewall se logra mediante la conexión entre las interfaces Eth de cada dispositivo con el servicio llamado Heartbeat propio del fabricante (Cisco, Fortinet, Alcatel Lucent, CheckPoint, etc.). Véase Fig.5.9.

El Anexo C muestra el momento que gatilla el Failover y el flujo de tráfico es trasladado al Firewall StandBy.

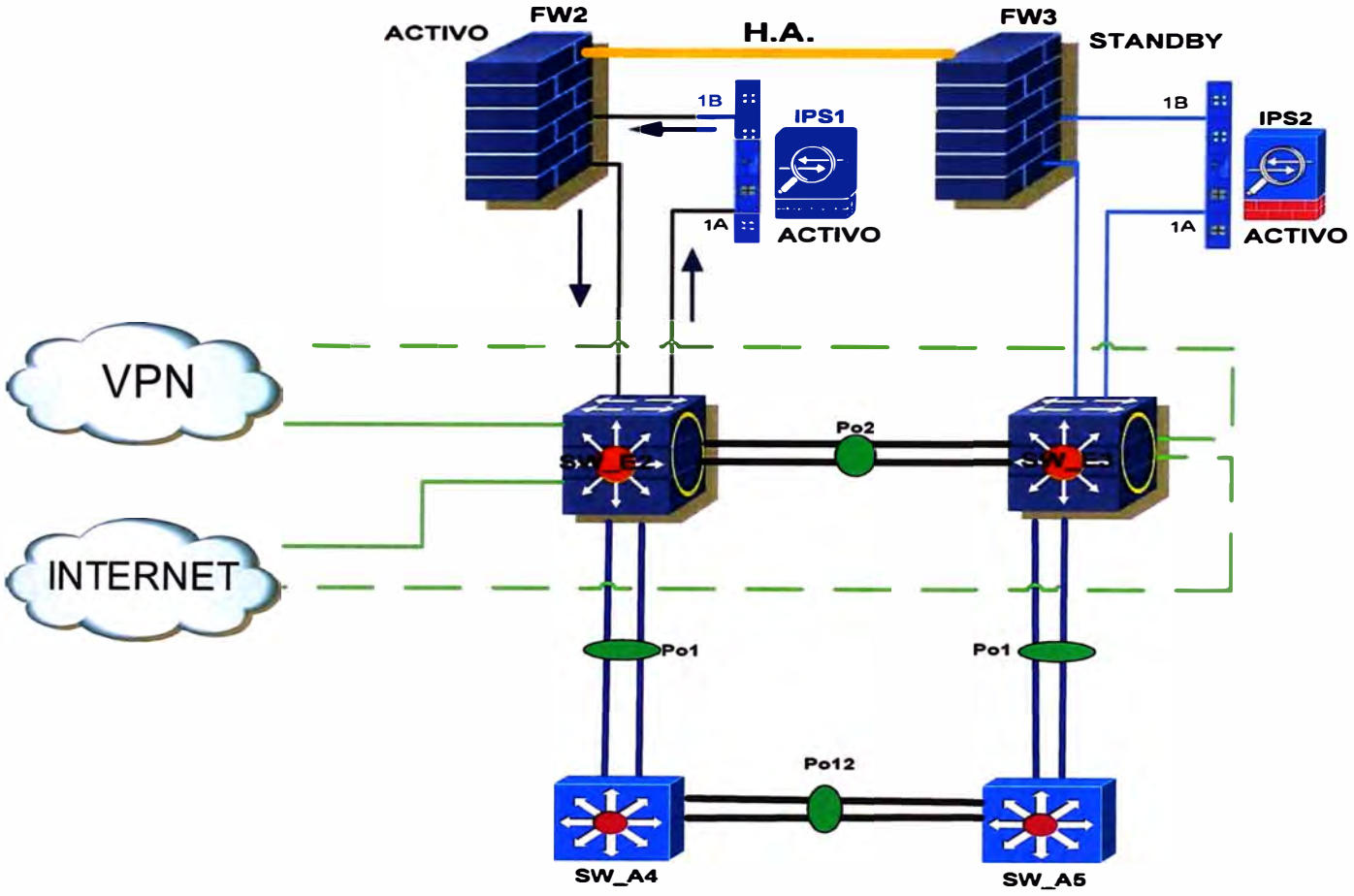

Fig. 5.9 Alta Disponibilidad De Firewall

5.3.2 Topología Física de los IPS

En la Fig. 5.10 muestra el diagrama de conexión del IPS en el sistema de seguridad perimetral propuesto, el IPS se coloca al mismo nivel que el Firewall, teniendo como prioridad el análisis del tráfico que viene de internet hacia la red de servidores o red LAN. Los IPS trabajan en modo activo, cuando se cae uno de los IPS este trabajan como un cable, dejando pasar el trafico sin haber perdida de servicio.

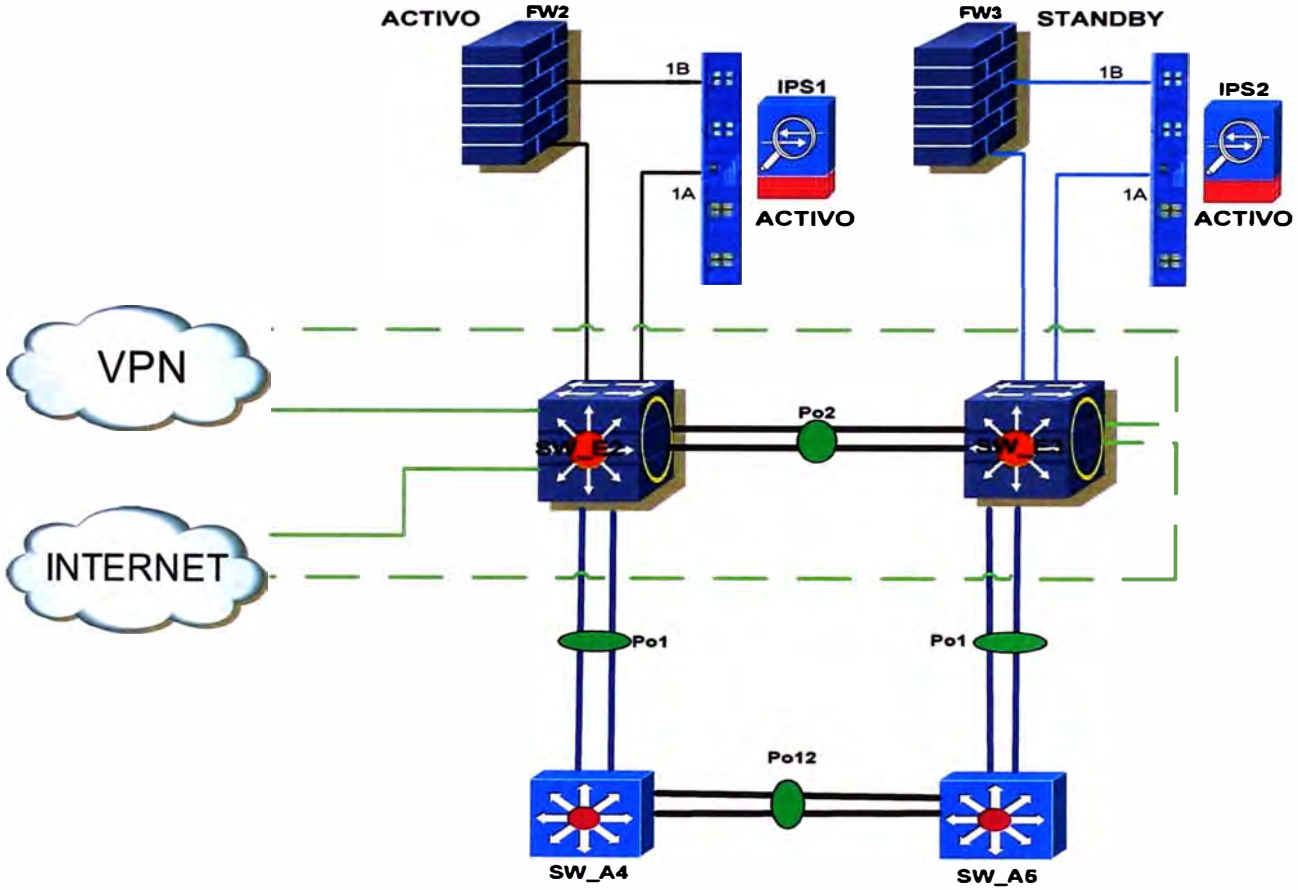

Fig. 5.10 Diagrama de conexión del IPS

5.3.3 Diagrama Físico del acceso VPN.

a) La topología de conexión VPN es como se muestra en el grafico 5.11 donde hay un router concentrador VPN, un servidor de Gestión de acceso para usuarios tanto para la VPN y los Dispositivos de red (Servidor ACS).

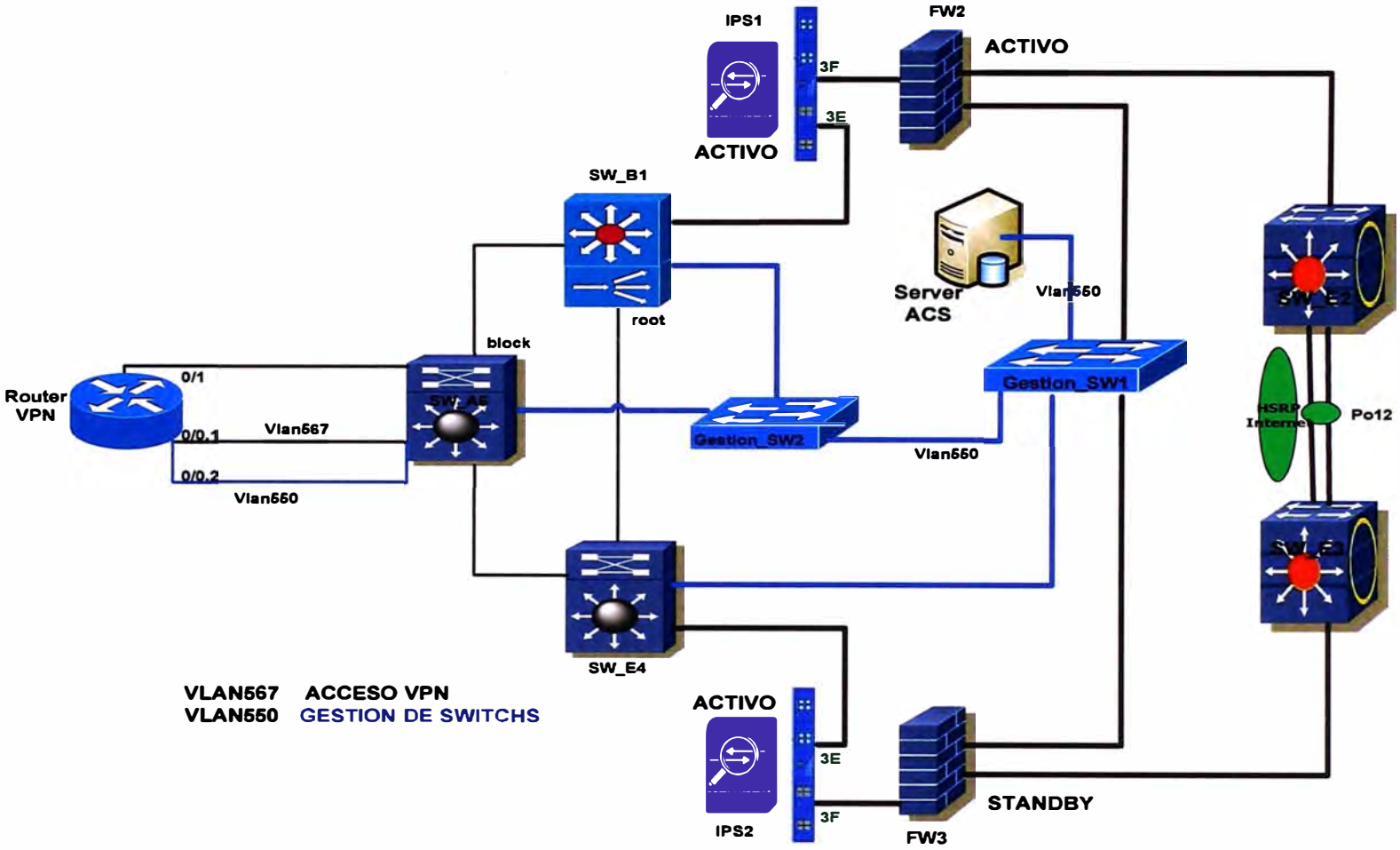

Fig. 5.11 Topología de Conexión VPN.

5.4 Topología Lógica de Red

5.4.1 Diagrama Lógico del acceso vía VPN.

a) La figura siguiente explica el flujo de tráfico que tiene los usuarios al momento de ingresar a la VPN, ya sea desde el mismo local de la empresa (Datacenter) o desde internet. Véase Fig.5.12.

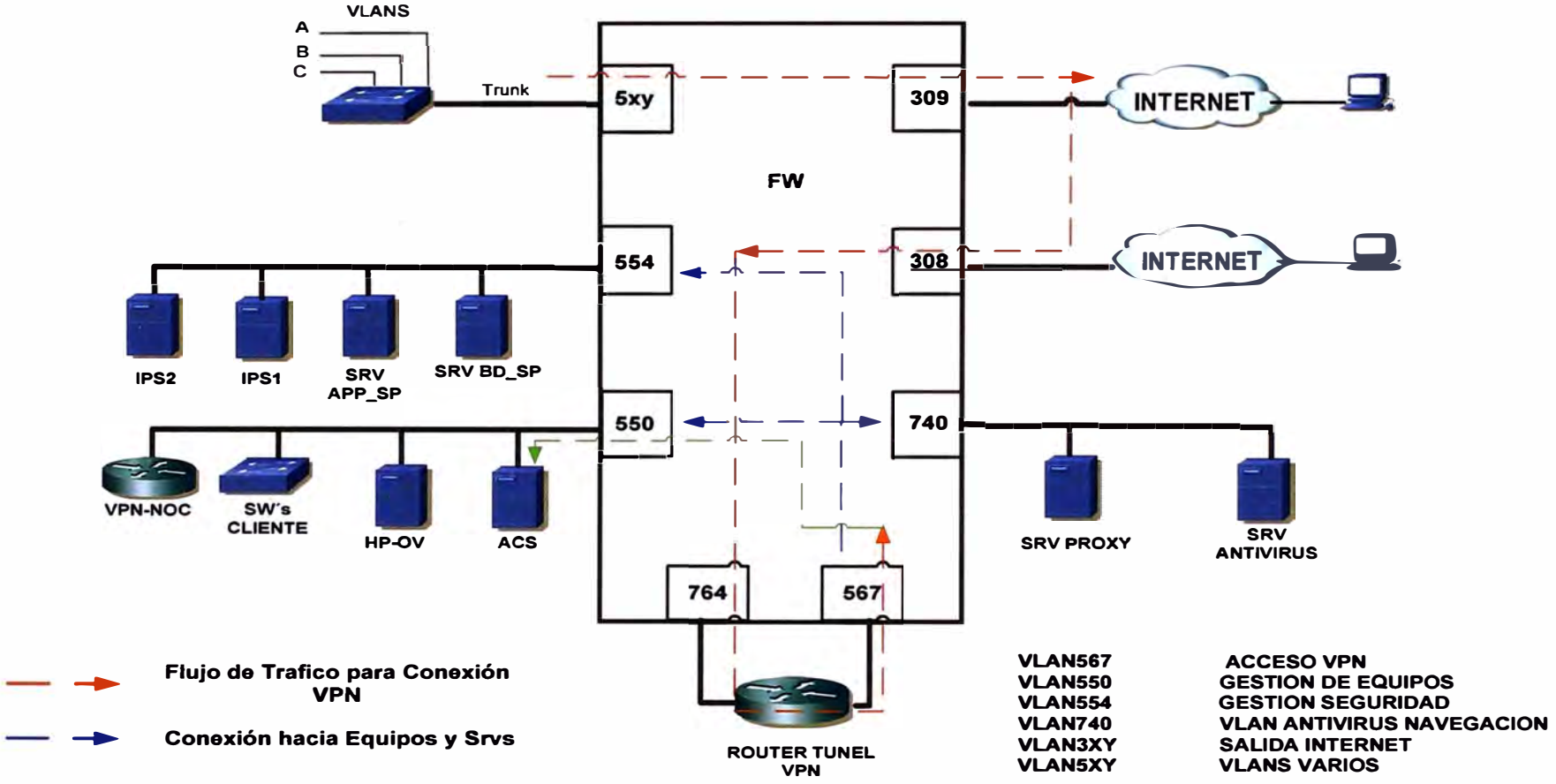

Fig. 5.12 Diagrama de Flujo de Conexión VPN.

b) Mediante el grafico 5.13 vemos los diferentes tipos de aéreas que acceden a los dispositivos de red (switches, routers, servidores , etc), donde el servidor ACS brinda un control de acceso y designa políticas de acuerdo al rol que desempeñan.

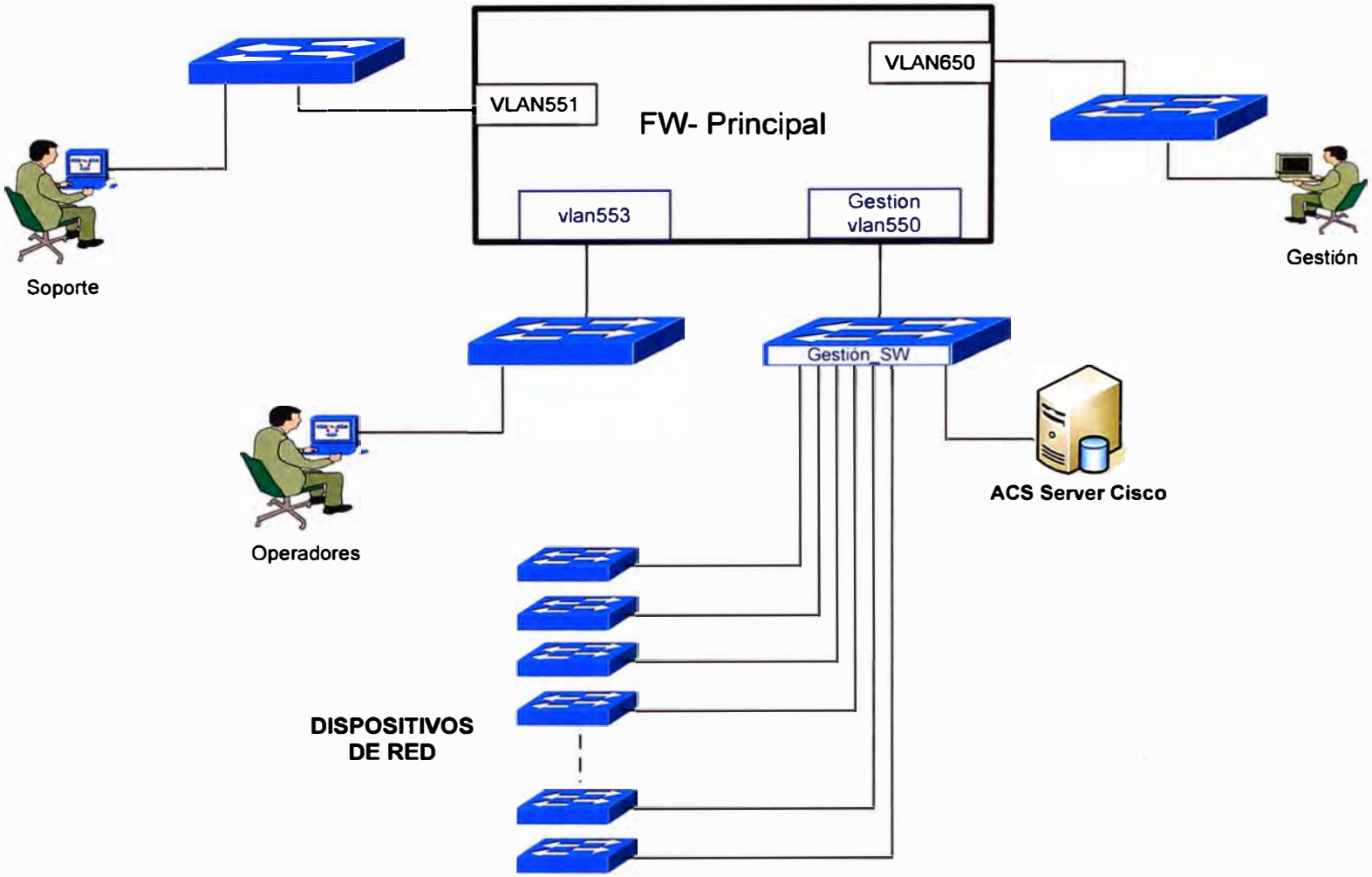

Fig. 5.13 Diagrama lógico de Gestión de Dispositivos de Red

5.4.2 Topología Lógica Servidores y equipos de Gestión.

a) La Fig. 5.14 muestra la ubicación lógica de los servidores de seguridad en sus respectivas VLAN dentro del firewall, creando diferentes redes virtuales para cada área dentro de la empresa (Datacenter).

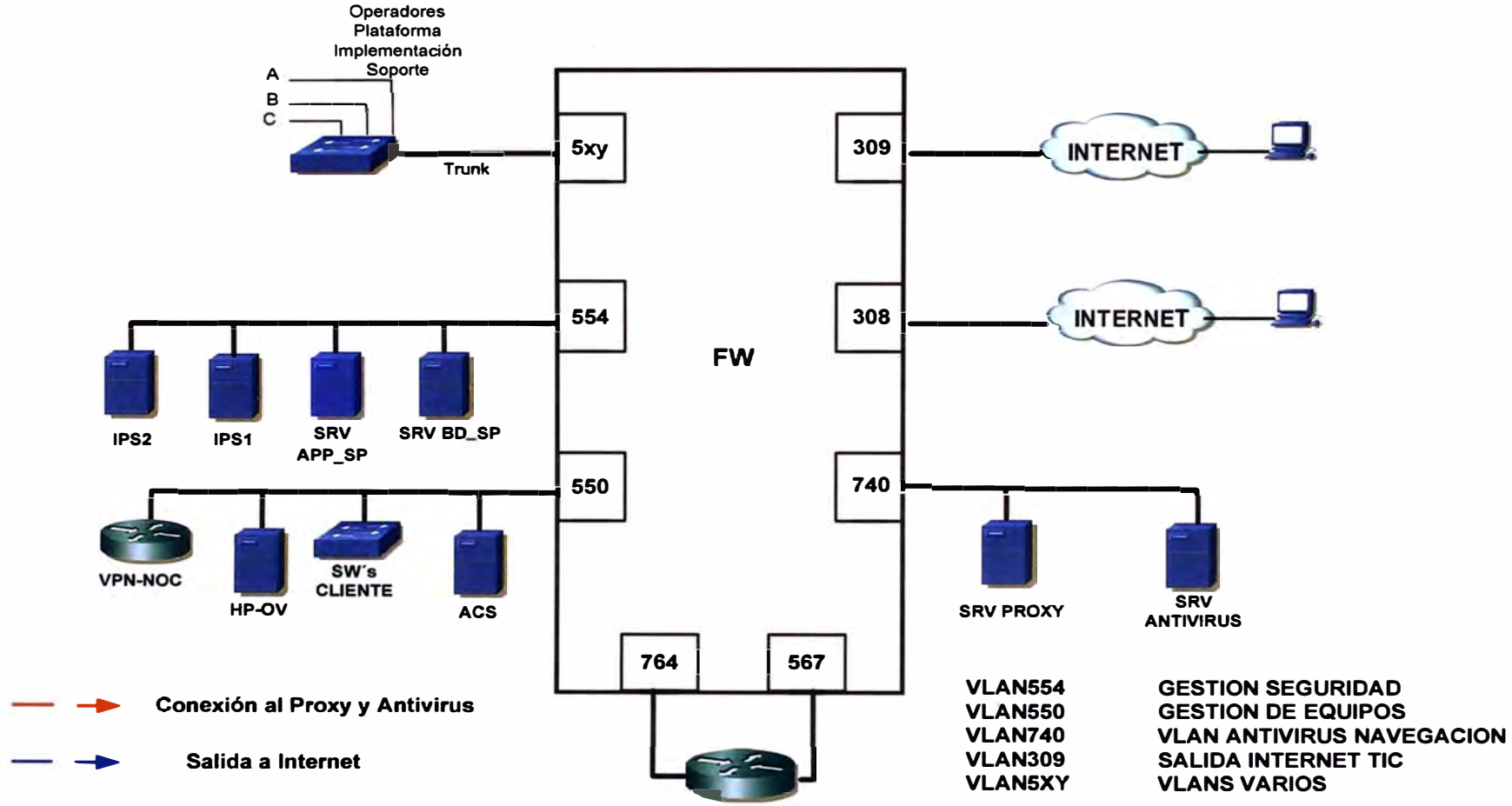

Fig. 5.14 Diagrama Lógico Servidores

b) La topología que presenta la Fig.5.15 es la ubicación física de los servidores que brindan el servicio de Proxy, Antivirus, Token , Cacti y servidores de Base de Datos, configurado en un equipo llamado Blade Server.

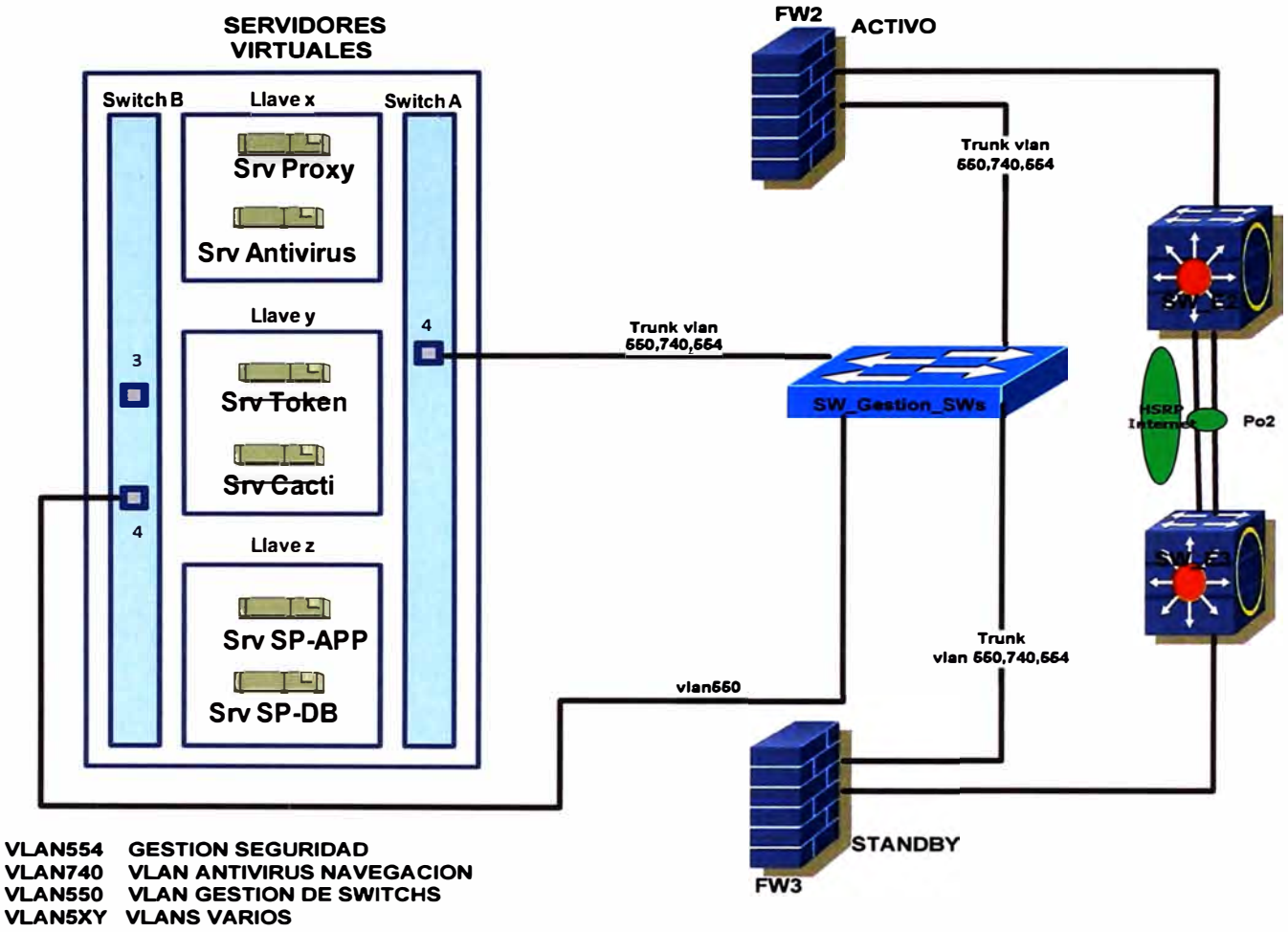

Fig. 5.15 Distribución Servidores Internos

5.4.3 Diagrama Lógico Tráfico de Navegación y Antivirus

La Fig.5.16 muestra la forma como los usuarios se conectan al servidor antivirus y descargan las actualizaciones y el acceso a internet por medio del servidor Proxy. Los usuarios y servidores se conectan a una VLAN creada especialmente para "Navegación y Antivirus".

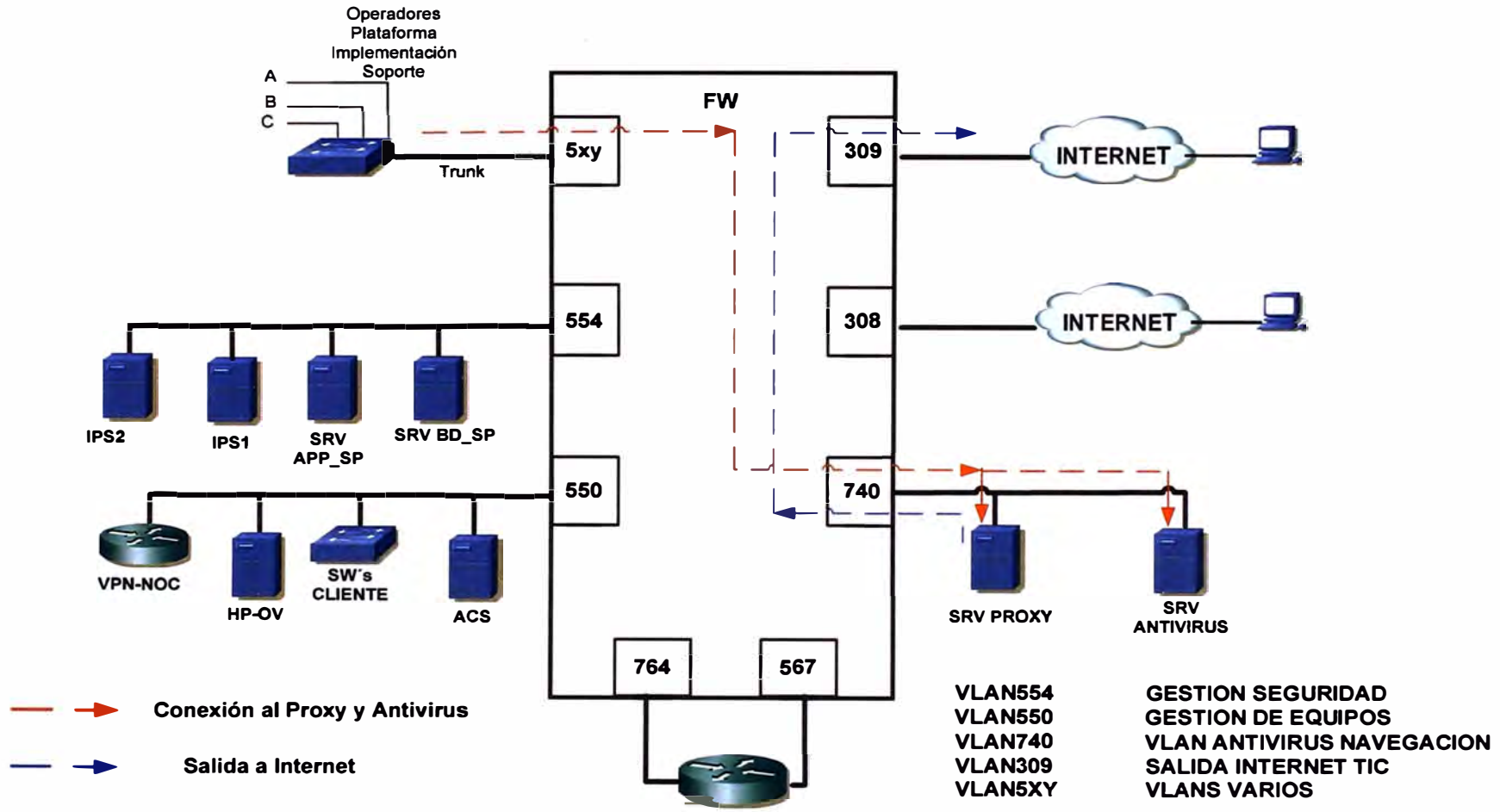

Fig. 5.16 Topología de Flujo de Salida Internet

CONCLUSIONES Y RECOMENDACIONES

1.- La realización de este trabajo ha permitido la obtención de una mayor compresión de la seguridad en las redes IP. No solo se ha profundizado en el estudio de los diferentes dispositivos que nos ayudan a comprender la importancia que tienen en la actualidad, sino en los diferentes tipos de vulnerabilidades y políticas de seguridad para prevenirlos.

Son numerosos los ataques analizados que se basan en explotar algunas características de los protocolos de comunicación. Estos ataques buscan o bien el cese de las actividades o servicios que presta el ordenador atacado (ataques de denegación de servicio) o conseguir un acceso dentro de la máquina que le permita utilizarla a su conveniencia.

El uso de herramientas de seguridad clásica basado en filtrado simple de paquetes (firewall) se ha revelado insuficiente antes los ataques organizados. Cuando el atacante es único y está perfectamente identificado (por la dirección IP usualmente) los sistemas básicos de seguridad pueden resultar un muro de defensa relativamente efectivo.

Sin embargo, cuando el atacante no está identificado de una forma explícita o el número de atacantes es desconocido (ataques de denegación de servicio distribuido), estos sistemas no pueden dar la respuesta adecuada.

2.- Debemos tener en cuenta que muchas veces no basta únicamente con protegernos de las posibles amenazas que provienen de internet. En el caso de que un sistema fuera comprometido por el motivo que fuese, el resto de ataques que lanzaría el atacante hacia nuestra red serían ataques internos que pasarían desapercibidos.

Los sistemas de prevención de intrusos (IPS) son mecanismos de seguridad activa que se encargan de monitorizar todo el tráfico existente en nuestra red, tanto local como remota.

Los sistemas IPS unen la capacidad de filtrado del trafico con la detección de firmas (patrones específicos de ataques conocidos) y el seguimiento de las comunicaciones desde un nivel de flujo de las comunicaciones.

Lo problemático de estos sistemas son principalmente la posibilidad de generar falsos positivos que pueden desvirtuar la efectividad del sistema, además de generar una inmensa cantidad de información al tratar con todo el trafico existente en la red (benigno y maligno)

lo que dificulta el análisis posterior.

3.- Tener presente que antes de realizar una implementación de un IPS, es recomendable que el dispositivo primero este en trabajando en modo promiscuo, porque es ahí donde se puede verificar el tipo de trafico que está pasando por la red, además de ver qué tipo de signature se debería utilizar si hubiera algún tráfico malicioso.

Teniendo el IPS en el modo promiscuo y luego en modo inline, los valores de falsos positivos disminuirán y será más confiable al momento de realizar el bloqueo de tráfico.

4.- Las conexiones que realizamos hacia los equipos de seguridad deben estar configuradas en una red "out of band" es decir diferente al intranet, dichas conexiones se establecen mediante conexiones VPN ya sea IpSec o SSL para garantizar la encriptación de la data.

De acuerdo a las políticas de seguridad se darán los permisos para cada una de las áreas de nuestra compañía o niveles de acceso según desempeño del administrador junior o administrador sénior.

Las conexiones VPN nos permiten un grado mayor de seguridad en la transferencia de información, establecimiento de sesiones, ingresos a los servidores desde internet.

5.- La función del servidor Proxy en el diseño de seguridad es poder controlar el filtro de páginas a los usuarios mediante políticas que se implementan en las compañías de acuerdo al aérea y función que desempeñan, es muy importante trabajar con los filtros web (Proxy o WebSense) ya que nos proporcionan un control interno de ataque que vienen de las URL´s, o también aplicativos de mensajería como MSN, AOL, etc.

Otro nivel de seguridad para la Intranet es la instalación de servidores Antivirus (McaFee EPO; Nod32, Karpesky, etc), trabajan como IPS dentro de las PCs de los usuarios o los Servidores para proteger tanto la maquina como la red interna, los antivirus trabajan como pequeños Firewall o Antispam de acuerdo a la tecnología.

6.- Para la administración de los Firewall, IPS y de cualquier equipo de seguridad, es recomendable tener personal con conocimiento y experiencia de la tecnología y el tráfico que transita en la red, porque ante cualquier intermitencia, ataque o problema, el personal pueda actuar rápido y no afecte mucho en los servicios.

7.- Los sistemas de monitoreo en la actualidad se han vuelto muy importante para las empresas en temas de: administración de eventos, visualización de tráfico de red, detección de intrusos. Por ello es recomendable siempre tener servidores correlacionadores instalados en la red porque ayudan a desarrollar una mejor gestión de los eventos, un análisis más minucioso frente alguna incidencia y la generación de reportes.

ANEXO A

DOMINIOS Y ORGANIZACIONES DE SEGURIDAD EN REDES.

1.- Organizaciones de Seguridad en Redes

Los profesionales dc seguridad en redes deben colaborar con colegas profesionales con más frecuencia que en muchas otras profesiones. Esto incluye la asistencia a talleres y conferencias que a menudo son afiliadas, patrocinadas u organizadas por organizaciones dc tecnología local, nacional, o internacionales.

a) Tres de las organizaciones de seguridad más reconocidas son:

b) SysAdmim Audit Network Security (SANS) Institute.

c) Computer Emergency Response Team (CERT).

International Information Systems Security Certification Consortium (pronounce (ISC)2 as "I-S-C-squared").

1.1 SANS Institute: SANS fue establecido en 1989 como una investigación cooperativa y organización de educación. El enfoque de SANS es la capacitación y la certificación de seguridad de la información. SANS desarrolla documentos de investigación sobre varios aspectos de la seguridad dc la información.

Una serie de individuos, auditores, administradores de red, oficiales y jefes de seguridad de la información, comparte lecciones aprendidas y soluciones. En el corazón de las redes SANS hay profesionales de seguridad en diversas organizaciones mundiales, practicantes de seguridad en muchas empresas, universidades, trabajando juntos para ayudar a toda la comunidad de seguridad en redes.

SANS desarrolla cursos de seguridad que pueden ser tomados para prepararse para la Global information Assurance Certification (GIAC) en auditoria, administración, operaciones, asuntos legales, administración de seguridad, y seguridad de software. El GIAC valida las habilidades de profesionales de seguridad, desde el nivel de seguridad de la información inicial hasta áreas avanzadas como la auditoría, detección de intrusos, gestión de incidentes, firewall, protección perimetral, análisis forense de datos, técnicas de los hackers, Windows, sistema operativo UNIX de seguridad, software seguro y codificación de aplicaciones.[19]

1.2 Computer Emergency Response Team (CERT): CERT responde a incidentes de seguridad, análisis de las principales vulnerabilidades de productos. Trabaja para administrar los cambios relativos a las técnicas de intrusión progresivas y la dificultad para descubrir ataques y capturar atacantes. El CERT desarrolla y promueve el uso de tecnología apropiada, prácticas de dirección de sistemas para resistir a ataques contra sistemas conectados a una red para limitar el daño y asegurar la continuidad de servicios.

CERT se concentra en cinco áreas: el aseguramiento de software, los sistemas de seguridad, la seguridad de la organización, coordinación de respuesta, educación y formación de profesionales.

Difunde información publicando: artículos, investigaciones, informes técnicos y documentos sobre una variedad de temas de seguridad. CERT trabaja con los medios de comunicación para crear conciencia de los riesgos en el Internet y los pasos que los usuarios pueden tomar para protegerse. CERT trabaja con otras organizaciones de tecnología principales, como FIRST e IETF, para aumentar el compromiso de la seguridad y supervivencia. También asesora a las organizaciones del gobierno estadounidenses, como el Centro de Evaluación de Amenaza Nacional, el Consejo Nacional de Seguridad, el Consejo de Seguridad de Patria [20].

1.3 $(ISC)^2$: La misión de $(ISC)^2$ es hacer que el mundo cibernético sea un lugar seguro mediante boletines, artículos, etc. con el fin de elevar el nivel de seguridad de la información en internet y promover el desarrollo de profesionales de seguridad en todo el mundo.

Es universalmente reconocido por sus cuatro certificaciones de seguridad de la información, incluida una de las certificaciones más populares en la profesión de seguridad de redes: Profesional de Seguridad de Sistemas de Información Certificado (CISSP). Estas credenciales ayudan a asegurar que los empleadores con empleados certificados, mantenga los activos de la información e infraestructura seguros.

(ISC)2 promueve la experiencia en el manejo de las amenazas de seguridad a través de sus programas de educación y certificación. Como miembro las personas tienen acceso a la información actual de la industria y la oportunidad de pertenecer a la red de profesionales certificados de seguridad de la información.

Varias otras organizaciones de seguridad de red son también importantes para los profesionales de seguridad de red. El "InfoSysSec" es una organización de seguridad de red que aloja un portal de noticias de seguridad, proporcionando las últimas noticias de última hora en relación a alertas, exploits y vulnerabilidades. La "Mitre Corporation" mantiene una lista de vulnerabilidades y exposiciones comunes (CVE) utilizados por organizaciones de seguridad importantes. Finalmente "FIRST" es una organización de seguridad que reúne una gran variedad de equipos de respuesta a incidentes de seguridad: Entidades del gobierno, Centros de Comercio y Organizaciones Educativas para fomentar la cooperación, coordinación y prevención de incidentes mediante una rápida reacción.

Fig.A.1 Organizaciones de Seguridad de Red Fuente: www.cisco.com

2.- Dominios de Seguridad en Redes.

Es de vital importancia para los profesionales de seguridad en redes comprender los estándares internacionales (ISO) y estar familiarizado con las organizaciones dedicadas a su desarrollo, tener una comprensión de los diferentes dominios de seguridad proporciona un marco organizado para facilitar el aprendizaje acerca de la seguridad.

Hay 11 dominios de seguridad especificada por la Organización Internacional de Normalización (ISO) / Comisión Electrotécnica Internacional (IEC) descrito por la norma ISO / IEC 27001 [22], los dominios sirven para organizar a un alto nivel la seguridad en redes y tienen algunos paralelos importantes con dominios definidos por la certificación CISSP.

2.1 Estructura del ISO 27001.

La cobertura del estándar ISO 27001: Véase Fig. A4. :

a) Política de Seguridad
b) Organización de la Seguridad.
c) Clasificación y Control de los Activos.
d) Seguridad de los RRHH.
e) Seguridad Fisica y del Entorno.
f) Gestión de Comunicaciones y Operaciones.

g) Control de accesos.

h) Desarrollo y Mantenimiento.

i) Gestión de Incidencias.

j) Gestión de Continuidad.

k) Cumplimiento.

Fig.A2 Estructura del ISO 27001

Fuente: www.iso27000.es

ANEXO B
ESPECIFICACIONES TECNICAS DE LOS EQUIPOS

A) Lucent Firewall Brick

Aplicaciones de seguridad que integran inspección de la capa de aplicación, función de firewall con capacidades de VPN avanzadas para oficinas pequeñas a través de los requisitos de centros de datos.

Servidor de gestión de seguridad (SMS) Alcatel-Lucent: software para firewall, VPN, calidad de servicio y VLAN sólido y perfectamente sincronizado, y gestión de políticas de firewall virtual [15]. Véase FigB1

Fig.B1 Firewall Brick Fuente: www.lucent.com

Características:

A) Procesador 2.8Ghz con 512MB de RAM.
B) IOS : Security System Hardened (Propietario de Lucent)
C) Software del Server Management Soporta: Windows 2003 Server, Solaris.
D) Hardware SUN WorkStation.
E) (8) 10/100/1000 TX puertos.
F) 1.7 Gbps Firewall.
G) 425Mbps 3DES
H) 1000 sesiones concurrentes.
I) 750 VPN túneles.
J) 350 virtual firewall.
K) SVGA video, DB9 serial, PS/2 keyboard, 4xUSB.
L) Number of VLANs supported – 4,094.
M) Normal Operating Temperature: 0 to 40° C.
N) 48.3 cm x 48.23 cm x 4.4 cm (1U) Rack Mountable per EIA-310 specification.
O) Sun Solaris™ 2.8, 2.9 or 2.10 on SPARC processors
P) USA – FCC Part 15, Class A certificaficaciones EMC
Q) Canada – IC-ES003 certificaciones EMC

B) Cisco Intrusion Prevention System (IPS)

Cisco IPS ofrece protección contra intrusos en tiempo real para el perímetro de la red, externa e interna. El sistema utiliza sensores, equipos de red de alta velocidad que analizan y detectan cualquier actividad sospechosa. Ver FigB.2

Fig.B2 Intrusión Prevention System. Fuente: www.cisco.com

Características:

- Modelo Cisco IPS 4240
- IOS : IPS-4240-K9-sys-1l-a-7.0.4-E4.img
- Signature Update : IPS-sig-S581-req-E4.pkg
- Thoughput : 250 Mbps
- Conexiones: 2500 Conexiones nuevas TCP por segundo
- 2500 HTTP transacciones por segundo.
- Enclosure : 1 Unidad de Rack.
- Dimensiones: 4.37cm (H) x 43.82 cm(W) x 36.83 cm(D).
- Peso 9.07 kg.
- interfaces de Monitoreo: Cuatro 10/100/1000BASE-T
- Interfaces de Administración: One 10/100BASE-T
- Bypass de Hadware integrado: si
- IPS 4240 no soporta redundancia en Fuente de poder.
- Frecuencia : 47 to 63 Hz.
- Voltage : 100V to 240V AC
- Valor de Corriente : 3.0 A
- Potencia Constante : 150W y Maximo 190 W.
- Dinámico Sistema de Calificación para los ataques (Risk Rating).
- IPS can trabajar en Modo "Inline" , "Promiscuo" o en ambas opciones.
- Software de Administración de eventos y Politicas (IME, IDM).

C) Router Concentrador VPN.

Los Cisco 2800 Series Integrated Services Routers ofrecen diferentes características, entre las que se incluyen:

* Seguridad integrada, como firewall, cifrado y protección contra piratas informáticos.
* Conector de suministro de energía redundante integrado en la mayoría de los modelos para una mayor protección.
* Mayor confiabilidad y flexibilidad que le permite dar prioridad al tráfico de voz o al intercambio de datos para que la entrega de información se adapte a las necesidades de su empresa.
* Soporte para conexiones de red privada virtual para conectar socio de negocios y oficinas remotas.
* Soporte para cobertura LAN inalámbrica en toda la oficina con una seguridad robusta y capacidades de acceso de invitado, que soportan todos los estándares inalámbricos IEEE 802.11a/b/g/n.
* Diferentes opciones de conectividad de banda ancha y red.
* Opciones de suministro de energía a los dispositivos de red a través de su conexión Ethernet (Power Over Ethernet) para reducir los costos de cableado. Ver FigB.3.

Fig.B3 Router 2811 concentrador VPN. Fuente: www.cisco.com

Características.

- Dos interfaces integradas 10/100 FastEthernet Ports.
- IOS : c2800nm-advipservicesk9-mz.124-25e.bin
- Memory upgrade for both Flash and DRAM: (32-MB Flash and 128-MB DRAM)
- Soporta arriba de 1500 VPN con el AIM-EPII-PLUS Modulo.
- Antivirus Defense por Medio de NAC.
- Software IOS de Firewall y IPS.
- Opcional soporte de layer 2 con Power Over Ethernet (PoE).

D) Cisco Catalyst 2960 Series Switches.

Los switches de Cisco Catalyst 2960 Series ofrecen una amplia gama de características, entre las que se incluyen:

* Soporte para comunicaciones de datos, inalámbricas y voz que le permite instalar una única red para todas sus necesidades de comunicación.
* Función Power over Ethernet que le permite implementar fácilmente nuevas funciones como comunicaciones por voz e inalámbricas sin necesidad de realizar nuevas conexiones.
* Opción de Fast Ethernet (transferencia de datos de 100 megabits por segundo) o Gigabit Ethernet (transferencia de datos de 1000 megabits por segundo), en función del precio y sus necesidades de rendimiento.
* Varias configuraciones de modelo con la capacidad de conectar escritorios, servidores, teléfonos IP, puntos de acceso inalámbrico, cámaras de TV de circuito cerrado u otros dispositivos de red.
* Capacidad de configurar LAN virtuales (VLAN) de forma que los empleados estén conectados a través de funciones de organización, equipos de proyecto o aplicaciones en lugar de por criterios físicos o geográficos.
* Seguridad integrada
* Funciones de supervisión de red y solución de problemas de conectividad mejoradas.

IOS : c2960s-universalk9-tar.122-58.SE1.tar Ver Fig.B.4

Fig.B4 Catalyst 2960 Series Fuente: www.cisco.com

E) Secure Access Control (ACS).

Para satisfacer las nuevas demandas para la gestión de control de acceso para las políticas cada vez más complejo que requiere su organización , Cisco Secure Access Control System es una plataforma de generación de políticas en un componente básico de la política de Cisco solución.

Se Obtiene los siguientes Beneficios:

* Implementar fácilmente con otros componentes Cisco TrustSec de un amplio control de

acceso y la solución de confidencialidad.

* Soporta dos distintos Protocolos de Autenticación : Radius, Tacacs+.

* Sistema Operativo: ADE-OS versión de compilación: 1.2.0.146 y ACS 5.1

* Utiliza múltiple Base de Datos para una mayor flexibilidad.

* IOS: propio de Cisco para estos dispositivos

* Disfrute de una fuerte y flexible políticas de control de acceso que puede incluir autenticación de varios dispositivos. Véase Fig.B5

Fig.B5 Secure Access Control System Fuente: www.cisco.com

F) Software de Scaneo de Trafico Malicioso.

a) Acunetix: Web Aplication Security.

* Escaneo avanzado y profundo contra inyección de SQL y Cross site scripting.

* Herramienta avanzada de pruebas de penetración, como el HTTP Editor y HTTP Fuzzer. grabador de macro de Visual hace pruebas de formularios web y áreas protegidas por contraseñas fáciles

* Soporte a las páginas con "Single Sign-on" y mecanismo "Two Factor authentication".

* Realización de Reportes detallado.

* Acunetix rastrea y analiza sitios web, incluyendo el contenido flash, SOAP y AJAX

* Explora puertos en el servidor web y ejecuta los controles de seguridad contra los servicios de red que se ejecuta en el server.

acunetix WEB APPLICATION SECURITY

Fig.B6 Acunetix Web Application Security Fuente: www.acunetix.com

b) CoreImpact.

CoreImpact es un software comercial automatizado para realizar pruebas de penetración, desarrollado por Core Security Technology, permite al usuario investigar y explotar las

vulnerabilidades de seguridad en las redes, aplicaciones de internet y redes inalámbricas.

Core Impact presenta las caracteristicas :

* Automatiza las tareas que consumen tiempo relacionado con la creación y explotación de la ejecución de pruebas de penetración.
* Permiten a los usuarios realizar pruebas a través de múltiples configuraciones y vectores de ataques que simulen los mismos ataques hacia los activos de TI.
* Las son consistentes y repetibles para establecer una línea de base y demostrar la eficacia de los sistemas de seguridad y los esfuerzos de remediación.
* Velocidad en pruebas de penetración con el lanzamiento de ataques múltiples y simultaneos.

Mayor Información en el siguiente link [17]:

http://www.coresecurity.com/content/features-and-benefits-pro

Fig.B7 Core Impact Software. Fuente: www.coresecurity.com

ANEXO C:

REPORTES Y EVIDENCIAS DE CONTINUIDAD DEL SERVICIO.

1.- Alta Disponibilidad de los Firewall.

A) La Fig.C.1 muestra la interfaz Gig2/0/2 del SW_E2 hacia el FW1 en un periodo de un mes.

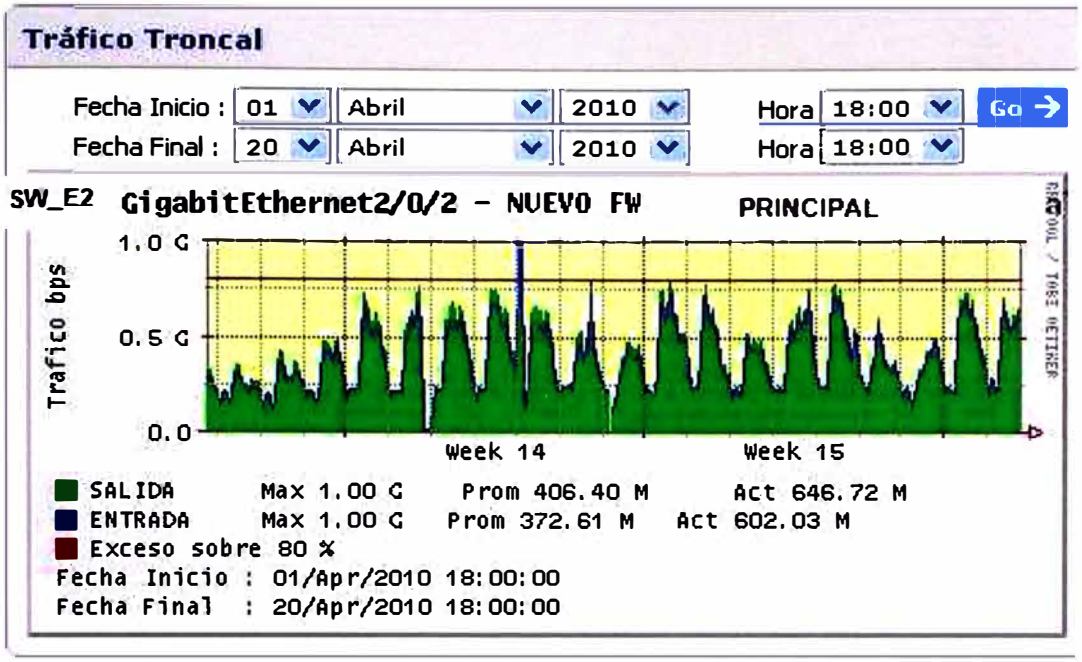

Fig.C.1 Tráfico del Firewall Principal

En la Fig. C.2, el tráfico de la interfaz Gig2/0/2 del SW_E3 se nota con un pico, es decir se produjo un Failover y el trafico conmuto hacia el Firewall Backup.

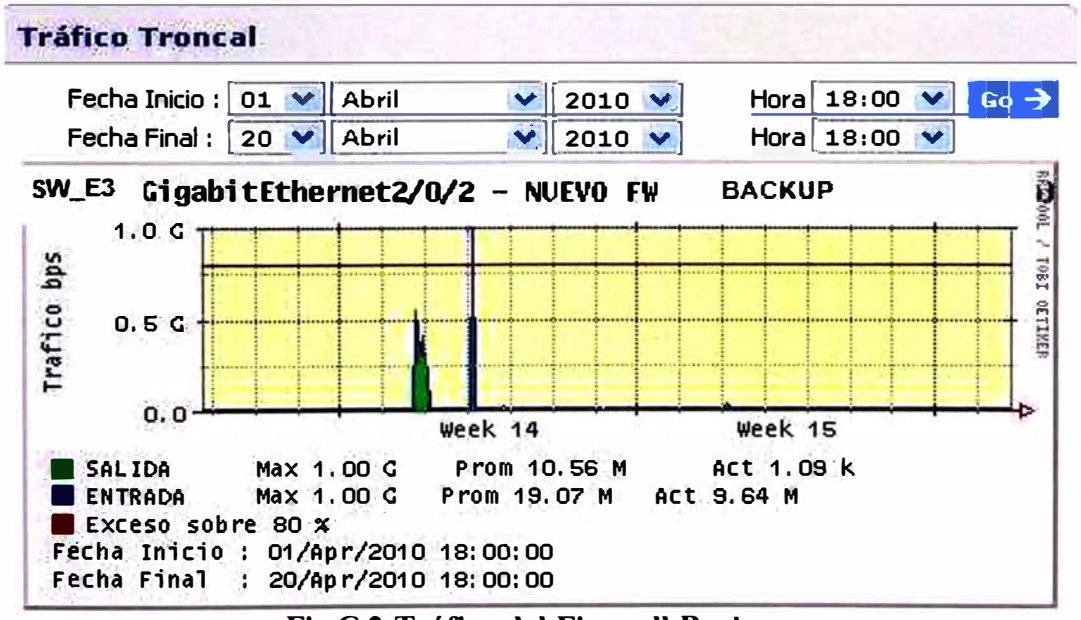

Fig.C.2 Tráfico del Firewall Backup

B) La Fig. C.3 detalla el periodo de tiempo cuando el firewall principal sufrió algún problema de conectividad ya sea software o hardware produciéndose Failover.

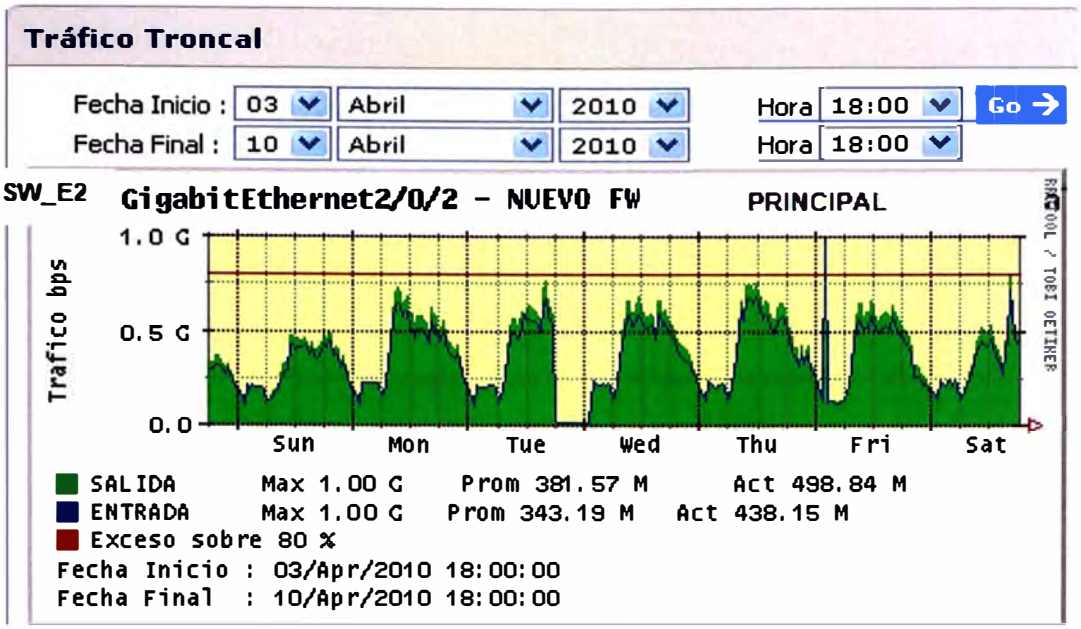

Fig. C.3. Trafico del Firewall Principal

El Firewall Backup responde inmediatamente al sensar que alguna interfaz dejo de funcionar o el firewall perdió conectividad, el tráfico conmuto de inmediato al firewall Backup tal como se muestra en la Fig.C.4.

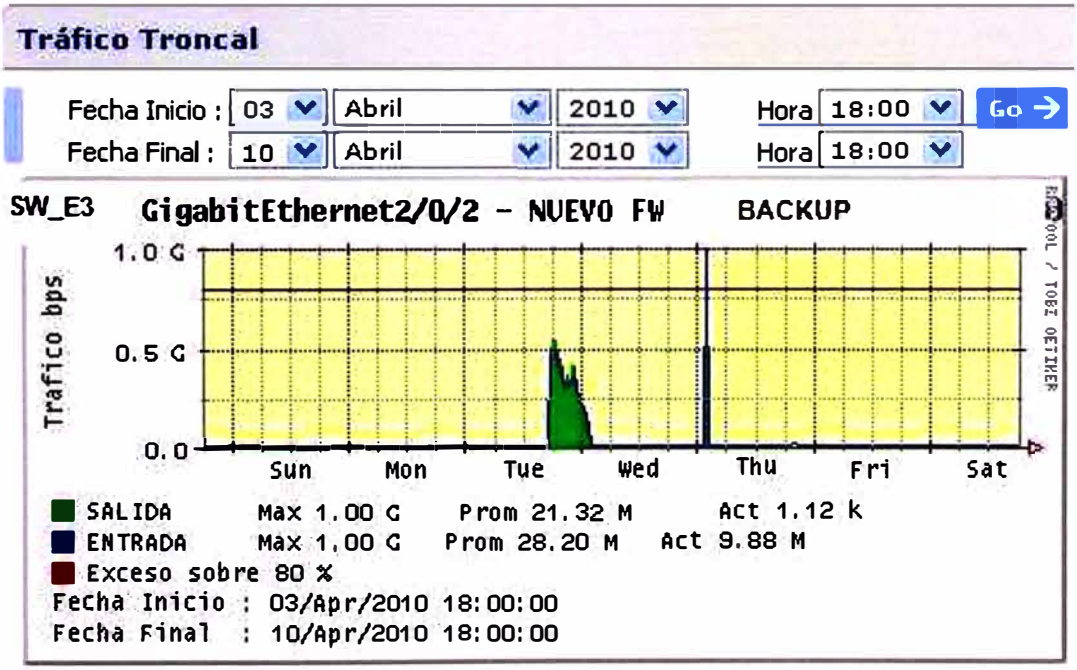

Fig.C.4 Trafico del Firewall Backup

2.- Trafico del IPS.

Las siguientes graficas muestra como el IPS toma acción frente a un tráfico que se le indico que era malicioso, utilizaremos en software de administración llamado IME (IPS Manager Express) para visualizar los tipo de tráfico.

A) La Fig.C.6, muestra el tráfico producido por el software NMAP, el cual es reconocido

por el IPS con el signature ID 3046.

Severity	Date	Time	Device	Sig. Name	Sig. ID	Attacker IP	Victim IP	Actions Taken
medium	10/14/2010	12:22:52	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	
medium	10/14/2010	12:22:54	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	
medium	10/14/2010	12:22:54	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	
medium	10/14/2010	12:22:57	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	
medium	10/14/2010	12:22:57	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	
medium	10/14/2010	12:23:00	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	
medium	10/14/2010	12:23:00	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	
medium	10/14/2010	12:23:02	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	
medium	10/14/2010	12:23:02	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	

Fig.C.6 Tráfico generado por NMAP

La Fig.C.7 detalla la acción que toma el IPS al descubrir el tráfico malicioso o cuando se le indica cómo reaccionar a un tipo de tráfico en particular mostrando el mensaje "DenyPacketRequest".

Severity	Date	Time	Device	Sig. Name	Sig. ID	Attacker IP	Victim IP	Actions Taken	Victim Port
medium	10/14/2010	12:33:02	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	denyPacketReq...	21
medium	10/14/2010	12:33:04	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	denyPacketReq...	21
medium	10/14/2010	12:33:04	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	denyPacketReq...	21
medium	10/14/2010	12:33:04	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	denyPacketReq...	21
medium	10/14/2010	12:33:04	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	denyPacketReq...	21
medium	10/14/2010	12:33:06	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	denyPacketReq...	21
medium	10/14/2010	12:33:06	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	denyPacketReq...	21
medium	10/14/2010	12:33:06	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	denyPacketReq...	21
medium	10/14/2010	12:33:06	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	denyPacketReq...	21
medium	10/14/2010	12:33:10	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	denyPacketReq...	21
medium	10/14/2010	12:33:10	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	denyPacketReq...	21
medium	10/14/2010	12:33:10	IPS-	NMAP OS Fingerprint	3046/0	192.168.0.23	192.168.254.3	denyPacketReq...	21

FigC.7 Trafico analizado por el IPS.

B) Probaremos ahora la firma "***1628: ICMPv6 Traffic over Ipv4***" la cual se dispara cuando el IPS detecta que el campo "protocol" de la cabecera IP tiene el valor 58 (equivalente a ICMPv6). Fabricaremos un paquete dirigido a la IP 172.25.255.10 cuyo campo "protocol" tenga el valor 58, lo cual deberá disparar dicha firma. Para comprobarlo usaremos el siguiente comando:

```
C:\>nmap -PN -sO –p58  172.25.255.10
Nmap scan report for 172.25.255.10
Host is up.
PROTOCOL STATE        SERVICE
58       open|filtered ipv6-icmp
Nmap done: 1 IP address (1 host up) scanned in 2.83 seconds
```

Además desactivaremos la firma "***1101: Unknown IP Protocol***" la cual se dispara cuando el IPS detecta que el campo "protocol" de la cabecera IP tiene un valor entre 134 y 255. Para ello quitamos el check al campo "Enabled"

FigC.8 Signature Deshabilitada.

Luego fabricaremos un paquete dirigido a la IP 172.25.255.10 cuyo campo "protocol" tenga el valor 135. Ya que la firma está desactivada no se deberá disparar ningún evento.

Para comprobarlo usaremos el siguiente comando:

C:\>nmap -PN -sO -p135 172.25.255.10

Nmap scan report for 172.25.255.10
Host is up.
PROTOCOL STATE SERVICE
135 open|filtered unknown
Nmap done: 1 IP address (1 host up) scanned in 2.88 seconds

Verificamos en el Software IME, el signature "ID 1628" es evidenciado por el IPS. Véase Fig.C9

Fig.C9 Signature Mostrado por el IPS.

BIBLIOGRAFIA

[1]. The CISSP Prep Guide: Mastering the ten domains of compute security, Ronal L. Krutz /Russell Dean Vines, 2001.

[2]. SECUNIA, Half Year Report 2010.

[3]. CCNA-Security, Michael Watkins, Cisco System, 2008.

[4]. Web Application Security Statistics 2008: www.webaappsec.org.

[5]. Programa Integral Seguridad de Sistemas de Información – TECSUP.

[6]. Redes Autodefensivas - Cisco Systems Latinoamérica 2006.

[7]. http://en.wikipedia.org/wiki/High_availability

[8]. http://es.scribd.com/doc/36283005/HSRP-Teoria-y-Configuraciones

[9]. Understanding And Troubleshooting HSRP, Document ID 10583.

[10]. http://rfc2281.openrfc.org/

[11]. Guide to Computer Security Log Management, National Institute of standards and Technology (NIST), Karen Kent and Murugiah Souppaya, 2006.

[12]. Cisco Networks 2008 – Troubleshooting Firewall, BRKSEC-3020.

[13]. http://tools.cisco.com/security/center/viewAlert.x?alertId=47#BRKSEC_2009_Deploying_Network_Intrusion_Protection_System

[14]. Snort: http://www.snort.org

[15]. Cisco System : http://www.cisco.com

[16]. Lucent Technology: http://www.lucent.com.

[17]. Web Application Security : www.acunetix.com

[18]. Core Impact Professional: http://www.coresecurity.com/content/features-and-benefits-pro.

[19]. SANS Institute Reading Room: http://rr.sans.org.

[20]. CERT: http://www.cert.org.

[21]. (ISC)2 Security Transcends Technology: https://www.isc2.org/

[22]. ISO 27001 portal: http://www.iso27000.es/.

INDICE