UNIVERSIDAD TECNICA DE COTOPAXI

CARRERA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

PROYECTO DE TESIS PREVIO LA OBTENCION DEL TITULO DE INGENIERO EN INFORMATICA Y SISTEMAS COMPUTACIONALES

TEMA: "Implementación de un Sistema de Prevención de Intrusos (ips) basado en Linux Fedora en la Base Aérea Lago Agrio"

DIRECTOR: **ING. PATRICIO NAVAS MOYA**

POSTULANTES: ROBERTO PAUL MAYO QUEVEDO

ANGEL OSWALDO CAIZALUISA ALBUJA

LATACUNGA – ECUADOR

2009

PAGINA DE RESPONSABILIDAD DE AUTORÍA

Las ideas, opiniones y comentarios en este documento son de exclusiva responsabilidad de los autores, egresados: Paúl Mayo y Ángel Caizaluisa

…… ……..

Roberto Paúl Mayo Quevedo Ángel Oswaldo Caizaluisa Albuja

CERTIFICACIÓN

HONORABLE CONSEJO ACADÉMICO DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.

De mi consideración.

Cumpliendo con lo estipulado en el capitulo IV, (art. 9 literal f), del reglamento del curso profesional de la Universidad Técnica de Cotopaxi, informo que los postulantes: Roberto Paúl Mayo Quevedo y Ángel Oswaldo Caizaluisa Albuja, ha desarrollado su tesis de grado de acuerdo al planteamiento formulado en el plan de tesis con el tema: "**"Implementación de un Sistema de Prevención de Intrusos (ips) basado en Linux Fedora en la Base Aérea Lago Agrio"**", cumpliendo con los objetivos planteados.

En virtud de lo antes expuesto, considero que la presente tesis se encuentra habilitada para presentarse al acto de la defensa de tesis.

Latacunga, 13 de Abril del 2009

Atentamente,

Ing. Patricio Navas Moya

DIRECTOR DE TESIS

AGRADECIMENTO

Infinitamente gracias a Dios,

por darme la vida y permitirme culminar

con una más de mis metas y

a todas aquellas personas quienes con sus muestras de apoyo y esperanza me brindaron cálidas sugerencias que sirvieron para el éxito

de este trabajo de graduación.

Roberto Paúl

AGRADECIMIENTO

Como sujetos sociales llenos de valores, especialmente los morales y que si sabemos practicarlos, quiero hacer llegar mis sentimientos de gratitud a nuestra noble Institución de Educación Superior como es la "UNIVERSIDAD TÉCNICA DE COTOPAXI", institución que nos abrió sus puertas para iniciar la búsqueda de un objetivo que me propuse y que hoy gracias a la dedicación y responsabilidad he culminado con éxito tan ansiada carrera.

Vaya mi agradecimiento cordial y sincero a todas las autoridades, profesores y compañeros, los cuales han sabido transmitir sus conocimientos académicos y valores morales, los cuales he practicado, para enrúmbame por el camino del respeto, responsabilidad y solidaridad.

De manera especial dejo constancia de mi agradecimiento sincero a Dios y a mi familia, quienes son pilares fundamentales de mi vida.

ANGEL OSWALDO

DEDICATORIA

El presente trabajo que es el reflejo de los conocimientos adquiridos en las aulas de nuestra Institución, conjugado con el esfuerzo y sacrificio, lo dedico de corazón a mi esposa, e hijos quienes supieron apoyarme incondicionalmente, durante todos los días de la vida estudiantil hasta alcanzar el objetivo propuesto, la obtención de un título profesional, acorde a los tiempos de la modernización mundial.

Seguro estoy de no defraudarles y responder con ética a un trabajo a mi encomendado. También me comprometo a continuar en el campo de la investigación para alcanzar más logros y así mantener en alto el nombre de nuestra noble Institución.

ANGEL OSWALDO

DEDICATORIA

Dedico este trabajo
a mis Padres, a mi Familia, a mi Familia política y
especialmente a Ceci mi esposa y María Emilia mi hija,
quienes han sido mi aliciente
para luchar y no rendirme jamás
en mi alma. siempre estará
su apoyo y amor incondicional
por ello les entrego mi corazón
y el esfuerzo de mi vida profesional.

Roberto Paúl

ÍNDICE GENERAL

INTRODUCCIÓN

Una computadora es quizás, la herramienta más poderosa que el hombre ha tenido jamás en sus manos y en este momento interviene de forma directa ó indirecta en, prácticamente, todas las actividades humanas. Dejar que esta herramienta sea controlada y restringida por agentes solo interesados en su propio lucro supone un perjuicio para las sociedades, irreparable. El software Libre constituye una oportunidad histórica de tomar el control de nuestro propio destino. Por esta razón es hora ya que empresas, instituciones hagamos conciencia, y busquemos la manera de explotar de mejor manera este recurso.

Es asi que las Fuerzas Armadas y particularmente la Fuerza Aérea Ecuatoriana viene implementando una serie de actualizaciones en su servicio informático ya que solo de está manera va a precautelar toda la información que se genere y que siempre va a ser un riesgo que pueda caer en manos equivocadas, el software libre como política de estado se la debe implementar en toda institución publica y mas aun tratándose de la seguridad nacional.

La implementación de servidores de seguridad se refiere a la capacidad de una red de computadores de garantizar la calidad de servicio. Las tecnologías de calidad de servicio proporcionan los componentes

elementales que se utilizaran para aplicaciones futuras de seguridad en la Base Aérea de la ciudad de Lago Agrio, y las redes de proveedores de Internet (ISP).

El control de las seguridades que tenga la red de computadores de la Base Aérea le permite proporcionar mejor servicio a ciertos flujos, esto se hace midiendo la prioridad de un flujo o limitando la prioridad de otro flujo Cuando se utiliza herramientas de administración para la congestión, mediante el Sistema de prevención de Intrusos un servidor va a precautelar la información que aquie se genere. Las herramientas de Administración de Congestión usados en cola para evitar la congestión levanta la prioridad dejando caer los flujos de más baja prioridad antes de flujos de más alta prioridad.

A través de un diagnostico desarrollado en el Ministerio de Defensa Nacional se ha podido detectar de muchas falencias que tienen las seguridades de los distintos repartos militares y que se agudizo en los últimos sucesos ocurridos precisamente en la frontera norte de nuestro país.

Partiendo de lo expuesto nos hemos planteado como tema de tesis: **“Implementación de un Sistema de Prevención de**

Intrusos (ips) basado en Linux Fedora en la Base Aérea Lago Agrio”

El desarrollo de este servidor en este reparto militar va a posibilitar que la información que se genere a través de las distintas oficinas se encuentren precauteladas y de está forma ayudaríamos a que el pais en general se encuentre tranquilo.

La presente investigación generara información básica de lo que se cuenta en la actualidad en tecnología, que información se genera, de que oficina es la que más información genera, de que y de quien hay que cuidarse ya que un IPS no es un simple firewall que administra el flujo de información externa sino que administra todo, lo generado internamente así como lo generado externamente pero que es de competencia de la Fuerza y particularmente de la Base Aérea Lago Agrio.

Nuestro trabajo ha sido diseñado en tres capítulos:

El primero corresponde al conocimiento de algunos aspectos importantes de lo que son seguridades tanto físicas como lógicas a través de una red de computadores, explicamos que son, como trabajan los IDS(Sistema de

Detección de Intrusos), los IPS(Sistemas de Prevención de Intrusos), las diferencias más notorias y por ultimo obtuvimos las debidas conclusiones.

El segundo capitulo trata de la información de la Fuerza Aérea Ecuatoriana sus objetivos, la misión y visión institucional, una entrevista con el jefe de la Unidad de Tecnologías de la Información y las Comunicaciones y por ultimo la encuesta realizada al personal que labora en la Base Aérea.

El tercer capitulo es la implementación del servidor de IPS el mismo que cumplirá con los objetivos planteados en el proyecto, que sirvió como antesala de la investigación realizada

RESUMEN

La seguridad de la información por siempre ha sido un valor agregado en toda investigación, pero cuando se dispone de muchos usuarios de equipos de cómputo que generan variada información es preocupante observar que en algunos casos no se dispone de una técnica o de un equipo que precautele la información, convirtiéndose la unidad en blanco de potenciales ataques de hackers.

Un IPS basado en el desarrollo en herramientas de Código Abierto (Open Source), ha logrado disminuir costos y optimizar tiempo ya que al existir equipos(Hardware), que realizan está misma actividad hacen que se encarezca las actividades de una institución o empresa por cuanto requiere de capacitación y de conocer cuales son las políticas de la empresa que provee este servicio, por esta razón nos planteamos la implementación de un IPS basado en software y con herramientas que son de libre distribución y que la fuente bibliografíca abunda en el Internet.

La investigación está completa una vez implementada y que los usuarios noten la diferencia de tener un servidor con seguridades y que apoya las actividades de administración del tráfico en la red o de manejo de puertos.

CAPITULO I

1. FUNDAMENTACIÓN TEÓRICA DE LOS SISTEMAS DE PREVENCION DE INTRUSOS

1.1. SERVIDORES DE SEGURIDAD

1.1.1. Definición

Debido a la creciente confianza en computadoras de red poderosas para los negocios y en llevar un seguimiento de nuestra información personal, las industrias se forman considerando de antemano la práctica de seguridad de la computación y redes. Las corporaciones solicitan el conocimiento y habilidades de los expertos para auditar los sistemas y ajustar soluciones para satisfacer los requerimientos operativos de la organización. Puesto que la mayoría de las organizaciones son dinámicas por naturaleza, con trabajadores accesando los recursos informáticos de la organización local y remotamente, la necesidad de ambientes computacionales seguros se ha vuelto cada vez más relevante.

Desafortunadamente, la mayoría de las organizaciones (así como también usuarios individuales) dejan la seguridad como algo para

resolver luego, un proceso que es ignorado en favor de mayor poder, mayor productividad y en las preocupaciones presupuestarias. La implementación adecuada de la seguridad es a menudo realizada *postmortem*. Después que ocurre una intrusión no autorizada. Los expertos de seguridad consideran que el establecimiento de medidas adecuadas antes de conectar un sitio a una red insegura tal como la Internet, es una forma efectiva de frustrar la mayoría de los intentos de intrusión.

La seguridad de computación es un término general que cubre una gran área de computación y procesamiento de la información. Las industrias que dependen de sistemas computarizados y redes para ejecutar sus operaciones y transacciones de negocios diarias, consideran sus datos como una parte importante de sus activos generales. Muchos términos y medidas se han incorporado a nuestro vocabulario diario en los negocios, tales como costo total de propiedad (total cost of ownership, TCO) y calidad de servicios (QoS). Con estas medidas, las industrias calculan aspectos tales como integridad de los datos y alta disponibilidad como parte de los costos de planificación y administración de procesos.

En algunas industrias, como el comercio electrónico, la disponibilidad y confianza de los datos pueden hacer la diferencia entre el éxito y el fracaso.

En Febrero del año 2000, se descargó un ataque de Denegación de Servicios Distribuido (Distributed Denial of Service, DDoS) en varios de los sitios más traficados de la Internet. El ataque dejó a yahoo.com, cnn.com, amazon.com, fbi.gov, y muchos otros sitios completamente fuera del alcance de los usuarios normales. El ataque comprometió a los enrutadores por varias horas con grandes

transmisiones de paquetes ICMP, también llamado una *inundación de pings*. Este ataque fue llevado a cabo por agresores desconocidos usando programas especialmente creados y disponibles ampliamente que se encargan de escanear los servidores de red vulnerables, instalan aplicaciones cliente en los servidores llamadas *troyanos*, y programan un ataque con cada servidor infectado inundando a los sitios víctima y dejándolos indisponibles. Muchos culpan el ataque en fallas fundamentales en la forma en que están estructurados los enrutadores y los protocolos que usan para aceptar todos los datos entrantes, no importa donde o por qué motivos los paquetes sean enviados.

Esto nos trae al nuevo milenio, un momento en el que se estima que 945 millones de personas usan o han usado Internet (Almanaque de la Industria de Computación, 2004). Al mismo tiempo:

- En un día dado, hay aproximadamente 225 incidentes graves de violaciones de seguridad reportados al Centro de Coordinación CERT en la Universidad de Carnegie Mellon1

- En el año 2003, el número de incidentes reportados al CERT saltó a 137.529 de 82.094 en el 2002 y de 52.658 en el 2001.2

- Los impactos económicos a nivel mundial de los tres virus de Internet más peligrosos de los últimos dos años combinan un total de US$13.2 mil millones. 3

La seguridad en computación se ha convertido en un gasto cuantificable y justificable para todos los presupuestos de IT. Las organizaciones que requieren integridad de sus datos y alta disponibilidad, obtienen las habilidades de administradores de sistemas, desarrolladores e ingenieros para asegurar la confiabilidad 24x7 de sus sistemas, servicios e información. Convertirse en víctima de usuarios maliciosos, procesos, o ataques coordinados, es una amenaza directa al éxito de una organización.

Desafortunadamente, la seguridad de sistemas y redes puede ser una proposición difícil, requiriendo conocimiento intrincado de como una organización confía, utiliza, manipula y transmite su información. Entender la forma en que la organización lleva el negocio (y la gente que hace la organización) es primordial para implementar un plan de seguridad adecuado.

1.1.2. Tipo de Servidores de Seguridades

Debido al creciente desarrollo de nuevos y potentes Sistemas Operativos así como de tecnología por parte de las empresas desarrolladoras de software libre como del licenciado, hace que más empresas tiendan a la compra de este software para no quedarse atrás en la tecnología, mientras esto sucede hay gurús informáticos que se dedican a descubrir las vulnerabilidades de los sistemas operativos con diversas intenciones, por lo cual los clasificaremos en tres tipos:

"White Hats" (sombreros blancos, los buenos o hackers) o "Black Hats" ("sombreros negros", los malos o crackers), según

una clasificación de sus acciones (según sean sólo intrusivas o además destructivas). Aunque recientemente también ha aparecido el término "Grey Hat" ("sombrero gris") para referirse a aquellos hackers que ocasionalmente traspasan los límites entre un tipo u otro, o los que realizan acciones que sin ser moralmente reprobables se pueden considerar como ilegales o viceversa.

Estas tres clasificaciones mencionadas anteriormente se convierten en intrusos de la red de datos de varias empresas, ya que acceden de manera no autorizada y por vías ilegales a la información valiosa que en muchos de los casos es la razón de ser de la empresa y esta no se puede ver amenazada o interceptada por intrusos, por lo cual las organizaciones están optando por protegerse robusteciendo la red interna, con herramientas como:

- Firewall
- Cortafuegos
- IDS (Sistema de Detección de Intrusiones)
- IPS (Sistema de Prevención de Intrusiones)

Que logran aplacar este tipo de ataques a la red, que en la actualidad son más comunes al igual que los spam, gusanos, troyanos y virus que son creados por los crackers, para obtener algún beneficio o simplemente por el hecho de realizar una acción destructiva en contra de alguna empresa.

1.2. SERVIDORES DE FIREWALL

1.2.1. Características

La seguridad de la información es pensada a menudo como un proceso y no como un producto. Sin embargo, las implementaciones de seguridad estándar usualmente emplean alguna forma de mecanismo dedicado para controlar los privilegios de acceso y restringir los recursos de la red a los usuarios autorizados, identificables y localizables. Linux Fedora incluye muchas herramientas poderosas para asistir a los administradores y a los ingenieros de seguridad con los problemas de control de acceso al nivel de la red.

Junto a las soluciones de VPN tales como IPsec, los cortafuegos o Firewalls son uno de los componentes principales de la implementación de seguridad. Muchos vendedores de soluciones de cortafuegos dirigidas a todos los niveles del mercado: desde los usuarios del hogar protegiendo un PC hasta las soluciones de Centros de Datos resguardando información vital de la corporación. Los cortafuegos pueden ser soluciones de hardware independiente, tales como aparatos cortafuegos de Cisco, Nokia, y Sonicwall. También existen soluciones de cortafuegos de software propietario desarrolladas para los mercados del hogar y de negocios por vendedores tales como Checkpoint, McAfee y Symantec.

Aparte de las diferencias entre cortafuegos de hardware y software, también existen diferencias en la forma en que los cortafuegos funcionan que los separan unos de los otros.

1.2.2. Funcionalidad

Un firewall es un dispositivo que filtra el tráfico entre redes, como mínimo dos. El firewall puede ser un dispositivo físico o un

software sobre un sistema operativo. En general debemos verlo como una caja con DOS o mas interfaces de red en la que se establecen una reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no. Incluso puede ir más allá y realizar modificaciones sobre las comunicaciones, como el NAT.

Esa sería la definición genérica, hoy en dia un firewall es un hardware especifico con un sistema operativo o una IOS que filtra el tráfico TCP/UDP/ICMP/../IP y decide si un paquete pasa, se modifica, se convierte o se descarta. Para que un firewall entre redes funcione como tal debe tener al menos dos tarjetas de red. Esta sería la tipología clásica de un firewall:

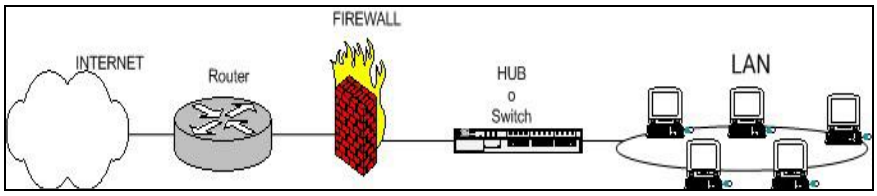


Grafico 1.1: Esquema típico de un Firewall
Fuente: http://www.monografias.com/firewall.htm

Dependiendo de las necesidades de cada red, puede ponerse uno o más firewalls para establecer distintos perímetros de seguridad en torno a un sistema. Es frecuente también que se necesite exponer algún servidor a Internet (como es el caso de un servidor Web, un servidor de correo, etc..), y en esos casos obviamente en principio se debe aceptar cualquier conexión a ellos. Lo que se recomienda en esa situación es situar ese servidor en lugar aparte de la red, el que denominamos DMZ o zona desmilitarizada. El firewall tiene entonces tres entradas:

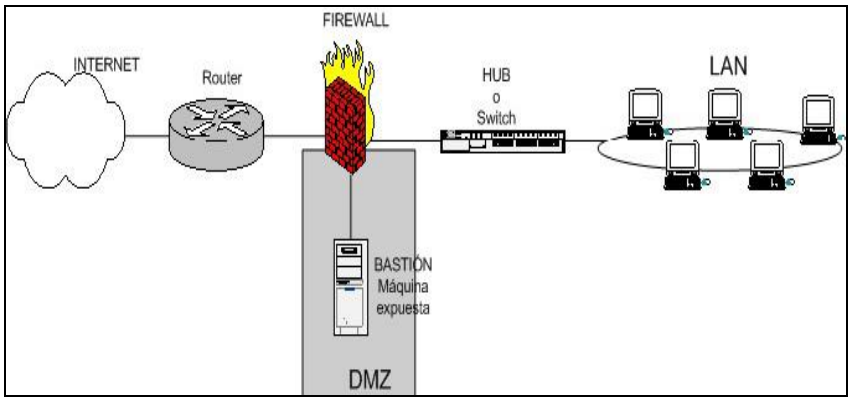


Grafico 1.2: Esquema de un Firewall mediante servidor.
Fuente: http://www.monografias.com/firewall.htm

En la zona desmilitarizada se pueden poner tantos servidores como se necesiten. Con esta arquitectura, permitimos que el servidor sea accesible desde Internet de tal forma que si es atacado y se gana acceso a él, la red local sigue protegida por el firewall. Esta estructura de DMZ puede hacerse también con un doble firewall (aunque como se ve se puede usar un único dispositivo con al menos tres interfaces de red). Sería un esquema como este:

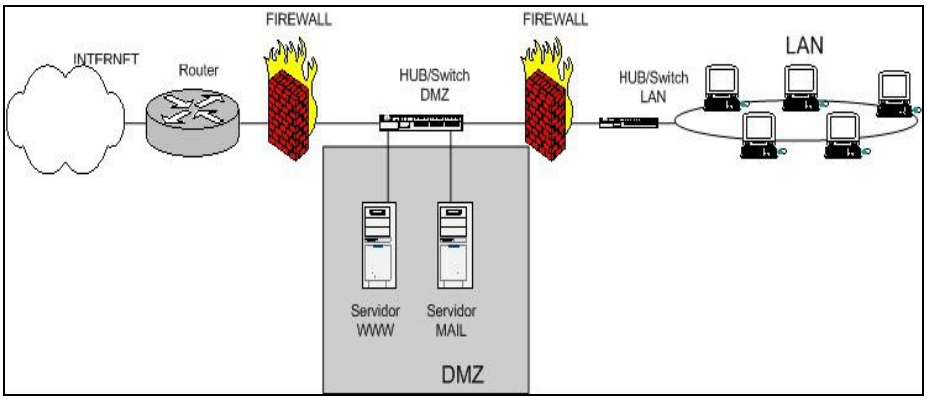


Grafico 1.3: Esquema de un Firewall para administrar DMZ.
Fuente: http://www.monografias.com/firewall.htm

Hay dos maneras de implementar un firewall:

1. Política por defecto ACEPTAR: en principio todo lo que entra y sale por el firewall se acepta y solo se denegará lo que se diga explícitamente.

2. Política por defecto DENEGAR: todo esta denegado, y solo se permitirá pasar por el firewall aquellos que se permita explícitamente.

Como es obvio imaginar, la primera política facilita mucho la gestión del firewall, ya que simplemente nos tenemos que preocupar de proteger aquellos puertos o direcciones que sabemos que nos interesa; el resto no importa tanto y se deja pasar. Por ejemplo, si queremos proteger una máquina linux, podemos hacer un netstat –ln (o netstat –an, o netstat – puta | grep LISTEN), saber que puertos están abiertos, poner reglas para proteger esos puertos y ya está. ¿Para qué vamos a proteger un puerto que realmente nunca se va a abrir?

El único problema que podemos tener es que no controlemos que es lo que esta abierto, o que en un momento dado se instale un software nuevo que abra un puerto determinado, o que no sepamos que determinados paquetes ICMP son peligrosos. Si la política por defecto es ACEPTAR y no se protege explícitamente, nos la estamos jugando un poco.

En cambio, si la política por defecto es DENEGAR, a no ser que lo permitamos explícitamente, el firewall se convierte en un auténtico MURO infranqueable. El problema es que es mucho más difícil preparar un firewall así, y hay que tener muy claro como funciona el sistema (sea

iptables o el que sea) y que es lo que se tiene que abrir sin caer en la tentación de empezar a meter reglas super-permisivas.

Esta configuración de firewall es la recomendada, aunque no es aconsejable usarla si no se domina mínimamente el sistema. Uno de los objetos principales de este documento es mostrar la forma de crear este tipo de firewalls.

1.3. EVALUACION DE VULNERABILIDADES

Con el tiempo suficiente, los recursos y la motivación, un intruso puede violar casi cualquier sistema.

Al final del día, todos los procedimientos de seguridad y la tecnología disponible actualmente no pueden garantizar que sus sistemas estén seguros de un ataque. Los enrutadores lo pueden ayudar a asegurar sus puertas de enlace (gateways) a la Internet. Los cortafuegos (firewalls) le permiten asegurar el borde de su red. Las redes privadas virtuales pueden pasar con seguridad sus datos en un flujo encriptado. Los sistemas de detección de intrusos pueden advertirlo de actividades maliciosas.

Sin embargo, el éxito de cada una de estas tecnologías depende de un número de variables, incluyendo:

- La experiencia del personal responsable de la configuración, supervisión y mantenimiento de las tecnologías.

- La habilidad de remendar y actualizar servicios y kernels rápida y eficientemente.

- La habilidad de aquellos responsables de mantener vigilancia constante sobre la red.

Dado el estado dinámico de los sistemas de datos y tecnologías, asegurar sus recursos corporativos puede ser bien complejo. Debido a esta complejidad, puede ser difícil encontrar recursos expertos para todos sus sistemas. Mientras que es posible tener personal con conocimientos en muchas áreas de seguridad de información a un nivel alto, es difícil mantener personal que sea experto en más de unas pocas áreas particulares. Esto se debe principalmente a que cada área en particular de seguridad de la información requiere constante atención y foco. La seguridad de información no se queda quieta.

1.3.1. Definición de la evaluación y pruebas

Las evaluaciones de vulnerabilidad se pueden dividir en dos grandes categorías: *Desde afuera viendo hacia adentro* y *Desde adentro viendo alrededor*.

Cuando se lleva a cabo una evaluación de vulnerabilidad desde afuera, usted está tratando de comprometer sus sistemas desde afuera. Al posicionarse desde afuera de la compañía puede ver las cosas desde el punto de vista del intruso. Usted ve lo que ve un intruso ve . direcciones IP públicas, sistemas en su *DMZ*, las interfaces externas de su cortafuegos y más. DMZ viene de "zona

desmilitarizada" lo que corresponde a un computador o a una pequeña subred que se coloca entre la red confiable interna, tal como la LAN corporativa, y una red externa no confiable, tal como la Internet.

Típicamente, la DMZ contiene dispositivos accesibles al tráfico de la Internet, tal como servidores Web (HTTP), FTP, SMTP (correo electrónico) y servidores DNS.

Cuando realiza una evaluación de vulnerabilidad desde adentro, de alguna forma usted tiene una ventaja puesto que ya está adentro y su estatus es elevado y de confianza. Este es el punto de vista suyo y de sus compañeros de trabajo una vez que se conectan a los sistemas. Puede ver los servidores de impresión, servidores de archivos, bases de datos y otros recursos.

Hay diferencias importantes entre estos dos tipos de evaluaciones de vulnerabilidad. Siendo interno a su compañía le otorga mayores privilegios. Mucho más que cualquier persona de fuera. Hoy día, en la mayoría de las organizaciones, la seguridad es configurada de forma tal que se mantengan a los intrusos afuera. Se hace muy poco para asegurar la parte interna de la organización (tales como cortafuegos departamentales, controles de acceso a nivel de usuario, procedimientos de autenticación para recursos internos y más). Típicamente, hay muchos más recursos cuando se está adentro y mirando alrededor pues la mayoría de los recursos son internos a la compañía. Una vez que se encuentra fuera de la compañía, inmediatamente se le da condición de no fiable. Los sistemas y recursos que tiene disponibles son típicamente mucho más limitados.

Considere la diferencia entre las evaluaciones de vulnerabilidad y las *pruebas de penetración*. Piense en una evaluación de vulnerabilidad como el primer paso de una prueba de penetración.

La información reunida a partir de la evaluación será usada en las pruebas. Mientras que la evaluación de vulnerabilidad busca huecos y vulnerabilidades potenciales, las pruebas de penetración tratan de explotar los resultados.

El acceso a la infraestructura de red es un proceso dinámico. La seguridad, tanto de información como física, es dinámica. Al realizar una evaluación, se tiene una vista general, la cual puede arrojar falsos positivos y falsos negativos.

Los administradores de seguridad son buenos en la medida que también lo sean las herramientas que usen y el conocimiento que posean. Tome por ejemplo cualquier herramienta de evaluación disponible en el mercado y ejecútela en su sistema. Es casi que garantizado que encontrará al menos algunos falsos positivos. Bien sea por un error del programa o del usuario, el resultado es el mismo. La herramienta puede encontrar vulnerabilidades que en realidad no existen (falsos positivos), o peor aún, la herramienta puede que no encuentre vulnerabilidades que actualmente si existen (falsos negativos).

Ahora que ya están definidas las diferencias entre evaluaciones de vulnerabilidad y pruebas de penetración, es una buena idea reunir las conclusiones de la evaluación y revisarlas cuidadosamente antes de llevar a cabo una prueba de penetración como parte de sus nuevos buenos hábitos.

1.4. SISTEMAS DE DETECCION DE INTRUSOS

1.4.1. IDS Basado en Software

Desafortunadamente los IDS actuales basan su funcionamiento en un esquema estático lo cual los convierte en sistemas muy ineficientes en el momento en el que un atacante codifica los datos de entrada.

La base de datos de las firmas de ataques sufren los mismos inconvenientes que los anti-virus, si la base de datos está desactualizada es muy probable que el sistema sea atacado sin ser detectado.

Adicionalmente el tiempo entre el descubrimiento de un nuevo ataque, la publicación de este y su inclusión en los IDS es bastante largo, teniendo en cuenta que el tiempo entre la publicación de dicho ataque y el uso indebido por parte de un posible atacante es muy corto.

Los *firewalls* de aplicación generalmente funcionan cubriendo la aplicación a proteger, lo cual los hace dependientes de 2 la aplicación y del sistema o arquitectura sobre el cual la aplicación a proteger se encuentra. Esto es una gran limitación en su implementación y puede generar nuevos problemas de seguridad ya que aumenta el nivel de complejidad de la aplicación a proteger, aumentando así la posibilidad de que se generen nuevos problemas de seguridad.

Viendo las limitaciones de los IDS actuales, algunos centros de investigación en el mundo empezaron a analizar el comportamiento para determinar la existencia de anomalías para la identificación de ataques. Los inicios del análisis de comportamientos se enfocaron principalmente en el desarrollo de mecanismos estadísticos para determinar anomalías en el comportamiento de los usuarios de un sistema determinado. La gran ventaja que presenta un mecanismo estadístico es que este es fácilmente adaptable a las nuevas condiciones cambiantes en el tiempo. Pero esa adaptabilidad es susceptible a cambios progresivos programados, lo cual permite la inclusión de actividades intrusitas evitando su detección.

Existen dos tipos de análisis de comportamientos, el análisis de comportamiento para la detección de anomalías (*anomaly detection*) y de uso erróneo (*misuse detection*). La detección de anomalías puede ser definida como el intento de detectar intrusiones descubriendo desviaciones significantes del comportamiento normal mientras que la detección de uso erróneo o indebido corresponde al enfoque actual donde se utilizan firmas de ataques previamente introducidas al sistema detector, las cuales son comparadas con actividades en el sistema para detectar un ataque.

IDS para protocolo http

Los IDS a nivel de red (NIDS) tienen su gran limitación en el nivel de captura de datos y en la tecnología utilizada para la obtención de estos datos a este nivel. Entre sus limitaciones se encuentra el no poder capturar y analizar todo el tráfico que debe ser observado. Esta limitación proviene de los mismos analizadores de tráfico

(*sniffers*), los cuales son los sensores del sistema. El sistema tiene que manejar problemas de red como la fragmentación de datos, lo cual implica utilizar poder de procesamiento en la manipulación de datos, bajando el rendimiento del sistema y la probabilidad que detecte un ataque. Además, debido a que se están tomando los datos directamente del nivel de red, el factor tiempo, se convierte en una técnica anti-ids ya que se pueden realizar ataques separados por franjas de tiempo superiores a las que puede manejar el NIDS. El panorama es mas sombrío si los datos a ese nivel están codificados con una técnica anti-ids o simplemente encriptados (HTTPS) en este caso el NIDS es totalmente inservible.

Adicionalmente el sensor debe estar estratégicamente posicionado y obtener la totalidad del tráfico a analizar, cosa que en una red con *switches* puede ser complicado. Teniendo en cuenta las limitaciones mencionadas, el primer problema consiste en definir una arquitectura que elimine las limitaciones actuales y ofrezca ventajas adicionales. Así la arquitectura elaborada se basa en un *proxy* inverso (*reverseproxy*), lo cual elimina los problemas directamente relacionados con el nivel de red para captura de datos, permite obtener la totalidad de los datos dirigidos hacia los servidores web, discriminando automáticamente los otros protocolos y si estos datos están encriptados en este punto pueden ser desencriptados y analizados antes de ser redirigidos hacia los servidores web protegidos en la zona desmilitarizada (DMZ) o zona de servicios públicos. Debido a que la manipulación de los datos se realiza a nivel de aplicación no existe una fragmentación de estos y por lo tanto pueden ser procesados, analizados correctamente y tomar decisiones que convierten al sistema en un sistema de prevención de intrusos. Adicionalmente, al separar el nivel de análisis y detección en un *proxy* inverso, se elimina el

riesgo inherente de la complejidad adicional generada por un *firewall* de aplicación y eliminamos la dependencia o problemas de compatibilidad del IDS con respecto a los servidores web protegidos y las arquitecturas de sus sistemas.

Básicamente el sistema IDS se convierte en un sistema genérico para la protección de cualquier tipo de servidor/aplicación web.

El uso de un *proxy* inverso como mecanismo de seguridad no es nuevo. Algunos justifican su uso por convertirse en un único punto de entrada hacia servidores web y principalmente por que esconde el direccionamiento IP interno. Lo cual es totalmente falso, ya que el esconder el direccionamiento interno, como lo hace un NAT, solo es funcional y efectivo a nivel de seguridad cuando cualquier requerimiento proveniente de una red insegura (Internet), no puede alcanzar a los *hosts* protegidos identificados con IPs inválidos. En un *proxy* inverso los requerimientos provenientes de Internet siempre alcanzan los servidores web protegidos aunque tengan IPs inválidas.

El manejo de un *proxy* inverso como único punto de entrada es eficiente solo si se hace algún tipo de análisis o tratamiento a nivel de seguridad sobre los requerimientos, lo cual hasta el momento solo sigue el mismo enfoque estático e ineficiente de firmas, para la posible detección de intrusos.

Los enfoques investigativos sobre el desarrollo de IDS, deben ser reestructurados para que sean efectivos y puedan salir del ámbito académico al mundo real. Dicha reestructuración, permite el desarrollo de IDS que eliminan las limitaciones de los sistemas actuales y con un bajo costo, cumplir con los niveles de seguridad

requeridos, ya que los IDS actuales, incluyendo los *firewalls* de aplicación, siguen congelados en arquitectura, diseño y funcionamiento.

La gran mayoría de las limitaciones en los IDS actuales provienen de la arquitectura en el nivel OSI en que trabajan, así a mayor nivel, menores serán las limitaciones dependientes de la arquitectura. Adicionalmente, el desarrollo de una clasificación viable, clara y sencilla para problemas de seguridad basada netamente en su causa, facilita la implementación de tecnologías como las redes neuronales artificiales, obteniendo así todos sus beneficios adicionales como lo es la identificación de ataques no conocidos. La detección de ataques conocidos y no conocidos en el protocolo HTTP debe estar basado en el desacoplamiento de la vulnerabilidad con el recurso que la posee, lo cual esta íntimamente ligado con la forma como se presentan los datos hacia el mecanismo de análisis y detección, principalmente en el uso de redes neuronales. Esto en conjunto a un buen balanceo de seguridad por niveles, la eliminación del nivel de red como fuente de datos para la detección de ataques y el manejar niveles superiores para la obtención de estos, traen ventajas adicionales que en conjunto con otros mecanismos de protección, ofrecen niveles de seguridad superiores a los actuales.

1.4.2. IDS Basado en Hardware

En grandes organizaciones (multinacionales) o universidades (dónde hay diferentes facultades, departamentos, laboratorios...) un único sistema IDS no proporciona la flexibilidad necesaria para la heterogeneidad de los elementos de que disponemos.

Los sistemas **DIDS** (*Distributed Intrusion Detection System*) proporcionan este servicio de detección de intrusos para grandes redes.

El análisis de los DIDS es tan o mas complejo que el realizado con los NIDS, con lo que queda fuera de este trabajo aunque se cita la bibliografía correspondiente.

Su característica diferenciadora respecto a los sistemas NIDS tradiciones, es la presencia de dos elementos nuevos en su arquitectura

- **Central Analysis Server**: Es el centro del sistema DIDS y es el encargado de recibir toda la información procedente de los agentes y realizar un repositorio común de conocimiento. También realiza las funciones de control y sincronización de los diferentes nodos que forman parte del sistema.

- **Co-operative Agent network**: Es un sistema autónomo encargado de la monitorización de una red. Detecta posibles incidentes e informa al servidor central para que comunique a todos los nodos el ataque detectado así como las contra-medidas a realizar. Dependiendo de la implementación, el agente puede llegar a tomar contra-medidas de forma autónoma (auque siempre informando y supeditándose al servidor central).

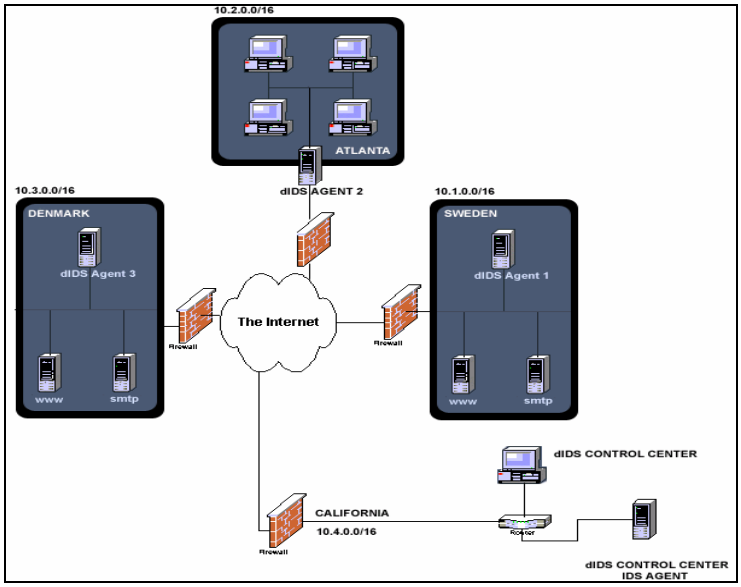


Grafico 1.1: representación Grafica IDS basado en Hardware
Fuente: www.monografias.com/ids.htm

Características de IDS

Un IDS, debe poseer las siguientes características:

- Escalable
- Ligero
- Confiable
- Robusto
- Distinguir lo que es un ataque de lo que es compartir un recurso del sistema.

Algunos IDS

IDS Comerciales

- DRAGON

- Intruder Alert
- NetProwler
- ISS RealSecure
- Cisco NetRanger
- Cyber Cop
- OMNIGUARD Intruder Alert
- POLYCENTER Security Intrusion Detector
- G-Server
- Watch Dog
- CMDS (Computer Misuse and Detection System)
- INTOUCH NSA (Network Security Agent)

IDS Gratuitos

- Shadow
- Network Flight Recorder
- Tripwire
- Snort

Snort

SNORT es una fuente abierta de prevención y detección de intrusos de red y sistema, utiliza una norma impulsada por el idioma, que combina los beneficios de la firma, protocolo y anomalía basada en métodos de inspección. Con millones de descargas hasta la fecha, Snort es la herramienta de detección y prevención de intrusiones, se ha convertido en el estándar de facto para la industria.

Características:

- Más de 700 firmas.
- Ligero.

- Distribución Gratuita.
- Análisis de tráfico en Tiempo Real.
- Uso de Filtros
- Detección de Strings o Host Arbitrarios.

Sourcefire Network Sensor

Sourcefire NS ofrece la detección de amenazas más completa del mercado. Mediante la implantación de un método de detección basado en reglas, el sensor detecta tanto ataques conocidos como comportamientos anómalos. Las reglas se utilizan para examinar los campos de protocolo y se pueden configurar para casos específicos de ataques contra un protocolo o para estudiar las condiciones de un ataque.

1.5. SISTEMAS DE PREVENCION DE INTRUSOS

Este sistema fue desarrollado en 1990, fue diseñado para monitorear el trafico de una red, en tiempo real y prevenir que se filtre cualquier actividad maliciosa conocida como intrusión en la misma, cuando se produce la caída de un paquete o este pasa dañado o incompleto, en una transmisión de información, inmediatamente la red bloquea la transmisión por prevenir un posible ataque o deformaciones en la transferencia de datos, es considerado una mejora con respeto a los Firewalls, y Cortafuegos, su diseño es una evolución de los IDS (Sistema de Detección de Intrusos).

A diferencia de los IDS esta nueva tecnología no se limita solo a escuchar el trafico de la red y a mandar alertas en una consola, después de que ocurre una intrusión, el IPS funciona a nivel de la capa 7 tiene la capacidad de descifrar protocolos como HTTP, FTP y SMTP, algunos IPS permiten establecer reglas como se lo hace en los Firewalls. La tecnología IPS ofrece una visión más profunda de las operaciones de la red proporcionando información sobre actividades maliciosas, malas conexiones, el contenido inapropiado de la red y muchas otras funciones de la capa de Aplicación, utiliza menos recursos que un IDS, siendo una solución ideal que contribuye a la seguridad de la información que se transmite por una red y disminución de costos, para una empresa que opta por adquirir sistemas de este tipo para preservar los datos que posee.

El IPS no utiliza dirección IP como lo hace un firewall, ni funciona igual que un cortafuegos, el IPS permite poner normas y restringir acceso a usuarios, aplicaciones y a host siempre y cuando se detectan que estos están teniendo actividades mal intencionadas o código malicioso en el tráfico de la red.

Ventajas

- Protección preventiva antes de que ocurra el ataque.
- Defensa completa (Vulnerabilidades del Sistema Operativo, Puertos,Trafico de IP, códigos maliciosos e intrusos).
- Maximiza la seguridad y aumenta la eficiencia en la prevención de intrusiones o ataques a la red de una empresa.
- Fácil instalación, configuración y administración
- Es escalable y permite la actualización de dispositivos a medida que crece la empresa

- No requiere tanta dedicación como un IDS tradicional; esto en consecuencia requeriría menos inversión en recursos para administrar y operar estos sistemas (en comparación con un IDS).

CARACTERISTICAS

- Capacidad de reacción automática ante incidentes
- Aplicación de nuevos filtros conforme detecta ataques en progreso.
- Mínima vigilancia
- Disminución de falsas alarmas de ataques a la red
- Bloqueo automático frente a ataques efectuados en tiempo real
- Protección de sistemas no parchados
- Optimización en el rendimiento del tráfico de la red

1.5.1. IPS Basado en Software

Esta aplicación de prevención de intrusiones reside en la dirección IP específica de un solo equipo, permite prevenir posibles ataques en los nodos débiles de una red es decir los host.

Symantec Sygate™ Enterprise Protection

Protege los puntos finales con un sistema de prevención de intrusos basado en host contra ataques conocidos y desconocidos con firewall de escritorio, prevención de intrusos basada en host y tecnologías de protección de gran adaptación.

Cumple con las normativas con Symantec™ Network Access Control (NAC), que incorpora un amplio soporte para integración

de la infraestructura de red. Gestione la solución integrada con la administración de políticas distribuidas de Symantec, que ofrecen distribución de políticas en tiempo-real.

Host de McAfee v6.0

Permite protección integral contra exploits mediante capacidades dinámicas de actualización de protección contra vulnerabilidades y la integración de la funcionalidad completa de Desktop Firewall en un solo agente de prevención de intrusos en host.
Además, los clientes de McAfee ahora pueden consolidar su administración de seguridad de sistemas al controlar el IPS para Host de McAfee con McAfee ePolicy Orchestrator® (ePO™).

El IPS para Host de McAfee protege las aplicaciones y los datos del uso no autorizado y mejora la disponibilidad, confidencialidad e integridad de los procesos comerciales críticos de una empresa. El IPS para Host de McAfee está totalmente integrado con McAfee ePO, lo que permite que todos los productos de seguridad de sistemas de antivirus, antispyware, antispam, prevención de intrusos en host y control de acceso a redes de McAfee se administren mediante una sola consola para obtener una protección de sistemas precisa, escalable y fácil de usar.

1.5.2. IPS Basado en Hardware

Esta aplicación IPS es en hardware y cualquier acción tomada para prevenir una intrusión en una red específica de host (s) se hace de una máquina con otra dirección IP en la red (Esto podría ser en un front-end de cortafuegos).

Son desarrollados específicamente para la plataformas hardware / software que analizan, detectan e informan sobre eventos relacionados con la seguridad. PIN están diseñados para inspeccionar el tráfico y la configuración de la política de seguridad, sobre la cual pueden verificar el tráfico malicioso.

Contenido de la Base IPS (CBIPS)

Inspecciona el contenido de la Base de Datos que se va almacenado en un IPS en base a patrones de comportamiento o firmas, para detectar y prevenir varios tipos de ataque conocidos como gusanos, virus y troyanos, aunque no son muy efectivos puesto que existe decenas o incluso cientos de exploit variantes

Protocolo de Análisis: Pueden decodificar la aplicación nativa de la capa de red protocolos, como HTTP o FTP, el motor de análisis del IPS puede evaluar diferentes partes del protocolo y analizar si este tiene un comportamiento anómalo. Por ejemplo, la existencia de un gran archivo binario en el campo Usuario-Agente de una solicitud HTTP sería muy inusual y probablemente una intrusión. Un analizador de protocolos puede detectar este comportamiento anómalo y alertar al motor IPS de la caída de los paquetes.

IPS basado en tarifa (RBIPS): Están principalmente destinadas a impedir los Negación de Servicio Distribuido. Funciona con la vigilancia normal de la red y el aprendizaje de conductas de patrones de comportamiento. A través del tráfico en tiempo real, el seguimiento y la comparación con las estadísticas almacenadas, RBIPS puede identificar tasas anormales para ciertos tipos de tráfico, por ejemplo TCP, UDP o paquetes ARP, las conexiones por segundo, conexión por paquetes, los paquetes específicos a los puertos etc, estos ataques se detectan basándose en estadísticas de tráfico almacenados.

Plataformas en Software de IPS basados en red

Tipping Point

Esta solución se diseño por 3com y es un IPS basado en red, permite bloquear los ataques phishing, que ocurren cuando una persona se hace pasar por una organización con la intención de obtener información privada de otra empresa, esta herramienta posee además: protección de vulnerabilidades, protección de coincidencia de patrones, y protección basada en comportamientos.

StoneGate IPS-2000

Utiliza técnicas múltiples y precisas de análisis del tráfico de red para proteger a las aplicaciones vulnerables y los sistemas operativos en intranets y en zonas "desmilitarizadas" (DMZs) frente a amenazas en red. StoneGate IPS también incluye protección frente al abuso, incluyendo ataques DoS y uso no autorizado de aplicaciones, tales como comunicación P2P y protocolos de streaming.

Plataformas en Hardware de IPS basados en red

DFL-300

Proporciona una solución económica para el suministro de pequeñas oficinas con cortafuegos fiable protección contra los ataques de piratas informáticos maliciosos en Internet. El DFL300 proporciona una interfaz basada en web

CAPITULO II

TRABAJO DE CAMPO

2. ANALISIS E INTERPRETACION DE RESULTADOS

2.1. Reseña de la Fuerza Aérea Ecuatoriana

Antecedentes de la FAE

El 27 de Octubre de 1920, el recientemente electo Presidente de la República Dr. José Luís Tamayo, consigue que el Congreso Nacional emita el decreto para la formación de dos escuelas de aviación, en Quito y Guayaquil. Esta fecha es cuando se crea la Aviación y es considerada como el día clásico de la Fuerza Aérea Ecuatoriana.

El 4 de Noviembre de 1920 el aviador Elia Liut, al mando del "Telégrafo I", se eleva por primera vez sobre los Andes ecuatorianos, en el vuelo realizado entre Guayaquil y Cuenca.

4 de diciembre de 1962 inicia las operaciones la Cia. de Transportes TAME, la cuál es una empresa de la Fuerza Aérea Ecuatoriana.

El 10 de febrero de 1995 se produce el primer combate aéreo en América durante el conflicto del Cenepa, logrando el derribo de 3 aviones: 2 Sukoy y un A-37B, alcanzando la superioridad aérea local, neutralizando las amenazas enemigas y con ello garantizando la supervivencia de la nación ecuatoriana. El 10 de febrero es el día de la aviación de combate.

MISION

La misión constitucional de las Fuerzas Armadas, y por ende de la Fuerza Aérea, es la defensa de la soberanía e integridad territorial y la de garantizar la paz y estabilidad ciudadanas, entonces se comprende que la Fuerza Aérea debe ser parte de la lucha de la nación contra factores que provoquen inestabilidad y pueden convertirse en amenazas contra la supervivencia del Estado.

VISION

Ser una institución moderna, profesional y competitiva, respetada y aceptada por la sociedad, líder en la defensa del estado ecuatoriano y en el desarrollo aeroespacial, fundamentada en los principios, valores y con recursos humanos altamente motivados y orgullosos de la institución.

ENTIDADES ADSCRITAS

DIAF

La DIAF recibe certificación ISO 9001-2000

La Dirección de la Industria Aeronáutica de la FAE comprometida con el mejoramiento continuo, se encuentra inmersa en la implementación y certificación de calidad en todos sus componentes, es por eso que a finales de agosto del 2006 se realizó la entrega de la Certificación de Calidad ISO 9001-2000 del Centro de Mantenimiento Aeronáutico (CEMA) ubicado en la ciudad de Latacunga, certificación otorgada por la CAB (American Certification Body) y por QSZ (Quality Service Zurich), mediante el asesoramiento de la Empresa Q3 BUREAU.

SAB

El SAB Servicio a Bordo es una empresa adscrita a la FAE, líder en catering aéreo a nivel nacional. Este liderazgo por más de tres décadas, se debe gracias a un ingrediente principal, la calidad en todas las etapas de producción. Los productos elaborados por el SAB, constituyen básicamente: snaks, almuerzos, cenas y desayunos, todos debidamente empacados y elaborados de acuerdo a la normativa internacional, para lo cual se cuenta con personal capacitado.

El SAB cuenta con la certificación internacional de calidad ISO 9001, 2000, esto sumado a su personal altamente calificado, ambiente aséptico, tecnología de punta, precios sin competencia y un exquisito gusto por la buena comida, hacen del SAB su mejor alternativa de Catering y servicio de bufetes, para toda ocasión.

EMSA

La Empresa de Servicios Aeroportuarios es una en entidad adscrita a la Fuerza Aérea Ecuatoriana, especializada en diversos servicios aeroportuarios como el uso de escalinatas especiales para que los

pasajeros ingresen de forma cómoda y segura a las diversas aeronaves comerciales.

AEROSTAR

La Fuerza Aérea Ecuatoriana en enero del 2001 inicia las operaciones de empresa adscrita Aerostar, como una alternativa en la oferta de servicios aéreos de: aerocombustibles y gases criogénicos.

El área de aerocombustibles se dedica la comercialización de combustibles de aviación, tanto para aerolíneas comerciales privadas, internacionales y militares. Y el área de gases criogénicos se encarga de la producción, comercialización y distribución de oxígeno y nitrógeno, con el 99.8% de pureza, lo que garantiza su efectividad.

Para Aerostar no existe nada más importante que el cliente, por ello fue implantado el Sistema de Gestión de Calidad ISO 9001:2000. Además, cuenta con una planta completamente nueva, cuya capacidad de producción es de 6 toneladas por día. Conjuntamente, opera con un parque de cilindros y un banco para realizar pruebas hidrostáticas. Aerostar cumple con los cuatro requisitos exigidos para un producto de niveles internacionales: calidad, tiempo, precio y seguridad. Atención personalizada, entrega de productos oportuna, el mejor precio del mercado y cero accidentes

PRINCIPALES PRODUCTOS Y/O SERVICIOS

ALAS PARA EL DESARROLLO:

La Fuerza Aérea Ecuatoriana estableció este programa dando prioridad en su accionar principalmente a la región oriental. Se atiende a las comunidades indígenas desde pequeñas pistas abiertas en la selva. Para ellos el vuelo de la Fuerza Aérea constituye el único medio de enlace con el resto del país, en poblaciones como: Amazonas, Taisha, Montalvo, Tena, Coca, Macará, Lago Agrio entre otras; en promedio se transportan anualmente a la región oriental cerca de 10.000 colonos y más 250.000 libras de carga.

De igual manera en la región insular la presencia de la Fuerza Aérea crea una época de desarrollo social, al realizar vuelos logísticos cada 15 días, a las islas de Baltra, Isabela y San Cristóbal, transportando principalmente colonos, alimentos y vituallas. Anualmente se benefician aproximadamente 6.000 colonos y se despacha más de 600.000 libras de carga.

ALAS PARA LA SALUD:

La Fuerza Aérea a inicios de 1967 en el ya legendario avión C-47 trasportó la primera tripulación médica dentro de un programa denominado: Alas para la Salud, programa solidario que busca contribuir con el mejoramiento de la difícil situación salubre que viven cientos de comunidades en todo el territorio nacional, es por ello que durante cerca de cuatro décadas, la FAE ha trabajado tesoneramente en beneficio de los más necesitados, suscribiendo diversos convenios de cooperación interinstitucional para apoyar las labores humanitarias que cumple esta entidad, logrando recuperar la felicidad de miles de familias ecuatorianas, quienes asistidas con brigadas médicas gratuitas, llevando médicos

calificados, medicinas, vacunas y demás insumos. Anualmente más de 10.000 familias a nivel nacional se benefician de este programa.

ALAS PARA LA ALEGRIA:

La ilusión de todo pequeño es asemejarse a sus héroes, miles de niños ecuatorianos sueñan con ser pilotos y navegar por los cielos en poderosas naves. La Fuerza Aérea está también comprometida con la alegría y contribuye a que este sueño se haga realidad con el programa Alas para la Alegría, organizando vuelos gratuitos para los futuros héroes de los cielos; este programa está dirigido a la población infantil de escasos recursos económicos llevándolos a volar sobre las principales ciudades del Ecuador. Cada año se benefician aproximadamente unos 5.000 niños de todos los rincones de la patria al hacer realidad su sueño de volar.

ALAS PARA LA EDUCACION

Estamos convencidos de que la única salida para enfrentar el subdesarrollo es la educación, con esta premisa nace ALAS para la educación. La Fuerza Aérea Ecuatoriana realizando un gran esfuerzo, lleva materiales educativos como libros, cuadernos y demás útiles escolares ayudando de esta manera a sobrellevar la difícil condición económica por las que atraviesan cientos de familias ecuatorianas. Además nuestros guerreros empuñan los libros y enseñan las primeras letras a los niños más necesitados de nuestro país.

PRINCIPALES MERCADOS Y/O CLIENTES

USUARIOS DE MANTENIMIENTO Y ABASTECIMIENTOS:

Ala 11 Quito
Ala 12 Latacunga
Ala 21 Taura
Ala 22 Guayaquil
Ala 23 Manta
Ala 24 Salinas
Subdirección de Abastecimientos Quito (Aduanas, Central Pedidos, Administradores de Programa, Órdenes Técnicas, Jefes de Material Aeronáutico, Subdirectores, Directores)
Oficina Logística Olfamia - Miami

Ventas Anuales / tamaño de la Empresa.

Ventas Anuales: Información confidencial

La institución esta formado por:
Oficiales: 789
Aerotécnicos: 5189
Cadetes, Alumnos y Conscriptos: 1202
Empleados Civiles: 1478
TOTAL: 8658.
Presupuesto Anual: Información Confidencial.

DESCRIPCION DEL PROCESO

Descripción del proceso en la Actualidad

El control del inventario del material de aviación tales como: partes y repuestos, combustibles y lubricantes, equipo y vestuario, material bélico y suministros, en los diferentes repartos de la Fuerza Aérea, se maneja en la actualidad mediante diversos sistemas informáticos, hojas de cálculo, tarjetas de transacción, tarjetas de conteo, etc.

Anteriormente, el control del inventario de partes y repuestos en los escuadrones de abastecimientos JAGUAR MIRAGE y KFIR en la Base Aérea de Taura, se lo llevaba en el sistema informático WANG, el cual, por su discontinuidad tecnológica colapsó, haciéndose imposible la recuperación de esta información y obligando a volver al uso de tarjetas kárdex en unos casos y en otros al uso de diversas aplicaciones informáticas, en forma aislada.

Todo esto ha conllevado a que en la Subdirección de Abastecimientos no se disponga de información real en cuanto a existencias en cada bodega de los escuadrones, los pedidos generados en cada reparto no están estandarizados y su situación del estado no se la conoce obligando a los Administradores de cada avión realizar insistencias a través de radiogramas a la Comandancia General de la FAE. Por tal razón al no existir la información consistente e integrada el mando no puede planificar adquisiciones de compra o mantenimiento.

Relevancia para la cadena de valor de la Institución.

La logística, desde el punto de vista gerencial es una estrategia necesaria para manejar de forma integral la cadena de las líneas de artículos, de tal forma que logre el balance óptimo entre las necesidades de los usuarios y los recursos disponibles de la empresa y su desempeño debe ser medido a través del servicio de los usuarios de mantenimiento de aeronaves.

Relación con las dimensiones estratégicas y operativas de la empresa.

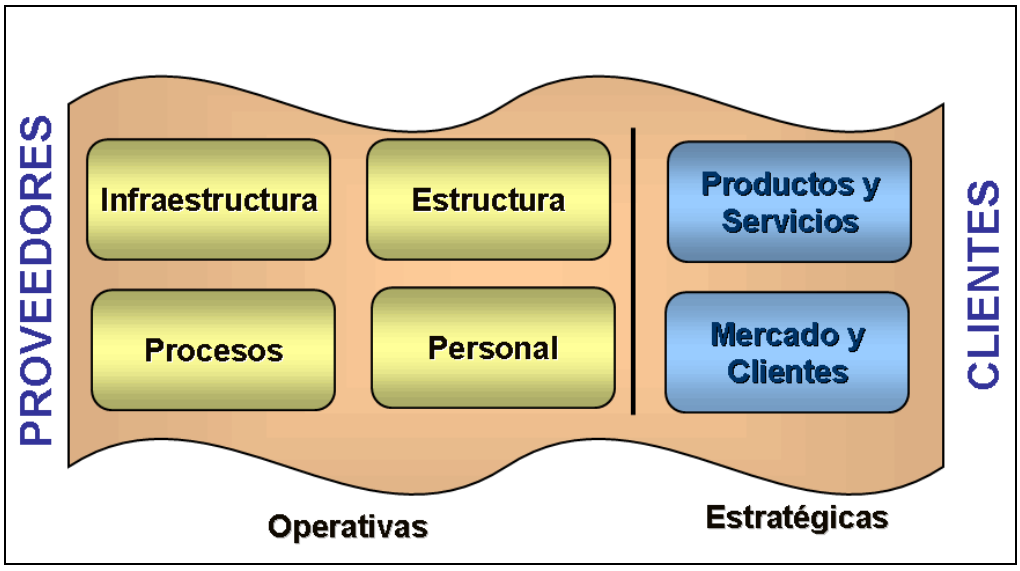


Gráfico 2.1: Organización de la FAE
Fuente: Fuerza Aérea Ecuatoriana

2.2. Entrevista al Señor Jefe de Tecnologías de la información y las Telecomunicaciones de la Base Aérea Lago Agrio

En la actualidad la Base Aérea Lago Agrio se encuentra en franco proceso de automatización de todas sus áreas y principalmente la Unidad de Sistemas de información y las Telecomunicaciones, es así que con lo sucedido el año anterior en Angostura el Señor Presidente Constitucional de la Republica se ha visto en la necesidad de que urgentemente se actualicen los equipos que tenia la Fuerza Aérea, y se adquirieron nuevos radares que tienen trabajo directo con el aérea informática, esto ha hecho que nosotros como miembros de la fuerza tengamos que actualizarnos a la par.

En vista de lo manifestado en días anteriores se planteo la realización de un proyecto de investigación el mismo que va a beneficiar a la Fuerza y por este intermedio a nosotros como estudiantes de la Universidad Técnica de Cotopaxi ya que de está manera vamos a obtener el titulo de Ingenieros en Informática y Sistemas Computacionales.

Buenos Días Señor Sargento Segundo Ingeniero Carlos Pérez, encargado de la Unidad de Tecnologías de la Información y las Comunicaciones, podría por favor comentarnos como es llevado las seguridades en está importante unidad y que opina de la implementación de un servidor de seguridades mediante IPS utilizando Software Libre como lo es el Sistema Operativo Linux.

En la actualidad la Fuerza Aérea cuenta con una intranet la misma que sirve para la comunicación mediante correo o Chat, para está actividad se dispone de un servidor con Lotus Notes, este servidor principal o Domino Server de ;Aotus se encuentra en Quito en las oficinas del Ministerio de

Defensa Nacional, aquí en la Base Aérea Lago Agrio disponemos de un servidor local para transferir los correos a los usuarios del Lotus.

Además de este servidor se cuenta con un servidor de Dominio en Windows 2003 el mismo que administra grupos de trabajo y usuarios de acuerdo a los perfiles y a la utilización de la red así como el desempeño que tenga cada punto o puerto, en este se encuentra de igual manera el servidor de Internet denominado también como Proxy. No tenemos seguridades aquí en la Base ya que todo el ingreso del exterior hacia las fuerzas armadas es decir lo de Internet se encuentra centralizado en Quito y ellos son quienes depuran y de igual manera administran el ancho de banda para el acceso de nuestros usuarios al servicio de Internet, lo cual es siempre insuficiente ya que para nosotros esta asignado un total de 128 Kbps de upload y 256 Kbps de download, por lo uqe se ha solicitado se nos permita contratar un proveedor del servicio local, y para este efecto se hace imprescindible la adquisición de un servidor de seguridades ya sea a nivel de IDS o IPS.

Por lo que tengo entendido un IPS(sistema de Prevención de Intrusos), es un servidor el cual se encarga de normar el ingreso a la red tanto extaerna como interna, administrar el servidor Proxy el mismo que asigna privilegios de ingreso al servicio de Internet.

Debemos tener en cuenta que Windows 2003 nos ha servido para mantener el control de los usuarios de la red como servidor de dominio, es muy importante tener en cuenta esto ya que el proyecto planteado hace mención a la implementación de un servidor de Linux lo cual es beneficioso para nosotros teniendo en cuenta que el Señor Presidente de la Republica ha manifestado que todas las instituciones deben migrar sus sistemas operativos y aplicaciones a lo que es Open Source(Codigo Abierto).

Del departamento a mi cargo se va a brindar todas las facilidades para la implementación de este y notros proyectos que vayan a beneficiar a la Fuerza Aérea.

2.3. Encuestas al personal que labora en la base Aérea largo Agrio.

Dentro de toda investigación resulta muy importante la obtención de información y una de las técnicas más utilizadas por su forma puntual y cuantificable es la Encuesta.

Dentro de la Base Aérea se cuenta con personal clasificado de la siguiente manera:

- Señores Oficiales
- Señores Aerotécnicos
- Señores Empleados Civiles

Para obtener el criterio de todo el personal que labora en la Base Aérea Lago Agrio hemos aplicado unas encuestas las mismas que han arrojado los siguientes resultados:

Primera Pregunta:

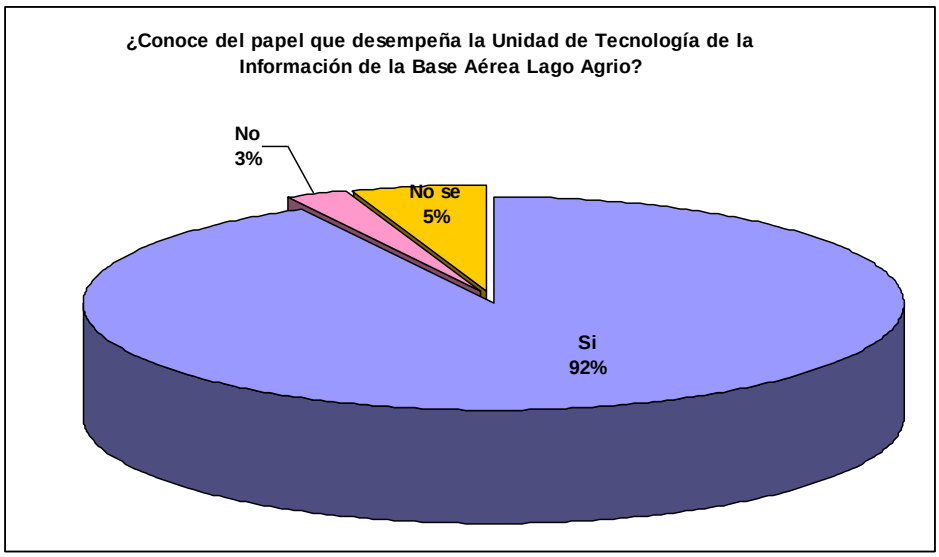
¿Conoce del papel que desempeña la Unidad de Tecnología de la Información de la Base Aérea Lago Agrio?

Tabla 2.1: Resultados pregunta 1.
Fuente: Grupo Investigador

PREGUNTA	Si	No	No se
¿Conoce del papel que desempeña la Unidad de Tecnología de la Información de la Base Aérea Lago Agrio?	35	1	2

Gráficamente y en porcentajes el personal de la Base Aérea en está pregunta se pronunciaron:

Grafico 2.1: Resultados pregunta 1.
Fuente: Grupo Investigador



A la pregunta planteada se tuvo un altísimo porcentaje que conoce de la Unidad y sobre todo que actividades desempeña, lo cual es de mucho beneficio para el normal desenvolvimiento de nuestras actividades en el proceso de implementación del servidor planteado.

Lo que si preocupa es que todavía tenemos un 5% que desconoce de la actividad de la Unidad siendo que es un pilar fundamental para el normal desenvolvimiento de las funciones del personal.

Segunda Pregunta:

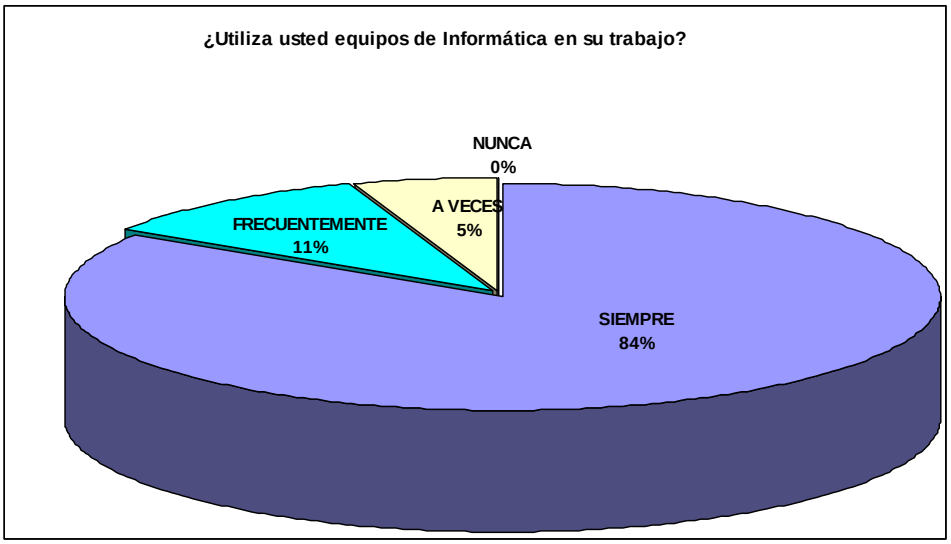
¿Utiliza usted equipos de Informática en su trabajo?

Tabla 2.2: Resultados pregunta 2.
Fuente: Grupo Investigador

PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿Utiliza usted equipos de Informática en su trabajo?	32	4	2	0

Gráficamente y en porcentajes el personal de la Base Aérea en está pregunta se pronunciaron:

Grafico 2.2: Resultados pregunta 2.
Fuente: Grupo Investigador



En la Base todos alguna vez han utilizado un equipo informático para desarrollar cualquier actividad, u lo que resulta mejor es que mas de las ¾ partes de la Base siempre están en contacto con un computador, lo que nos dice que nuestra Fuerza Aérea tiene personal capacitado.

Tercera Pregunta:

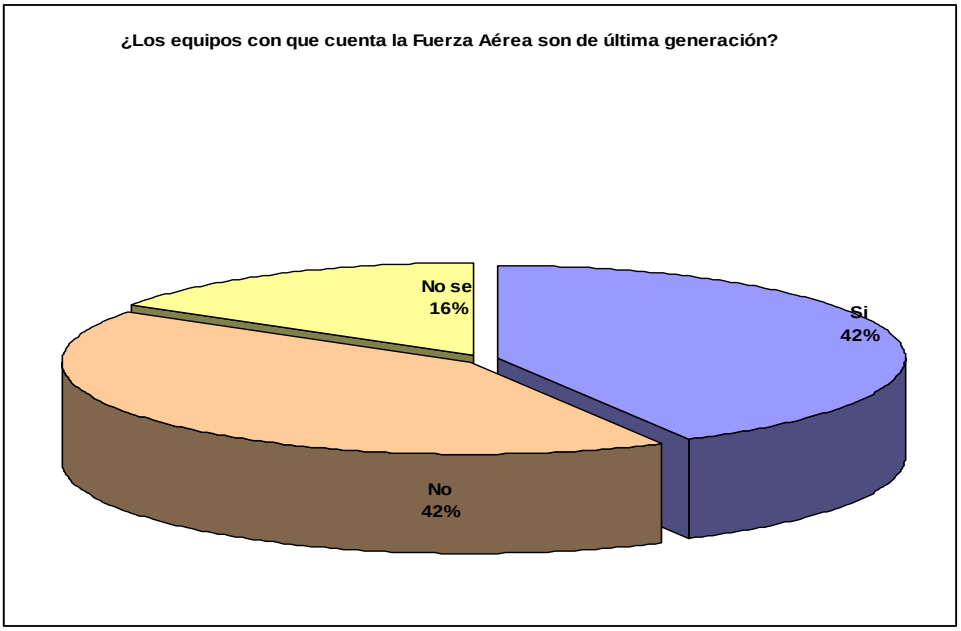
¿Los equipos con que cuenta la Fuerza Aérea son de última generación?

Tabla 2.3: Resultados pregunta 3.
Fuente: Grupo Investigador

PREGUNTA	Si	No	No se
¿Los equipos con que cuenta la Fuerza Aérea son de última generación?	16	16	6

Gráficamente y en porcentajes el personal de la Base Aérea en está pregunta se pronunciaron:

Grafico 2.3: Resultados pregunta 3.
Fuente: Grupo Investigador



Por el nivel de desempeño de actividades y las funciones que desempeñan se puede observar que conocen de características de los computadores y sobre todo tienen el conocimiento de cuales serian los equipos de ultima generación.

Se conoce de igual manera que un 16% del personal desconoce por lo que seria beneficioso para la Fuerza brindar capacitación a este personal para que este más acorde al avance tecnológico.

Cuarta Pregunta:

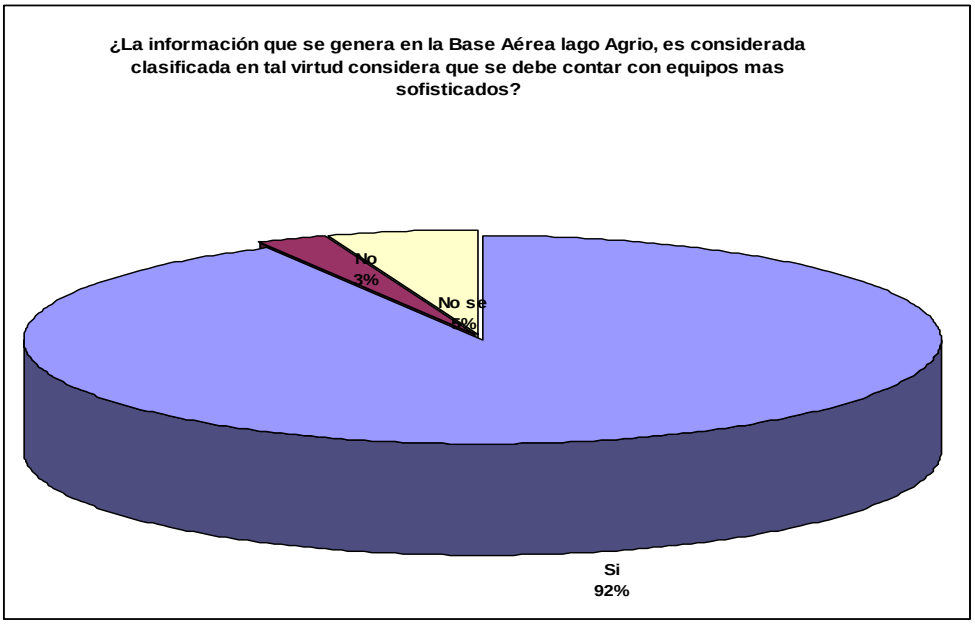
¿La información que se genera en la Base Aérea lago Agrio, es considerada clasificada en tal virtud considera que se debe contar con equipos mas sofisticados?

Tabla 2.4: Resultados pregunta 4.
Fuente: Grupo Investigador

PREGUNTA	Si	No	No se
¿La información que se genera en la Base Aérea lago Agrio, es considerada clasificada en tal virtud considera que se debe contar con equipos mas sofisticados?	35	1	2

Gráficamente y en porcentajes el personal de la Base Aérea en está pregunta se pronunciaron:

Grafico 2.4: Resultados pregunta 4.
Fuente: Grupo Investigador



La importancia de contar con un servidor de seguridades en la Base es sin lugar a dudas por el tipo de información que aquí se genera, ya que es de mucha importancia precautelar las actividades del personal.

Quinta Pregunta:

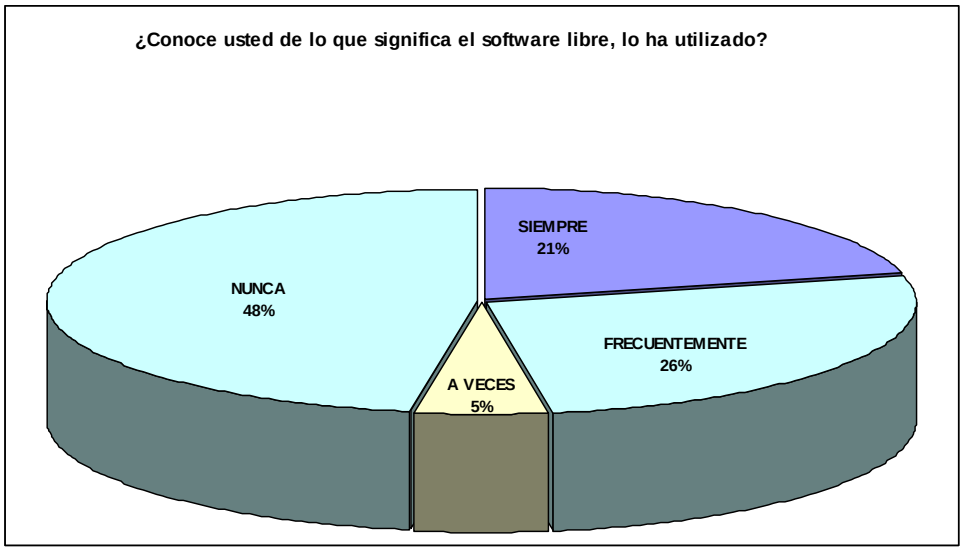
¿Conoce usted de lo que significa el software libre, lo ha utilizado?

Tabla 2.5: Resultados pregunta 5.
Fuente: Grupo Investigador

PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿Conoce usted de lo que significa el software libre, lo ha utilizado?	8	10	2	18

Gráficamente y en porcentajes el personal de la Base Aérea en está pregunta se pronunciaron:

Grafico 2.5: Resultados pregunta 5.
Fuente: Grupo Investigador



De igual manera resulta preocupante que un amplio sector de la Base no ha trabajado con Software Libre es decir no han tenido contacto con el sistema operativo Linux, y es más al desconocer de éste en la brevedad posible se debe capacitar para poder entrar en el proceso de actualización a Open Source que esta auspiciando el Señor Presidente de la Republica.

Sexta Pregunta:

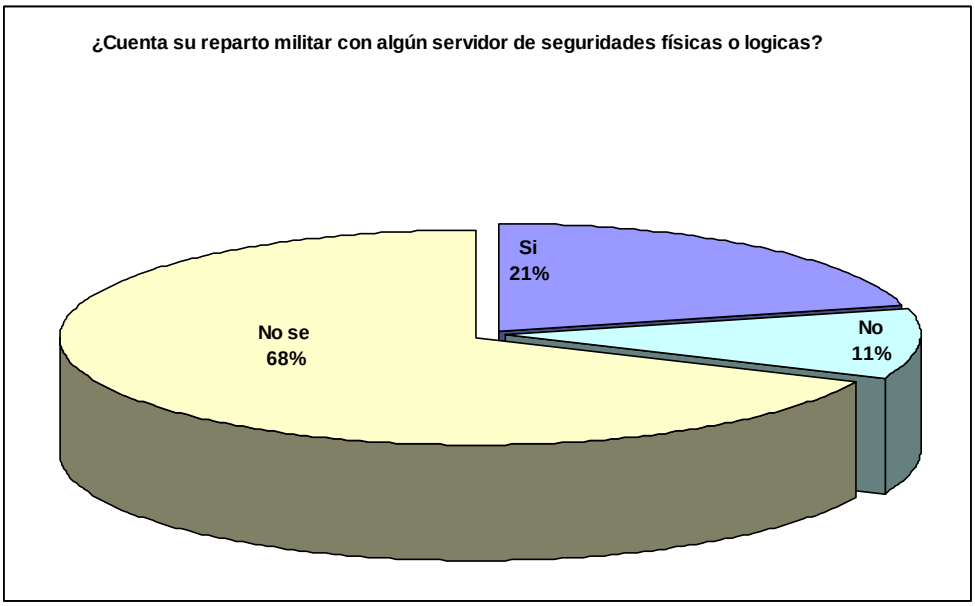
¿Cuenta su reparto militar con algún servidor de seguridades físicas o logicas?

Tabla 2.6: Resultados pregunta 6.
Fuente: Grupo Investigador

PREGUNTA	Si	No	No se
¿Cuenta su reparto militar con algún servidor de seguridades físicas o logicas?	8	4	26

Gráficamente y en porcentajes el personal de la Base Aérea en está pregunta se pronunciaron:

Grafico 2.6: Resultados pregunta 6.
Fuente: Grupo Investigador



En la base se puede observar de que existe un desconocimiento total de cómo se administra la información, lo que deja saber que se dedican a realizar su trabajo sin percatarse de donde y quien cuidad su información.

Séptima Pregunta:

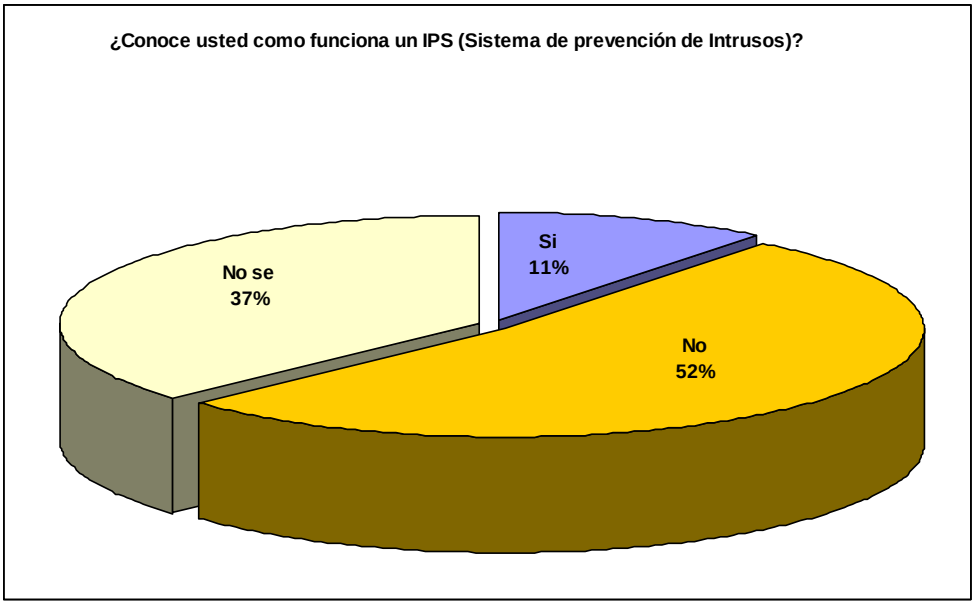
¿Conoce usted como funciona un IPS (Sistema de prevención de Intrusos)?

Tabla 2.7: Resultados pregunta 7.
Fuente: Grupo Investigador

PREGUNTA	Si	No	No se
¿Conoce usted como funciona un IPS (Sistema de prevención de Intrusos)?	4	20	14

Gráficamente y en porcentajes el personal de la Base Aérea en está pregunta se pronunciaron:

Grafico 2.7: Resultados pregunta 7.
Fuente: Grupo Investigador



Solamente el personal que está a cargo del área de sistemas y comunicaciones conocían de que es un IPS o de su funcionamiento, y el resto de personal en algunas personas habían escuchado sobre estos servidores y otros desconocían totalmente.

Muchos de ellos solamente investigan las cosas que son propias de un militar y no se interesa de conocer un poco más sobre la tecnología.

Octava Pregunta:

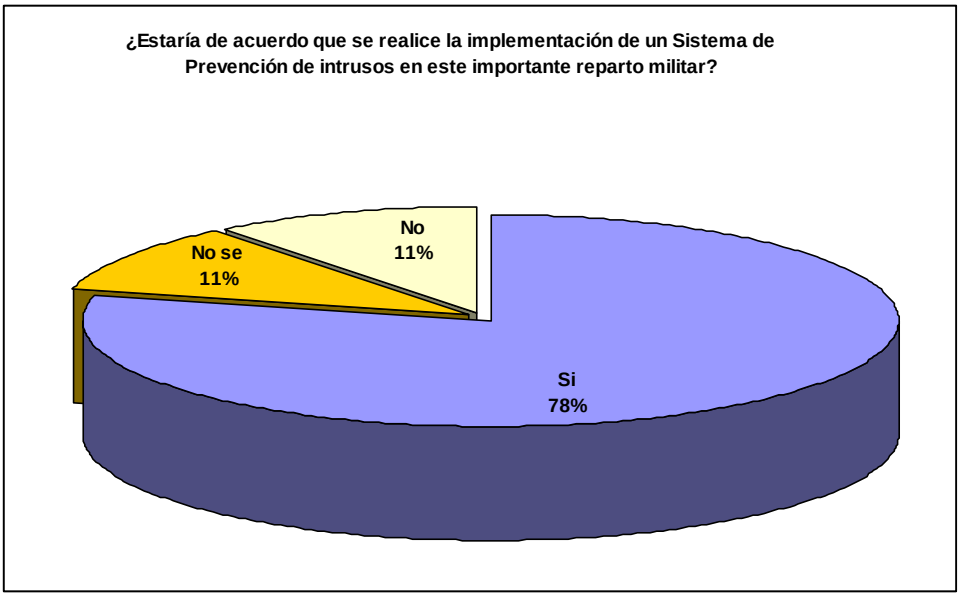
¿Estaría de acuerdo que se realice la implementación de un Sistema de Prevención de intrusos en este importante reparto militar?

Tabla 2.8: Resultados pregunta 8.
Fuente: Grupo Investigador

PREGUNTA	Si	No	No se
¿Estaría de acuerdo que se realice la implementación de un Sistema de Prevención de intrusos en este importante reparto militar?	30	4	4

Gráficamente y en porcentajes el personal de la Base Aérea en está pregunta se pronunciaron:

Grafico 2.8: Resultados pregunta 8.
Fuente: Grupo Investigador



Las opiniones vertidas sobre está pregunta resulta que no es lo esperado, ya que seria ideal que un 100% se interese que la información y todas sus actividades sean cuidadas por un servidor de seguridades.

Deja ver que a muchos miembros del personal poco o nada les interesa sobre si se mejora o no el servicio.

Novena Pregunta:

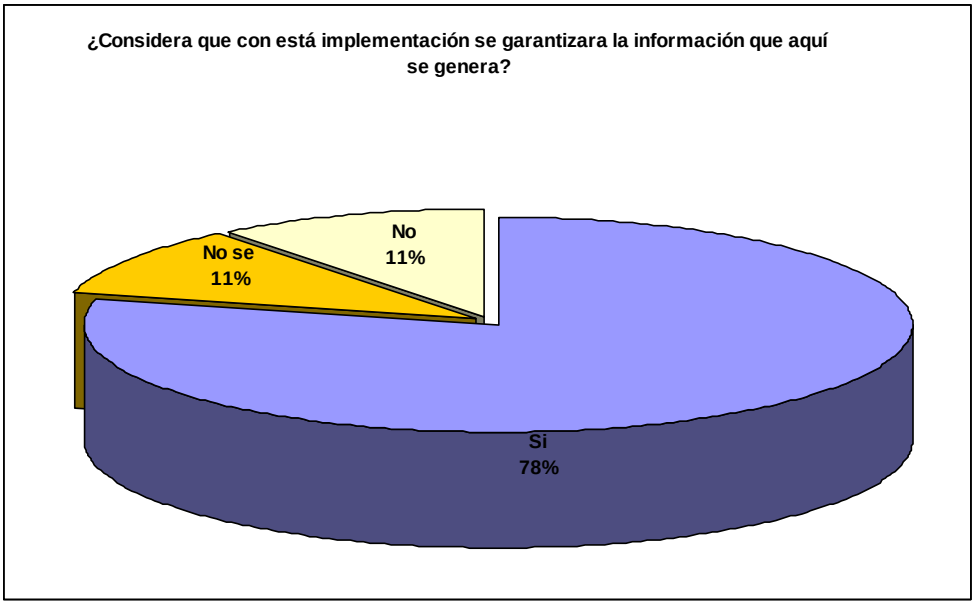
¿Considera que con está implementación se garantizara la información que aquí se genera?

Tabla 2.9: Resultados pregunta 9.
Fuente: Grupo Investigador

PREGUNTA	Si	No	No se
¿Considera que con está implementación se garantizara la información que aquí se genera?	30	4	4

Gráficamente y en porcentajes el personal de la Base Aérea en está pregunta se pronunciaron:

Grafico 2.9: Resultados pregunta 9.
Fuente: Grupo Investigador



Los que conocen sobre los IPS o tienen un poco de conocimiento de sistemas están de acuerdo con la implementación de un servidor de IPS lo que ayuda en nuestro trabajo para disponer del personal que se necesite para poder realizar las pruebas.

2.4. Análisis de las Encuestas al personal que labora en la base Aérea Lago Agrio

En términos generales tanto las entrevistas como las encuestas fueron positivas para nosotros como grupo de investigación ya que pudimos obtener datos muy importantes.

Se deja ver que dentro de la Base existe un amplio número de personal militar que desconoce de temas de tecnología lo que seria muy preocupante, más aun cuando el presidente de la republica ha manifestado que toda plataforma debe ser migrada a Código Abierto.

En un amplio numero de encuestados están de acuerdo de que las seguridades no deben ser a nivel de Fuerza Aérea sino también de forma local es decir a nivel de la Base Aérea Lago Agrio.

CAPITULO III

3. PROPUESTA PARA LA REALIZACIÓN DE LA IMPLEMENTACION DE UN SISTEMAS PREVENCION DE INTRUSOS IPS BASADO EN LINUX FEDORA ENLLA BASE AEREA LAGO AGRIO.

3.1. DISEÑO Y FACTIBILIDADES DE LAS REDES

Cada año que pasa nos encontramos en este mundo de la seguridad IT con nuevos términos, conceptos o categorías de soluciones. Y es que a pesar de que los fundamentos sean los mismos que antaño, las aproximaciones a la resolución de los problemas cambia. Este cambio viene justificado por la evolución tecnológica, por los cambios en los modelos de negocio y por qué no, por la necesidad de vender nuevos mensajes y diferenciarse la competencia. Uno de esos nuevos términos, que nos ha llegado a lo largo de los últimos meses, es el de la prevención de intrusiones.

Durante el proceso de investigación nos hemos planteado siempre una inquietud, ¿qué es exactamente la prevención de intrusiones? Para responder a esta pregunta hay que considerar cómo se hace (o debería hacer) la implantación de la defensa frente a ataques de seguridad en un entorno organizativo. Como se pudo observar en el primer capitulo de este trabajo de investigación Bruce Schneier propone un sencillo modelo de .proceso de seguridad. Basado, exclusivamente, en tres estadios asociados a la seguridad en un sistema: Prevención o Protección, Detección, y Reacción o Respuesta.

Gráfico 3.1: Modo de empleo de un IPS
Fuente: www.monografias.com/ips.html

Prevención o Protección: en este estado se han implantado elementos que protegen a los sistemas de la organización frente a ataques que

puedan producirse, basándose en un correcto análisis de riesgos que ha definido previamente los activos a proteger y las contramedidas a adoptar para protegerse de sus posibles vulnerabilidades. Dentro de los sistemas de prevención se implanta la supresión de ataques mediante la eliminación de la amenaza de forma general, evitando evitando su aparición. Es por tanto una aproximación proactiva, previa a la aparición del ataque en sí mismo. Ejemplo clásico de esta aproximación es el diseño de sistemas para que fallen de forma segura, el uso de puntos de control en una red, la defensa en profundidad y la compartimentalización.

Detección. La detección de ataques se despliega como complemento a las medidas de prevención para llenar los huecos que dejan éstas. Dicho de otra forma, para atajar el nivel de riesgo residual que no pueden rebajar las medidas de protección. Se dota a una infraestructura de medidas de detección porque se asume que las de prevención no son suficientes para atajar todos los ataques, y es necesario saber cuándo las medidas de protección no han sido efectivas.

Reacción o Respuesta. Pero la detección ha de tener siempre el complemento de la respuesta, bien automatizada (con apoyo de un sistema de decisión), bien realizada con intervención humana, es decir, de forma manual. Así, en un caso la salida del sistema de detección será una alerta, enviada a una consola o dispositivo, almacenada o impresa, en el otro, una serie de acciones encaminadas a eliminar o mitigar el ataque. El objetivo final es recuperar el sistema atacado.

3.1.1. FACTIBILIDAD TECNICA PARA LA IMPLEMENTACION

Por definición, los sistemas de detección de intrusos sólo detectan y no bloquean el tráfico no deseado. El IPS de Linux Fedora funciona en línea en la red, bloqueando el tráfico malicioso y no deseado, mientras permite pasar sin interrupciones al tráfico "bueno". De hecho, el IPS de Linux optimiza el desempeño del tráfico "bueno" al sanearla red y priorizar las aplicaciones de misión crítica. El alto desempeño y la extraordinaria precisión de la prevención de intrusos de el IPS de Linux han redefinido la seguridad de red, y han modificado fundamentalmente la forma en la que la gente protege su organización.

Ya no es necesario limpiar después de que un ciber-ataque haya comprometido sus servidores y estaciones de trabajo. Se acabó el parcheo ad-hoc y de emergencia. Se acabaron las aplicaciones dañinas fuera de control, como por ejemplo las aplicaciones P2P y la mensajería instantánea funcionando impunemente por toda la red. Los ataques de negación de servicio (DoS) que atascan las conexiones a Internet o que provocan fallos en aplicaciones de misión crítica ya son cosa del pasado.

Al eliminar el parcheo ad-hoc y las respuestas a alarmas, las soluciones de Linux Fedora permiten reducir los costos informáticos de forma continua y, mediante el ahorro de ancho de banda y la protección de las aplicaciones críticas, permiten también aumentar la productividad y la rentabilidad informática de forma continua.

El IPS de Linux ofrece las capacidades de administración más avanzadas, que son sencillas de usar y extremadamente potentes. El sistema de administración de seguridad (SMS) de Linux es una ventaja de gran confiabilidad que proporciona una visión y un control global sobre múltiples sistemas Linux. El SMS es

responsable de la recuperación, monitorización, configuración, diagnóstico, y generación de informes para hasta 1.000 sistemas operativos Linux. El SMS es un dispositivo de montaje en rack con una avanzada interfaz de cliente Java segura que permite obtener un análisis "de conjunto" con informes de tendencias, correlación y gráficos en tiempo real sobre estadísticas de tráfico, ataques filtrados, servidores y servicios de red, e inventario y estado de salud de las unidades IPS.

3.1.2. FACTIBILIDAD ECONOMICA

Siendo el Linux Fedora un sistema operativo de código abierto, la Base Aérea al adquirir el servidor se le otorgo la licencia de Linux Fedora 7, el mismo que se implemento para la administración estrictamente de seguridades a nivel de servidor y de redes.

Partiendo de que las seguridades es sin lugar a dudas lo más importante que se tiene dentro de una institución o una empresa, esta implementación va a satisfacer las necesidades de seguridades que tienen particularmente el personal de la Unidad de Tecnologías de la Información y las Comunicaciones y de forma general las Fuerzas Armadas representadas por la Fuerza Aérea.

Al no tener costo el Linux que es lo más importante se economiza una gran cantidad de dinero en relación a lo que es la firma Microsoft, sin contar que para hacer este tipo de trabajo se necesita de Hardware para poder cuidar la información y si es Microsoft se requiere de otras implementaciones tal es el caso del servidor de seguridades denominado ISA Server.

3.1.3. FACTIBILIDAD OPERACIONAL

Operativamente las seguridades basadas en Linux Fedora están dados por las características del Servidor desarrollado en Fedora, por lo cual siempre es complicado desde el momento mismo de su instalación para lo cual se debe tomar muy en cuenta algunos pasos los mismos que van a encaminar la administración de las seguridades.

Gráfico 3.2: Instalación de Linux Fedora
Fuente: Grupo Investigador

En los primeros pasos todo Linux son parecidos lo que facilita durante todo el proceso, lo que si hay que tener en cuenta es que esta versión de Linux esta diseñada para el trabajo con las seguridades de las redes, y siempre con 32 bits por el numero de Mb en memoria RAM.

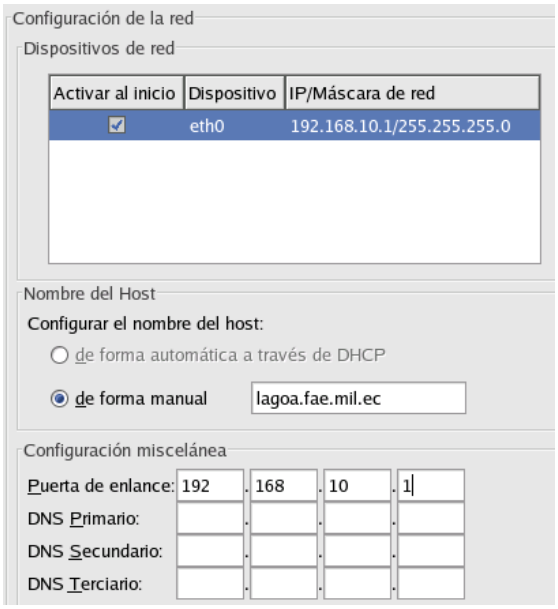


Gráfico 3.3: Configuración de red en Linux
Fuente: Grupo Investigador

Para la configuración de un IPS debemos partir como un servidor normal es decir aquel que tenga un servidor de dominios ya que es a donde se debe atacar por los hackers en su intento de irrumpir a la información de la Base Aérea. Debemos tener en cuenta que la dirección IP es la básica dentro de la clase C y de tipo particular, el dominio es el de lagoa.fae.mil.ec, que equivale a la Base Aérea Lago Agrio y que forma parte del DNS de ls Fuerza Aérea Ecuatoriana.

Las configuraciones avanzadas dentro de la implementación de un IPS esta dado por las configuraciones de las tarjetas de red y las direcciones MAC que son las que identifican a un PC o servidor.

En la actualidad por el fenómeno de saturación de las direcciones IP a nivel mundial se ha tomado en cuenta las direcciones basadas en IPv6 pero que para nuestro caso y siempre y cuando no se

encuentre 100% probadas estas direcciones nosotros no las vamos a tener en cuenta.

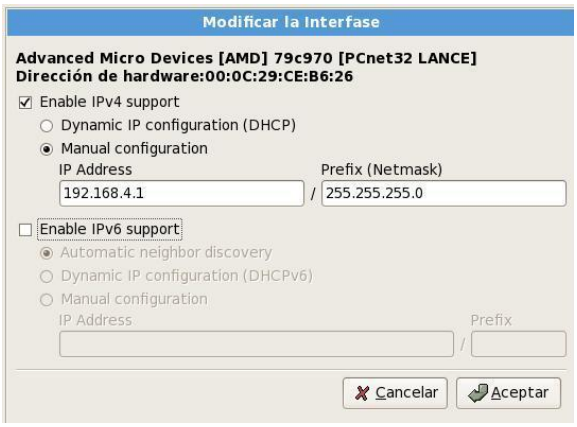


Gráfico 3.4: Configuración Avanzada de red en Linux
Fuente: Grupo Investigador

Para el servidor se tienen 3 tarjetas de red las mismas que están destinadas de la siguiente manera:

La primera está encaminada a trabajar como IPS(Sistema de Prevención de Intrusos) y que se configura como 192.168.5.1. Por ser considerado en el orden jerárquico como la quinta Base Aérea en total de personal laborando.

La segunda tarjeta es la que conecta al servidor de dominio que va administrara los usuarios que tienen Windows 2003 para logear mediante Windows XP o Windows Vista según sea el caso de conectarse a la red.

La tercera tarjeta de red va a conectar de forma segura la Intranet de la fae.mil.ec en donde se encuentra el servidor de Domino Server de Lotus Notes, el cual ya entraría con el filtro del IPS.

3.2. DISEÑO DE LA RED PLANTEADA CON SEGURIDADES

Estos IPS son evolución de los NIDS y hacen la función de un Bridge a nivel de capa dos, revisa todos los paquetes que circulan por la red en busca de firmas, si detecta alguna anomalía automáticamente es almacenado en un log, o puede permitir el paso de un paquete alterando su contenido para de esta manera frustrar un ataque, sin que el atacante se de cuenta. IPS inline más avanzados pueden realizar conexiones al DNS y obtener la identidad del atacante, gracias a que almacena los paquetes anómalos en un log.

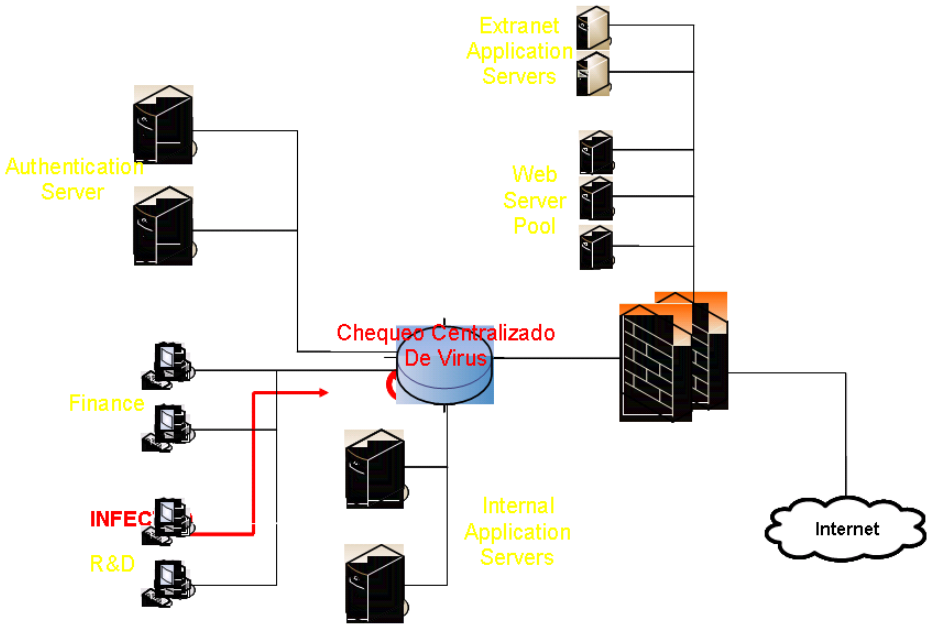


Gráfico 3.5: Configuración de una red con IPS

Fuente: Grupo Investigador

Como se puede observar en la grafica la distribución que se está dando dentro de la Base es siempre tratando de precautelar la información y nuestro equipo de IPS precautela hasta de los virus mediante centralización del antivirus, siempre con la ayuda de un firewall obviamente de la configuración del Proxy squid, habilitación del samba que permite el acceso a los archivos desde los clientes hacia el servidor de archivos, de igual manera se lo hace mediante protocolo IP.

3.2.1. SISTEMA DE PREVECION DE INTRUSOS

Como se pudo observar a lo largo del presenta trabajo de investigación los IPS(Sistema de Prevención de Intrusos),tenemos que el IPS no utiliza dirección IP como lo hace un firewall, ni funciona igual que un cortafuegos, el IPS permite poner normas y restringir acceso a usuarios, aplicaciones y a host siempre y cuando se detectan que estos están teniendo actividades mal intencionadas o código malicioso en el tráfico de la red.

Una vez configurada el IPS los accesos a los usuarios se ven de acuerdo a los privilegios que estos pueden tener, tomando en cuenta la posición y el cargo que desempeña, así como también el nivel de conocimiento que pueden tener ya que es muy importante de que no puedan afectar la información de los servidores.

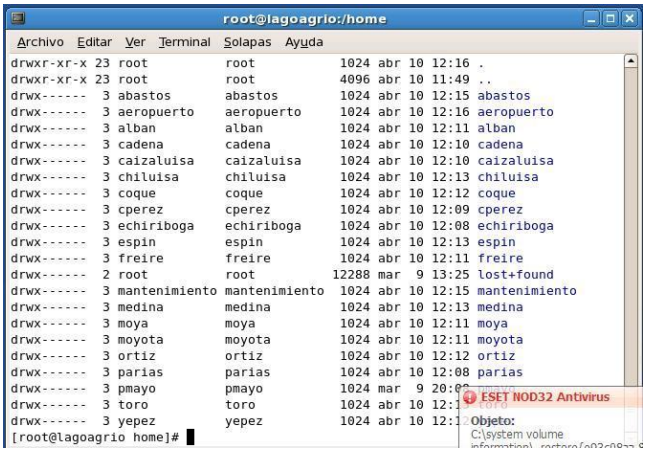


Gráfico 3.6: Privilegios de los usuarios de la Base Aérea
Fuente: Grupo Investigador

Como se observa en la grafica 3.6 al momento de prender el IPS por primera vez los usuarios no cuentan con privilegio alguno por lo que la restricción es total, es decir no se puede realizar ninguna actividad, sino es con la contraseña del Súper Usuario(Administrador).

De está manera lo que se controla es la administración total del servidor, ya que los usuarios solamente pueden logear y nada más, pero en cambio perjudica ya que siempre está activo el antivirus y por ende el firewall, y esto ocasiona cierta incomodidad en el trabajo del servidor.

Se debe precautelar la información y el desempeño de los servidores con el otorgamiento de permisos a los usuarios que lo necesiten. Siempre deben estar creados y clasificados por Grupos de Trabajo los mismos que son los que van a dar los privilegios.

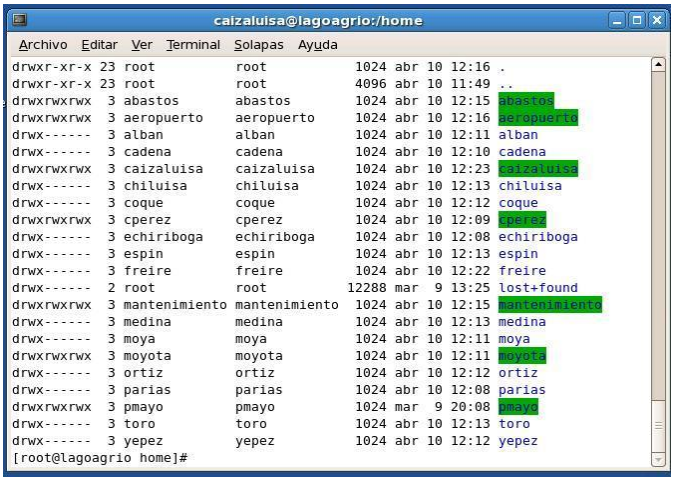


Gráfico 3.7: Privilegios de los usuarios de la Base Aérea
Fuente: Grupo Investigador

Una vez que el IPS(Sistema de Prevención de Intrusos) se encuentra configurado con los usuarios y grupos de trabajo completos se procede a dar privilegios que al tratarse de Linux, los permisos están dados por Lectura, Escritura y modificación a carpetas, archivos y usuarios.

Todos los usuarios que se encontraban el Windows 2003 Server dentro del Active Directory / Usuarios y Grupos de trabajo se les migro a Linux Fedora para la administración centralizada y no ha causado problema alguno ya que la migración fue satisfactoria, lo que se nos complico un tanto fue la adaptación por parte de los usuario ya que las pantallas de ingreso no son las que se esperaban, pero el manejo siempre era igual ya que al subir el servicio de comparticion de impresora y archivos mediante Samba no hay diferencia alguna.

3.2.2. DISTRIBUCION DE EQUIPOS EN LA RED DE AREA LOCAL

Con la implementación de un servidor IPS (Sistema de Prevención de Intrusos), lo que se consigue es precautelar la información que va hacia los servidores ya sea esta interna o externa.

El paso de la información siempre va a ser un proceso delicado más cunado se trata de una Base Aérea o institución militar ya que todo lo que aquí se genera siempre va a ser clasificado por lo que resulta importante conocer todos los usuarios o grupos de trabajo que van acceder a uno u otro servicio de la red.

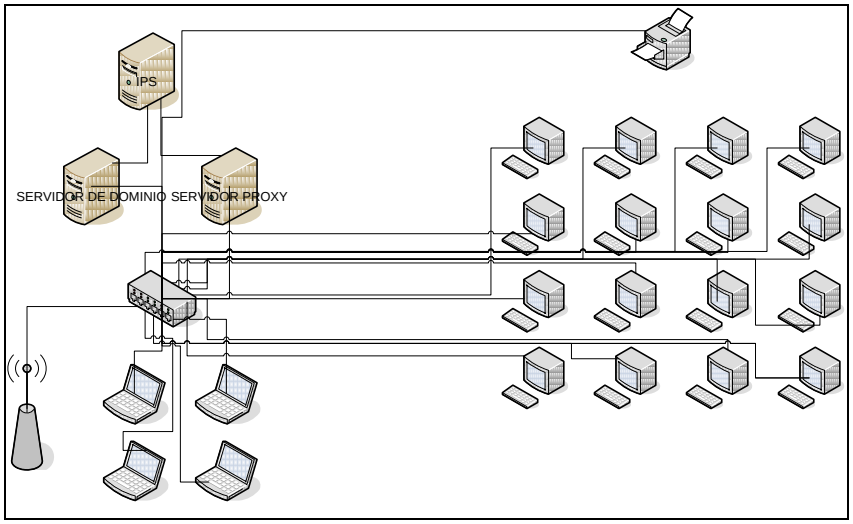


Gráfico 3.8: Distribución de los equipos en la Red
Fuente: Grupo Investigador

La distribución de los equipos se lo realizo tomando en cuenta cual es la función que desempeñan los usuarios en sus respectivas oficinas, las actividades que van a desarrollar y que tiene que ver con la utilización o no del servidor de dominio para el control de actividades.

Se ha tomado en cuenta el acceso inalámbrico de forma independiente ya que esta se utiliza solamente con usuarios que se les denomina esporádicos y que tienen privilegios solo para el acceso al Internet y para ninguna actividad adicional, lo que restringe el acceso a la impresora o a los archivos compartidos en el servidor, también esta bloqueado para la red inalámbrica el acceso a la Intranet de la FAE, por carecer de seguridades principalmente.

3.2.3. DISTRIBUCION DE LOS SERVIDORES

Sin lugar a dudas la parte medular de la investigación es el control, acceso y sobre todo administración de los servidores, siendo está tan importante la ubicación de los servidores se la debe hacer partiendo de acuerdo a la prioridad que se tenga para el manejo o frecuencia de administración de la información.

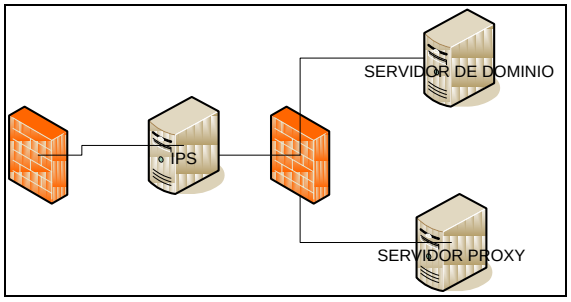


Gráfico 3.9: Distribución de los Servidores
Fuente: Grupo Investigador

En el caso de la Base Aérea Lago Agrio al tratarse de una base fronteriza el nivel de complejidad aumenta, esto hace que la información y la administración del servidor IPS(Sistema de

Prevención de Intrusos), se lo deba implementar en un sitio estratégico.

Un IPS(Sistema de Prevención de Intrusos) es un servidor que bien configurado puede ser un firewall de entrada externa e interna, puede medir el ancho de banda brindando de está manera Calidad de Servicio en todas las actividades que a través de este se realiza.

Un IPS(Sistema de Prevención de Intrusos) esta en la capacidad de brindar seguridad a los que acceden al Internet ya que funciona como servidor Proxy y tiene reglas que son configuradas mediante IPTABLES de características de un Firewall. Es importante hacer notar que en la aplicación del IPS también se le dio propiedades de un servidor samba para que puedan llevar y traer documentos desde y hace Quito que es el punto principal de la Fuerza Aérea Ecuatoriana.

3.3. ASIGNACION DE PROTOCOLOS

Para la implementación de un IPS (Sistema de Prevención de Intrusos) se debe trabajar con el protocolo TCP/IP en coordinación del protocolo IPX/SPX para la interacción entre Linux y Windows, los protocolos siempre van a ser los necesarios para poder los subir los servicios necesarios lo que es una ventaja al momento de decidir cual o que servidor es el que administra la informaron que llega hacia y desde los servidores que se encuentran centralkizados en la ciudad de Quito.

Cunado sea necesario el sistema operativo soporta o está en la capacidad la actualización a TCP/IP versión 6 es decir direcciones con 6 en Hexadecimal, mientras tanto y como la base solamente tiene un numero

reducido de equipos es necesario trabajar con las direcciones en IP v4 y en la clase C porque los equipos no exceden los 250 incluidos los servidores, el switch, el router, el DTU, los computadores que se encuentran en las redes cableadas, ni los equipos eventuales de la red inalámbrica.

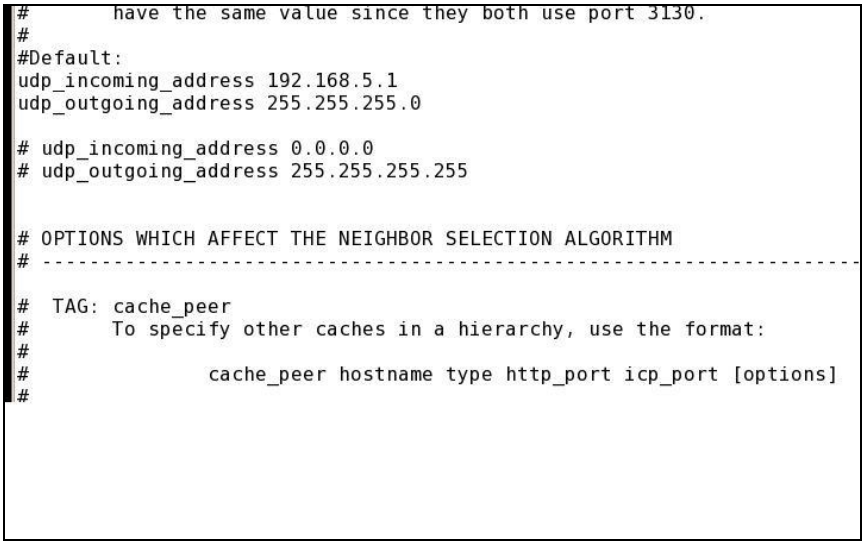


Gráfico 3.10: Configuración de Protocolos en el IPS
Fuente: Grupo Investigador

En el grafico se puede observar la configuración del IPS(Sistema de Prevención de Intrusos) del protocolo TCP/IP v4 para la administración tanto en la salida como en la entrada, que interpretando nos quiere decir que el ingreso es solamente al 192.168.5.1, mediante la mascara de subred 255.255.255.0.

3.4. ASIGNACION DE PUERTOS

Una vez configurada tanto los usuarios como los privilegios y los permisos, y que todos estos se encuentran claramente en el protocolo de transferencia

TCP/IP y que la administración local se lo hace en IPX/SPX a través de Samba, los puertos necesrios para una correcta aplicación de un IPS son lo siquienetes:

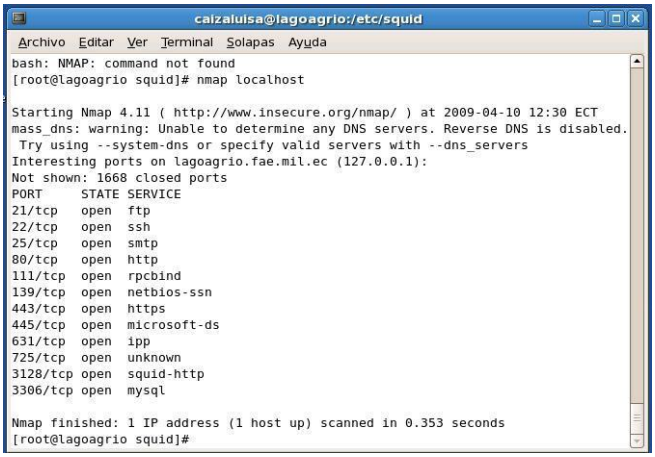


Gráfico 3.11: Configuración de Puertos en el IPS
Fuente: Grupo Investigador

Para la administración del servidor se requiere la activación de los puertos para el Protocolo de Transferencia de Archivos que es el que nos va ayudar a la actualización de la información con otras Bases del país, el SSH que es el protocolo de conexión remota de forma segura, tenemos activado el servidor Apache para en un futuro cercano activar la página Web de la base Aérea, asi como el puerto para páginas Web seguras.

La información del servidor Proxy mediante reglas reguladas con el IPTABLES se lo hará mediante el puerto 3128 y todas las salidas y entradas a través del Internet será siempre por este puerto, y ya no como se lo hacia por el puerto 80 del Proxy de Windows, hay que tener en cuenta que este puerto y este servicio mediante restricciones del firewall brinda calidad de servicio y sobre todo seguridad.

3.5. ASIGNACION MAXIMA Y ANCHO DE BANDA SEGÚN PROXY SQUID

Para la asignación de ancho de banda se lo hará solamente a la red inalámbrica ya que de está manera se precautela que no se desvié ningún KBPS ni que se puedan abrir aplicaciones no deseadas, ni pornografía y peor aun los denominados CHAT que son los que mas recursos consumen dentro del ancho de banda.

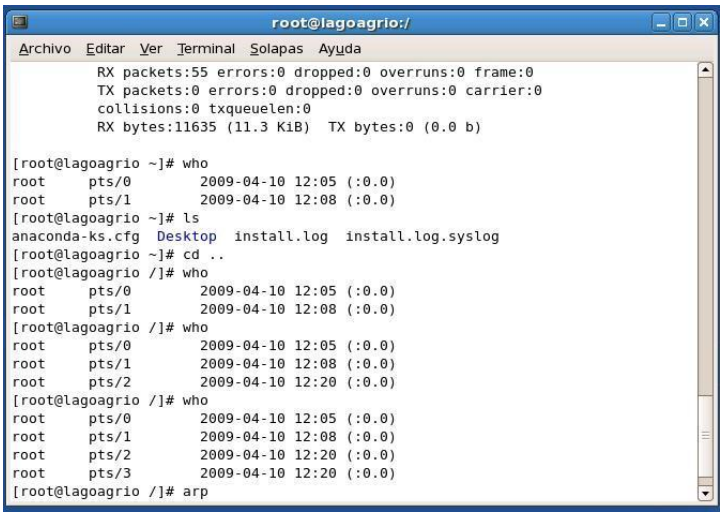


Gráfico 3.12: Control de acceso de usuarios al IPS
Fuente: Grupo Investigador

El ingreso a la red se encuentra siempre monitoreada, y conforme van accediendo al servidor se registra en un archivo de texto, en la grafica se muestra como se dan los ingresos con el tiempo y el nombre del usuario ,mediante el comando who que muestra todos los usuarios que se encuentran en la red y desde que puntos están accediendo a la red.

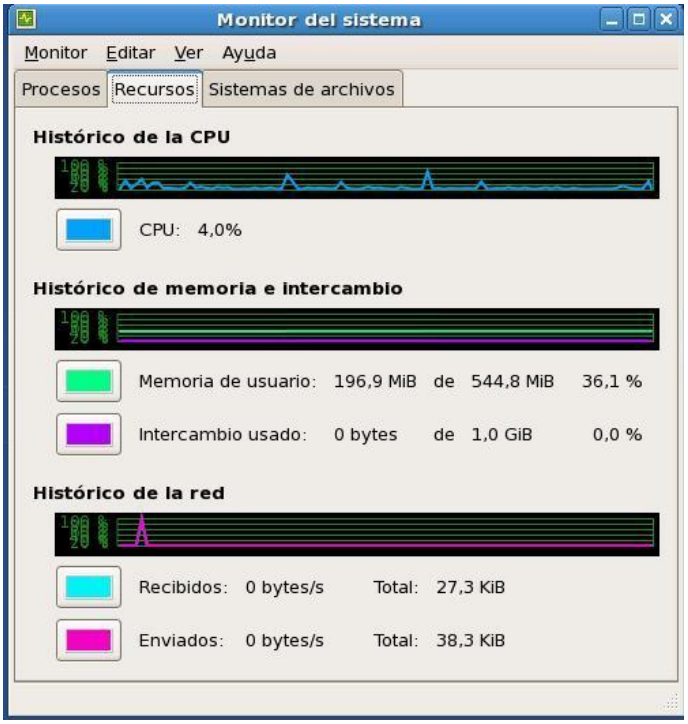


Gráfico 3.12: Monitoreo de Rendimiento en el IPS
Fuente: Grupo Investigador

La monitorización de la información y de los recursos del sistema se lo hace a través de un software que una vez configurado el IPS nos va a mostrar toda el flujo de los usuarios que pasan a través del servidor.

Existe un historial de cuando algún equipo ajeno a los logeados quiere acceder a nuestro IPS, esto de igual manera se encuentra en el archivo plano que se encuentra dentro de una carpeta llamada tmp la misma que debe tener una cierta cantidad de bytes para evitar que se sature el servidor con historiales de mal funcionamiento.

3.6. CONTROLAR DE MANERA EFICIENTE EL ACCESO A LA RED DE AREA LOCAL

Para la correcta administración del ancho de banda de la red debemos tener en cuenta que numero de usuarios disponen de un computador en horas pico es decir cuando mas numero de usuarios tienen el acceso a la red.

No es necesario o resulta utópico pensar que podríamos contar con mas de 38 usuarios por lo que el numero de puertos esta diseñado para ese numero abiertos, se conoce que en la actualidad por los costos la tendencia es a la adquisición de computadores portátiles y el acceso a la red se lo haga mediante redes inalámbricas pero resulta que ese es otro inconveniente ya que el filtrado para esta red esta totalmente apartado de el IPS ya que no se cuenta con una directiva que norme este tipo de servicio.

La red inalámbrica esta dada por las direcciones 192.168.5.200 en adelante con seguridades dadas por el Access Point el mismo que tiene el cifrado de contraseñas mediante WEP y marcación en el mismo aparato mediante la dirección MAC de la tarjeta de red del equipo que intente acceder a la red y por ende al servidor.

Contadas estas medidas lo que se trata es de que los virus no puedan hacer presa fácil de ninguno de los servidores.

Gráfico 3.13: Configuración de Puertos en el IPS
Fuente: Grupo Investigador

Cuando el IPS (Sistema de Prevención de Intrusos), se encuentra correctamente configurados debe contener los iconos propios de las actividades que realiza como se puede observar en la grafica de arriba.