ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA INGENIERIA EN SISTEMAS

“DESARROLLO DE UNA GUIA PARA EL CONTROL DE BRECHAS DE SEGURIDAD EN SERVICIOS DE INTERNET APLICADA A PETROPRODUCCION”

TESIS DE GRADO

PREVIA A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS INFORMATICOS

PRESENTADO POR:

HELMERR DANIEL AVILES CHACÓN

RIOBAMBA –ECUADOR

- 2009 -

Quiero dar gracias en primer lugar a Dios, porque me dio las fuerzas, ánimo e inteligencia necesaria para realizar esta tesis; a mis padres Gonzalo Aviles y Corina Chacón por su confianza, paciencia, y apoyo tanto emocional como económico. A mi esposa Dra. Carmen Balarezo por su comprensión y fe en mí; a mis hermanos Cristian y Karina Aviles Chacón por apoyarme, entenderme y darme el tiempo y espacio suficiente para realizar está tesis.

Agradezco también a mis maestros de Ingeniería en Sistemas de la "ESPOCH" en especial a mi maestra y amiga Ing. Ivóne Rodríguez por ser mi guía durante el proceso de elaboración de esta tesis.

¡Gracias a todos y que Dios los bendiga siempre!

Helmerr Daniel Aviles Chacón

Esta tesis está dedicada de una manera muy especial e importante para mi amada familia, por el apoyo incondicional y la confianza depositada en mí siempre, en especial a mis padres Gonzalo Aviles y Corina Chacón por haberme dado la vida y permitirme encontrar a la mujer que vive hoy a mi lado Carmen Balarezo espero que esta felicidad no termine nunca.

A mis Profesores por el empeño y la paciencia que tuvieron con mi persona, supieron proporcionarme una excelente educación humanística y específica en el área de Ingeniería en Sistemas.

Helmerr Daniel Aviles Chacón

FIRMAS DE RESPONSABLES Y NOTAS

NOMBRES	FIRMA	FECHA
Dr. Romero Rodríguez. **DECANO DE LA FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**	_____	_____
Ing. Iván Menes **DIRECTOR DE LA ESCUELA DE INGENIERÍA EN SISTEMAS**	_____	_____
Ing. Ivonne Rodríguez **DIRECTORA DE TESIS**	_____	_____
Ing. Diego Avila **MIEMBRO DEL TRIBUNAL**	_____	_____
Ing. Patricio Moreno **MIEMBRO DEL TRIBUNAL**	_____	_____
Lcd. Carlos Rodríguez **DIRECTOR DEL CENTRO DE DOCUMENTACIÓN**	_____	_____

NOTA DE LA TESIS ……

“Yo, **HELMERR DANIEL AVILES CHACÓN**, soy el responsable de las ideas, doctrinas y resultados expuestos en esta tesis, y el patrimonio intelectual de la misma pertenece a la **ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO**”.

_ _.

Helmerr Daniel Aviles Chacón

INDICE GENERAL

INDICE DE GRÁFICOS

CAPITULO II

MARCO TEORICO

CAPITULO III

ANALIZAR LA VULNERABILIDAD, LIMITACIONES DEL ENTORNO INFORMATICO Y SUS DIFERENTES NIVELES DE SEGURIDAD DE PETROPRODUCCION

CAPITULO IV

ESTUDIO DE LAS PLATAFORMAS TÍPICAS DE SEGURIDAD EN LOS SERVICIOS DE INTERNET

CAPITULO V

DESARROLLO DE GUÍA PARA EL CONTROL DE BRECHAS DE SEGURIDAD EN LOS SERVICIOS DE INTERNET APLICADA A PETROPRODUCCION

TABLA DE CONTENIDOS

CAPITULO III

ANALIZAR LA VULNERABILIDAD, LIMITACIONES DEL ENTORNO INFORMATICO Y SUS DIFERENTES NIVELES DE SEGURIDAD DE PETROPRODUCCION

CAPITULO IV

ESTUDIO DE LAS PLATAFORMAS TÍPICAS DE SEGURIDAD EN LOS SERVICIOS DE INTERNET

CAPITULO V

DESARROLLO DE GUÍA PARA EL CONTROL DE BRECHAS DE SEGURIDAD EN LOS SERVICIOS DE INTERNET APLICADA A PETROPRODUCCION

TABLA DE ANEXOS

GLOSARIO

FTP:
File Transfer Protocol.

TCP
Transmission-Control-Protocol, en español Protocolo de Control de Transmisión

IP
(Internet Protocol)

HTTP
HyperText Transfer Protocol

DHCP
Dynamic Host Configuration Protocol

SMTP
Simple Mail Transfer Protocol

SSH
Secure SHell

FTP
File Transfer Protocol,

ICMP
Protocolo de Mensajes de Control de Internet o (por sus siglas de Internet Control Message Protocol)

MIME
Multipurpose Internet Mail Extensions, Extensiones de Correo Internet Multipropósito

SNMP
El Protocolo Simple de Administración de Red (Simple Network Management Protocol)

IRC
Internet Relay Chat

NIST
National Institute for Standars and Technology

DoS
Denial of Service

L2TP
Layer To Tunneling Protocol

PPTP
Point to Point Tunneling Protocol

HTML
HyperText Markup Language

VPN
REDES PRIVADAS VIRTUALES

DMZ
(Demilitarized Zone, Zona Desmilitarizada)

IPsec
(Internet Protocol security)

ISP
Internet Service Provider

IMAP
Internet Message Access Protocol

POP3
Post Office Protocol

RPC
Remote Procedure Call, Llamada a Procedimiento Remoto

SNMP
Protocolo Simple de Administración de Red

NNTP
Network News Transport Protocol

SQL
Structured Query Language o Lenguaje de consulta estructurado

MIF
Management Information Format

WMI
Windows Management Instrumentation

MD5
Message Digest

INTRODUCCIÓN

El incremento en el uso de ordenadores y sistemas de comunicación que permiten almacenar, procesar e intercambiar grandes cantidades de información está siendo espectacular en los últimos años. Este hecho provoca, que cada vez, un mayor número de organizaciones considere a su información y a la tecnología, como uno de sus activos más importantes.

El ataque a organizaciones, empresas y demás entidades en la actualidad se dan por falta de un buen aseguramiento informático, por tener un concepto erróneo de seguridad y una inadecuada manera de asegurar su entorno informático.

A esto, se debe agregar las ya conocidas vulnerabilidades en los sistemas informáticos, que permiten, entre otras cosas, accesos no autorizados que pueden ser perjudiciales para las organizaciones, debido a que cuando existe una vulnerabilidad informática y existe alguien que la descubre puede aprovecharse de la misma, esto se genera debido a la ineficientes utilización de sistemas informáticos al nivel aplicativo que no son bien cubiertas por los mecanismos tradicionales.

Actualmente PETROPRODUCCIÓN para el ámbito de seguridad cuenta con plataforma hardware como software para asegurar su entorno informático como:

- Plataforma tanto software como hardware para Tivoli de IBM adquirido para control de Inventario y Monitoreo de la Red.
- Router que conforma el Firewall
- Dos servidores con la aplicación de Symantec Security
- Un Netenforcer

De las cuales se encuentra funcionando tan solo el Firewall y la aplicación de Symantec Security, debido a que la plataforma software y hardware de Tivoli no esta operativa, y la parte del Netenforce está en mal funcionamiento.

Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las guías son, esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Es por ello que hoy en día las empresas buscan la mejor forma de asegurar la organización y los recursos de la misma. En consecuencia surgen, tanto las empresas dedicadas a la Seguridad informática y a los servicios de consultoría para el aseguramiento de los recursos tecnológicos y humanos que se ven involucrados en la organización, como los departamentos encargados de la seguridad de tecnología de información de las organizaciones. En ambos casos, es creciente la necesidad de establecer formas para justificar frente a los clientes, o a la alta gerencia, las ganancias o beneficios que se pueden llegar a obtener al implementar un proyecto de seguridad de la información realizando las respectivas inversiones en ello.

CAPITULO I

DESARROLLO DE UNA GUIA PARA EL CONTROL DE BRECHAS DE SEGURIDAD EN SERVICIOS DE INTERNET APLICADA A PETROPRODUCCION

1.1 ANTESEDENTES

PETROPRODUCCIÓN en la actualidad maneja el ámbito de seguridad de una manera ambigua ya que no cuenta con una documentación que le guié en el aseguramiento de su entorno informático.

Por lo cual se ha planteado desarrollar una guía para el control de brechas de seguridad en los servicios de Internet aplicada a PETROPRODUCCIÓN mediante la utilización de la plataforma Astaro y software free como software de versión demo de las empresas de renombre en el ámbito de seguridad informática para de esta manera brindar y garantizar mayor seguridad en los sistemas informáticos.

La Seguridad Informática es una disciplina cuya importancia crece día a día. Aunque la seguridad es un concepto difícil de medir, su influencia afecta directamente a todas las actividades de cualquier entorno informatizado, por lo que se considerada de vital importancia su utilización. El desarrollo de una guía para el control de brechas de seguridad en los servicios de Internet para proteger de las múltiples y hasta desconocidas amenazas, permitirá garantizar fundamentalmente, la preservación de tres características: integridad, confidencialidad, disponibilidad.

Mediante el desarrollo y aplicación del sistema informático para el control de brechas de seguridad en servicios de Internet se podrá obtener una mayor eficiencia y aseguramiento del entorno informático así como también optimizar el tiempo y recursos de la empresa.

1.2 JUSTIFICACION

El amplio desarrollo de las nuevas tecnologías informáticas está ofreciendo un nuevo campo de acción a conductas antisociales y delictivas que se manifiestan en formas imposibles de imaginar, ofreciendo la posibilidad de cometer delitos tradicionales en formas no tradicionales.

La Seguridad Informática es una disciplina cuya importancia crece día a día, aunque la seguridad es un concepto difícil de medir, su influencia afecta directamente a todas las actividades de cualquier entorno informatizado, por lo que es de vital importancia.

- Integridad**:** Que garantice la talidad de los datos y los métodos de procesamiento;
- Confidencialidad**:** Que la información sea accesible sólo y exclusivamente a las personas autorizadas;
- Disponibilidad**:** Que los usuarios autorizados tengan acceso a la información y a los recursos cuando los necesiten.

El alcance del presente es desarrollar un estudio del estado actual de Seguridad Informática, que continuamente no es tomado muy en cuenta y que en realidad se lo conoce muy poco; así como también desarrollar una guía para el control de brechas de seguridad en los servicios de Internet; que si bien no brindan la solución total (como muchos prometen), podrá cubrir parte del “agujero” que hoy se presenta al hablar de Seguridad Informática.

La mayoría en el mundo informático desconoce la magnitud del problema con el que se enfrenta y, generalmente no se invierte ni el capital humano ni económico necesario para prevenir, principalmente, el daño y/o pérdida de la información que en última instancia es el conocimiento con que se cuenta.

Paradójicamente, en el mundo informático, existe una demanda constante de herramientas, metodologías, guías que están esperando a que alguien los atienda.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

- Desarrollar una guía para el control de brechas de seguridad en los servicios de Correo Electrónico, Internet, y FTP como medida de seguridad del entorno informático de PETROPRODUCCION.

1.3.2 OBJETIVOS ESPECÍFICOS

- Estudiar las plataformas típicas de seguridad para los servicios de Internet.

- Analizar la vulnerabilidad, limitaciones del entorno informático y sus diferentes niveles de seguridad de PETROPRODUCCION.

- Usar la plataforma más óptima para el control de brechas de seguridad.

- Desarrollo de la guía para el control de brechas de seguridad en Internet.

- Aplicar la guía para el control de brechas de seguridad en los servicios de Internet a PETROPRODUCCION.

1.4 HIPÓTESIS

- Mediante el desarrollo de una guía para el control de brechas de seguridad en servicios de Internet se podrá tener un mejor aseguramiento del entorno informático así como también optimizar el tiempo y recursos de la empresa.

CAPITULO II

MARCO TEORICO

El motivo del presente es realizar un estudio del estado actual de Seguridad Informática, que continuamente se pone sobre el tapete y en realidad se conoce muy poco; se suele manejar con el amarillismo de los medios no especializados, dificultando esto su accionar y colocando en tela de juicio el arduo trabajo de los especialistas. También brindare una guía para el control de brechas de seguridad, que sin bien no brindan la solución total, podrá cubrir parte del "agujero" que hoy se presenta al hablar de Seguridad Informática.

El amplio desarrollo de tecnologías informáticas están ofreciendo un nuevo campo de acción a conductas antisociales y delictivas manifestadas en formas antes imposibles de imaginar, ofreciendo la posibilidad de cometer delitos tradicionales en formas no tradicionales.

El mundo informático desconoce la magnitud del problema con el que se enfrentan día a día, generalmente no se invierte el capital humano ni económico necesario para prevenir, daños y/o pérdidas de la información que, en última instancia es el conocimiento con que se cuenta. Paradójicamente, en el mundo informático, existe una demanda constante y muy importante que está esperando a que alguien los atienda.

2.1 EVOLUCIÓN DEL TÉRMINO SEGURIDAD

La “Seguridad es una necesidad básica. Estando interesada en la prevención de la vida y las posesiones, es tan antigua como ella”

Los primeros conceptos de seguridad se evidencian en los inicios de la escritura con los Sumerios (3000 AC) o el Hammurabi (2000 AC). También en la Biblia, Homero, Cicerón, César han sido autores de obras en donde aparecen ciertos rasgos de la seguridad en la guerra y el gobierno.

Se sabe que los primitivos, para evitar amenazas, reaccionaban con los mismos métodos defensivos de los animales: luchando o huyendo (fight or flight), para eliminar o evitar la causa. Así la pugna por la vida se convertía en una parte esencial y los conceptos de alertar, evitar, detectar, alarmar y reaccionar ya eran manejados por ellos.

La primera evidencia de una cultura y organización en seguridad “madura” aparece en los documentos de la Republica (estado) de Roma Imperial y Republicana. El próximo paso de la Seguridad fue la especialización. Así nace la Seguridad Externa (Aquella que se preocupa por la amenaza de entes externos hacia la organización); y la Seguridad Interna (aquella preocupada por las amenazas de nuestra organización con la organización misma).

La seguridad desde el punto de vista técnico, la seguridad está en manos de la dirección de las organizaciones y, en última instancia, en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y el conocimiento en este nuevo milenio.

Es en este proceso en donde se aprecia que no se ha añadido ningún nuevo concepto a los ya conocidos en la antigüedad; los actuales sólo son perfeccionamientos de aquellos: llaves, cerraduras, cajas fuertes, puertas blindadas, trampas, vigilancia, y más.

“La Seguridad hoy en día es una profesión compleja con funciones especializadas”

Para dar una respuesta satisfactoria es necesario eliminar la incertidumbre y distinguir entre la seguridad filosófica y la operacional o práctica.

Analizando. En el problema planteado pueden apreciarse tres figuras[1]:

1. El poseedor del valor: Protector**.**
2. Un aspirante a poseedor: Competidor **–** Agresor**.**
3. Un elemento a proteger: Valor**.**

Luego, la Seguridad se definirá como:

"La interrelación dinámica (competencia) entre el agresor y el protector para conservar el valor tratado, enmarcada por la situación global."

Los competidores se pueden subdividir en:

- Competidor Interno**:** es aquel que piensa que el interés de la organización está por encima de sus intereses y, por lo tanto, actúa para sobreponer su interés personal, provocando daños a la organización.

- Competidor Externo**:** es aquel que actúa para arrebatar al poseedor lo que para él significa un valor empresarial o personal (clientes, mercado, información, etc.).

2.2 ANÁLISIS DEL OBJETIVO DE LA SEGURIDAD INFORMÁTICA

Para comenzar el análisis de la Seguridad Informática se deberá conocer las características de lo que se pretende proteger: la Información

Así, definimos Dato como "la unidad mínima con la que compone cierta información. Datum es una palabra latina, que significa "lo que se da".

[1] Presentación del libro "Seguridad: una Introducción". Dr MANUNTA, Giovanni. Consultor y Profesor de Seguridad de Cranfield University. Revista Seguridad Corporativa. *http://www.seguridadcorporativa.org*

La Información “es una agregación de datos que tiene un significado específico más allá de cada uno de éstos”, y tendrá un sentido particular según como y quien la procese.

Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación.

La Integridad de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

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

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

El Control sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuando y como permitir el acceso a la misma.
La Autenticidad permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

Cabe definir Amenaza, en el entorno informático, como cualquier elemento que comprometa al sistema.

Figura II.1 Amenazas para la Seguridad

Las amenazas pueden ser analizadas en tres momentos: antes del ataque durante y después del mismo. Estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema informático.

2.2.1 SISTEMA DE SEGURIDAD

Reconocimiento**:** Cada usuario deberá identificarse al usar el sistema y cada operación del mismo será registrada con esta identificación. En este proceso se quiere conseguir que no se produzca un acceso y/o manipulación indebida de los datos o que en su defecto, esta quede registrada.

Integridad**:** Un sistema integro es aquel en el que todas las partes que lo constituyen funcionan en forma correcta y en su totalidad.

Aislamiento**:** Los datos utilizados por un usuario deben ser independientes de los de otro física y lógicamente (usando técnicas de ocultación y/o compartimiento). También se debe lograr independencia entre los datos accesibles y los considerados críticos.

Auditabilidad**:** A procedimiento utilizado en la elaboración de exámenes, demostraciones, verificaciones o comprobaciones del sistema. Estas comprobaciones deben ser periódicas y tales que brinden datos precisos y aporten confianza a la dirección. Deben apuntar a contestar preguntas como:

1. ¿El uso del sistema es adecuado?
2. ¿El sistema se ajusta a las normas internas y externas vigentes?
3. ¿Los datos arrojados por el sistema se ajustan a las expectativas creadas?

4. ¿Todas las transacciones realizadas por el sistema pueden ser registradas adecuadamente?
5. ¿Contienen información referente al entorno: tiempo, lugar, autoridad, recurso, empleado, etc.?

Controlhabilidad**:** todos los sistemas y subsistemas deben estar bajo control permanente.

Recuperabilidad**:** en caso de emergencia, debe existir la posibilidad de recuperar los recursos perdidos o dañados.

Administración y Custodia**:** la vigilancia nos permitirá conocer, en todo momento, cualquier suceso, para luego realizar un seguimiento de los hechos y permitir una realimentación del sistema de seguridad, de forma tal de mantenerlo actualizado contra nuevas amenazas.

2.2.2 DE QUIEN DEBEMOS PROTEGERNOS

Se llama Intruso o Atacante a la persona que accede (o intenta acceder) sin autorización a un sistema ajeno, en forma intencional o no.
Ante la pregunta de los tipos de intrusos existentes actualmente, Julio C. Ardita [2]Contesta lo siguiente:
"Los tipos de Intrusos podríamos caracterizarlos desde el punto de vista del nivel de conocimiento, formando una pirámide.

- Clase A**:** El 80% en la base son los nuevos intrusos que bajan programas de Internet, son pequeños grupos que se juntan y dicen vamos a probar.
- Clase B: Es el 12% son más peligroso, saben compilar programas aunque no saben programar. Prueban programas, conocen como detectar que sistema operativo está usando la víctima, analizan las vulnerabilidades del mismo e ingresan por ellas.
- Clase C: es el 5%. Es gente que sabe**,** que conoce y define sus objetivos. A partir de aquí buscan todos los accesos remotos e intentan ingresar.

[2] ARDITA, Julio César. Director de Cybsec S.A. Security System y ex–Hacker. Entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. *http://www.cybsec.com*

- Clase D**:** el 3% restante. Cuando entran a determinados sistemas saben lo que buscan y necesitan.

Para llegar desde la base hasta el último nivel se tarda desde 4 a 6 años, por el nivel de conocimiento que se requiere asimilar. Es práctica, conocer, programar, mucha tarea y mucho trabajo.

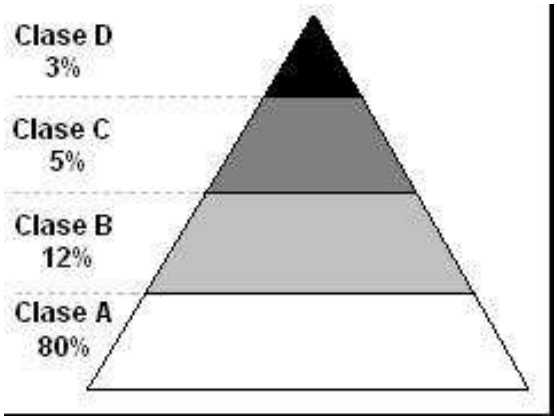


Figura II.2 – Tipos de Intrusos. Fuente: CybSec S.A. http://www.cybsec.com

2.2.3 QUE DEBEMOS PROTEGER

En cualquier sistema informático existen tres elementos básicos a proteger: el hardware, el software y los datos. Además, generalmente se habla de un cuarto elemento llamado fungible; que son los aquellos datos que se gastan o desgastan con el uso continuo: papel, toner, tinta, cintas magnéticas, disquetes.

Para cualquiera de los elementos descriptos existen multitud de amenazas y ataques que se los puede clasificar en:

1. Ataques Pasivos**:** El atacante no altera la comunicación, sino que únicamente la "escucha" o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico. Generalmente se emplean para:

- Obtención del origen y destinatario de la comunicación, a través de la lectura de las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

2. Ataques Activos**:** Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos. Generalmente son realizados por hackers, piratas informáticos o intrusos remunerados y se los puede subdividir en cuatro categorías:

- Interrupción**:** Si hace que un objeto del sistema se pierda, quede inutilizable o no disponible.
- Intercepción**:** Si un elemento no autorizado consigue el acceso a un determinado objeto del sistema.
- Modificación**:** Si además de conseguir el acceso consigue modificar datos e información.
- Fabricación**:** Se consigue un objeto similar al original atacado de forma que es difícil distinguirlos.
- Destrucción**:** Es una modificación que destruye el objeto.

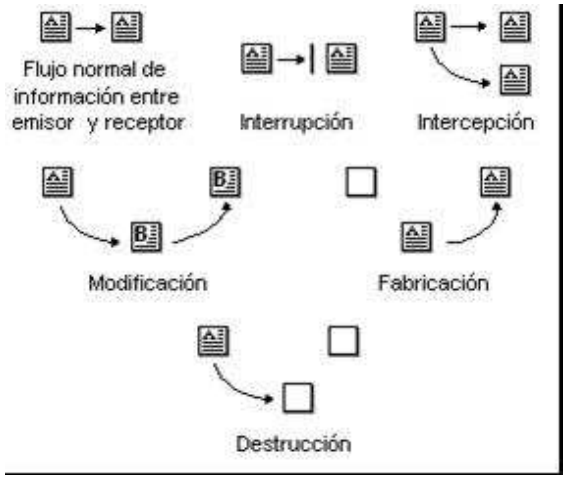


Figura II.3 – Tipos de Ataques Activos. Fuente

Con demasiada frecuencia se cree que los piratas son lo únicos que amenazan nuestro sistema, siendo pocos los administradores que consideran todos los demás riesgos analizados en el presente.

2.2.4 RELACION OPERATIVIDAD SEGURIDAD

Seleccionar las medidas de seguridad a implantar requiere considerar el equilibrio entre los intereses referidos a la seguridad, los requerimientos operacionales y la "amigabilidad" para el usuario.
Para enseñar lo antes dicho imaginemos una computadora “extremadamente” segura:

- Instalada a 20 metros bajo tierra en un recinto de hormigón.
- Aislada informativamente de otras computadoras.
- Aislada eléctricamente y alimentada por un sistema autónomo de triple reemplazo.

Ahora imaginemos la utilidad de está “súper segura” computadora: tendiente a nula. Con esto refleja que la Seguridad y la Utilidad de una computadora son inversamente proporcionales; es decir que incrementar la seguridad en un sistema informático, su operatividad desciende y viceversa.

$$\text{Operatividad} = -\frac{1}{\text{Seguridad}}$$

Como se observa en la Figura II.4 esta función se vuelve exponencial al acercarse al 100% de seguridad. Los costos se disparan (tendientes al infinito) por los complejos estudios que se deberán realizar para mantener este grado de seguridad.

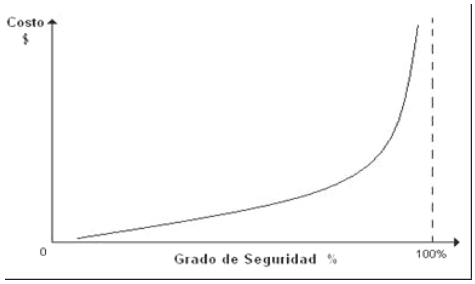


Figura II.4 – Relación Operatividad – Seguridad.

Más allá de ello, al tratarse de una ciencia social, no determinada, se mantendrá la incertidumbre propia del comportamiento humano, que puede permitir a un atacante violar el sistema, haciendo que los costos hayan sido, si bien no inútiles o excesivos.

Debemos recordar que el concepto de seguridad es relativo, pues no existe una prueba total contra engaños, sin embargo existen niveles de seguridad mínimos exigibles. Este nivel dependerá de un análisis de los riesgos que estamos dispuestos a aceptar, sus costos y de las medidas a tomar en cada caso.

- El 40% de las empresas estudiadas consideran como problema grave la seguridad informática.
- El "gasto" en seguridad informática oscila entre el 4% y el 10% del gasto total informático.
- El 83% de las empresas reconoce no haber emprendido nunca acciones legales después de un ataque.
- El 72% se muestra reacia a admitir que sus sistemas han sido saboteados.
- El 79% cree que existen mayores probabilidades de sufrir un ataque informático procedente del exterior.
- El 66% consideran a la seguridad y privacidad de la información el impedimento principal para el crecimiento del e – comerse.
- El 80% manifestó no haber experimentado un ataque por intrusión durante el año anterior; pero sólo el 33% indicó su capacidad para la detección de dichos ataques.
- Sólo el 39% hace uso de software estándar de seguridad y el 20% de este total hace uso avanzado de estas herramientas.

2.3 SEGURIDAD LÓGICA

Es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputo no será sobre los medios físicos sino contra información por él almacenada y procesada.
El activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la seguridad lógica. Es decir que la seguridad lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

Los objetivos que se plantean serán:

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

2.4 CONTROLES DE ACCESO

Estos controles pueden implementarse en el sistema operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso. Al respecto, el National Institute for Standars and Technology (NIST) [3] ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

2.4.1 IDENTIFICACIÓN Y AUTENTIFICACIÓN

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Desde el punto de vista la eficiencia, es conveniente para que los usuarios sean identificados y autenticados solamente una vez, de esta manera podrán acceder, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina "single log–in" o sincronización de passwords.

2.4.2 MODALIDAD DE ACCESO

Se refiere al modo de acceso que utiliza al usuario sobre los recursos y a la información. Esta modalidad puede ser:

- Lectura**:** El usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
- Escritura**:** Este tipo de acceso permite agregar datos, modificar o borrar información.
- Ejecución**:** Este acceso otorga al usuario el privilegio de ejecutar programas.
- Borrado**:** Permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.

[3] http://www.nist.gov

2.4.3 CONTROL DE ACCESO EXTERNO

Para el control de acceso externo tenemos un grupo de controles que se deben tener en cuenta los cuales se detallan a continuación.

2.4.3.1 DISPOSITIVOS DE CONTROL DE PUERTOS

Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.

2.4.3.2 FIREWALLS O PUERTAS DE SEGURIDAD

Permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada y otra externa (por ejemplo Internet). Los firewalls permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización.

2.4.3.3 ACCESOS PÚBLICOS

Para los sistemas de información consultados por el público en general, o los utilizados para distribuir o recibir información computarizada (por ejemplo, la distribución y recepción de formularios en soporte magnético, o la consulta y recepción de información a través del correo electrónico) deben tenerse en cuenta medidas especiales de seguridad, ya que se incrementa el riesgo y se dificulta su administración.

Debe considerarse para estos casos de sistemas públicos, que un ataque externo o interno puede acarrear un impacto negativo en la imagen de la organización.

2.4.4 ADMINISTRACIÓN

Una vez establecidos los controles de acceso sobre los sistemas y la aplicación, es necesario realizar una eficiente administración de estas medidas de seguridad lógica, lo que involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

La definición de los permisos de acceso requiere determinar cual será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible clasificar la información, determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados.

2.5 DELINCUENTE Y VICTIMA

2.5.1 SUJETO ACTIVO

Se llama así a las personas que cometen los delitos informáticos. Son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

2.6 AMENAZAS HUMANAS

Este apartado trata sobre cada uno de los personajes que pueden ser potenciales atacantes de nuestro sistema: el mundo under y el personal perteneciente a la organización. Será difícil mantener una posición objetiva de la situación global en cuanto a los hackers y las fuerzas de seguridad, ya que siempre he visto marcado mi camino de conocimiento por la curiosidad: principal ingrediente (como veremos) el hacker. Así mismo, siempre me he mantenido en la raya de la legalidad y la ética, siendo prueba de esto el presente documento.

2.6.1 LA ACTITUD DEL HACKER

Como en las artes creativas, el modo más efectivo de transformarse en un maestro es imitar la mentalidad de los maestros, no sólo intelectualmente, sino además emocionalmente. Se deberá aprender a puntuarse, principalmente, en función de lo que los otros hackers piensan acerca de las habilidades obtenidas (éste es el motivo por el cual no se puede ser un hacker de verdad hasta que otros hackers lo denominen así de manera consistente). Este hecho está empañado por la imagen del trabajo de hacker como trabajo solitario; también por un tabú cultural de los hackers (si bien en la actualidad es menor, aún es fuerte) que

impide que se admita al ego o la validación externa como elementos involucrados en la propia motivación.

2.6.2 DEFINICIÓN DE HACKER

Un Hacker es una persona que está siempre en una continua búsqueda de información, vive para aprender y todo para él es un reto; no existen barreras, y lucha por la difusión libre de información, distribución de software sin costo y la globalización de la comunicación.

El concepto de hacker, generalmente es confundido erróneamente con los mitos que existen acerca de este tema:

- Un hacker es pirata. Esto no es así ya que los piratas comercian con la información que obtienen, entre otras cosas, y un verdadero hacker solo obtiene esa información para su uso personal.
- Un hacker es el que entra en los sistemas ajenos y se dedica a destruir la información almacenada en ellos. El error consiste en que aquel que destruye información y sistemas ajenos, no es el hackers sino el Cracker.

"Nótese que ninguna definición define al Hacker como un criminal. En el mejor de los casos, los Hackers cambian precisamente la fabricación de la información en la que se sustenta la sociedad y contribuyen al flujo de tecnología. En el peor, los Hackers pueden ser traviesos perversos o exploradores curiosos. Los Hackers NO escriben dañinos virus de computadora. Quienes lo hacen son los programadores tristes, inseguros y mediocres. Los virus dañinos están completamente en contra de la ética de los Hackers" [4]

2.6.3 CRACKERS

Los Crackers, en realidad, son hackers cuyas intenciones van más allá de la investigación. Es una persona que tiene fines maliciosos o de venganza, quiere demostrar sus habilidades pero de la manera equivocada o simplemente personas que hacen daño solo por diversión. Los hackers opinan de ellos que son "... Hackers mediocres, no demasiados brillantes, que buscan violar (literalmente "break") un sistema".

[4] *http://www2.vo.lu/homepages/phahn/humor/hacker30.txt*

2.6.4 PHREAKERS

Otro personaje en el Underground es el conocido como Phreaker[5]. El Phreaking, es la actividad por medio de la cual algunas personas con ciertos conocimientos y herramientas de hardware y software, pueden engañar a las compañías telefónicas para que éstas no cobren las llamadas que se hacen.

La realidad indica que lo Phreakers son Cracker de las redes de comunicación. Personas con amplios (a veces mayor que el de los mismos empleados de las compañías telefónicas) conocimientos en telefonía.

2.6.5 CARDING – TRASHING

Entre las personas que dedicaban sus esfuerzos a romper la seguridad como reto intelectual hubo un grupo (con no tan buenas intenciones) que trabajaba para conseguir una tarjeta de crédito ajena. Así nació:

- El Carding, es el uso (o generación) ilegitimo de las tarjetas de crédito (o sus números), pertenecientes a otras personas con el fin de obtener los bienes realizando fraude con ellas. Se relaciona mucho con el Hacking y el Cracking, mediante los cuales se consiguen los números de las tarjetas.
- El Trashing, que consiste en rastrear en las papeleras en busca de información, contraseñas o directorios.

2.7 PERSONAL (INSIDERS)

Hasta aquí se ha presentado al personal como víctima de atacantes externos; sin embargo, de los robos, sabotajes o accidentes relacionados con los sistemas informáticos, el 70% son causados por el propio personal de la organización propietaria de dichos sistemas (“Inside Factor”). Hablando de los Insiders Julio C. Ardita[6] explica que “(...) desde mitad de 1996 hasta 1999 la empresa tuvo dos casos de intrusiones pero en el 2000 registramos siete, de las cuales 5 eran intrusos internos o ex–empleados.

---

[5] Fusión de las palabras Freak, Phone y Free: Mounstruo de los Teléfonos Libres (intento de traducción literal)

[6] ARDITA, Julio César. Director de Cybsec S.A. Security System y ex–Hacker. Entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. *http://www.cybsec.com*

En la Figura II.5 detalla los porcentajes de intrusiones clasificando a los atacantes en internos y externos.

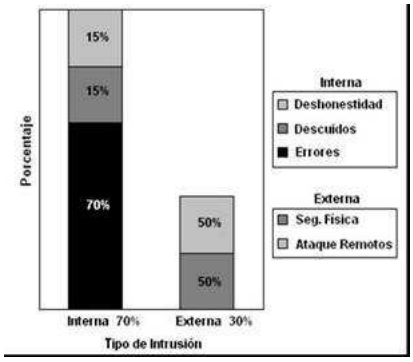


Figura II.5 – Intrusiones. Fuente: http://www.cybsec.com

Esto es realmente preocupante, ya que, una persona que trabaje con el administrador, el programador o el encargado de una máquina conoce perfectamente el sistema, sus puntos fuertes y débiles; de manera que un ataque realizado por esa persona podrá ser más directo, difícil de detectar y más efectivo que el que un atacante externo pueda realizar.

2.7.1 PERSONAL INTERNO

Las amenazas a la seguridad de un sistema, provenientes del personal del propio sistema informático, rara vez es tomada en cuenta porque se supone un ámbito de confianza muchas veces inexistente. Generalmente estos ataques son accidentes por desconocimiento o inexistencia de las normas básicas de seguridad; pero también pueden ser del tipo intencional. Es de destacar que un simple electricista puede ser más dañino que el más peligroso de los piratas informáticos, ya que un corte de energía puede causar un desastre en los datos del sistema. Al evaluar la situación, se verá que aquí el daño no es intencionado pero ello no está en discusión; el daño existió y esto es lo que compete a la seguridad informática.

2.7.2 EX –EMPLEADO

Este grupo puede estar especialmente interesado en violar la seguridad de nuestra empresa, sobre todo aquellos que han sido despedidos y no han quedado conformes; o bien aquellos

que han renunciado para pasar a trabajar en la competencia. Generalmente se trata de personas descontentas con la organización que conocen a la perfección la estructura del sistema y tienen los conocimientos necesarios como para causar cualquier tipo de daño. También han existido casos donde el ex–empleado deja Bombas Lógicas que “explotan” tiempo después de marcharse.

2.8 SERVICIOS DE INTERNET

Como sabemos, Internet es en la actualidad, la red de computadoras más grande del mundo. Sin embargo la importancia de Internet no reside solamente en el número de máquinas interconectadas sino en los servicios que brinda.

Los servicios y recursos de Internet (Gopher, News, Archie, WWW, etc.) son accesibles de diversas formas, principalmente tres: por Telnet, por e–mail, y por un programa cliente.

A través de Telnet o e–mail, el servicio presenta una interface ANSI (sin gráficos), sólo con caracteres alfanuméricos. Con un programa cliente, la gestión es más sencilla, visual y agradable, como sucede en la WWW donde se presentan cada una de las páginas en formato gráfico.

2.8.1 ICMP

El Internet Control Message Protocol es de características similares al UDP, pero con un formato aún más simple. Su utilidad no está en el transporte de datos "de usuario", sino en los mensajes de error y de control necesarios para los sistemas de la red.

2.8.2 FTP

El File Transfer Protocol se incluye como parte del TCP/IP, estando destinado proporcionar el servicio de transferencia de archivos. El FTP depende del protocolo TCP para las funciones de transporte, y guarda alguna relación con Telnet (protocolo para la conexión remota). FTP utiliza dos canales de conexión separados: uno es el canal de comandos que permanece abierto durante toda la sesión y el otro es el canal de transmisión de archivos.

El FTP permite acceder a algún servidor que disponga de este servicio y realizar tareas tales como moverse a través de su estructura de directorios, ver y descargar archivos al ordenador local, enviar o copiar archivos directamente de un servidor a otro de la red. Lógicamente y por motivos de seguridad se hace necesario contar con el permiso previo para poder realizar todas estas operaciones. El servidor FTP pedirá el nombre de usuario y clave de acceso al iniciar la sesión (login). Este debe ser suministrado correctamente para poder utilizar el servicio.

2.8.3 HTTP

Este HiperText Tranfer Protocol es la base de toda comunicación desarrollada en la Web. Utilizado desde principios de lo 90 es un protocolo ASCII que se ocupa de establecer una comunicación TCP segura entre el cliente y el servidor a través del puerto 80.

2.8.4 SMTP

El servicio de correo electrónico se proporciona a través del protocolo Simple Mail Transfer Protocol, (empleando redes TCP/IP) y permite enviar mensajes a otros usuarios de la red. A través de estos mensajes no sólo se puede intercambiar texto, sino también archivos binarios de cualquier tipo. El cliente de correo envía una solicitud a su e–mail Server (al puerto 25) para enviar un mensaje (y almacenarlo en dicho servidor). El Server establece una conexión SMTP donde emisor y receptor intercambian mensajes de identificación, errores y el cuerpo del mail. Luego de esto el emisor envía los comandos necesarios para la liberación de la conexión.

2.8.5 MIME

1. MIME–Versión: especifica la versión de MIME utilizado para codificar el mensaje.
2. Content–Type: especifica el tipo y subtipo de los datos no ASCII.
3. Contenet–Tranfer–Encoding: especifica el tipo de codificación usado para traducir los datos en ASCII.

2.8.6 SNMP

El Simple Network Management Protocol se utiliza para monitorizar, controlar y administrar múltiples redes físicas de diferentes fabricantes, donde no existe un protocolo común en la capa de Enlace. La estructura de este protocolo se basa en utilizar la capa de aplicación para evitar el contacto con la capa de enlace y, aunque es parte de la familia TCP/IP no depende del IP ya que fue diseñado para ser independiente y puede correr igual de fácil sobre, por ejemplo, IPX de Novell.

2.8.7 IRC

El Internet Relay Chat es un sistema de coloquio en tiempo real entre personas localizadas en distintos puntos de la red. Es un servicio basado exclusivamente en texto por teclado. Fue desarrollado en 1988 en Finlandia y es sin duda, hoy, uno de los servicios más populares de Internet.

Su gran atractivo es que permite las conversaciones en vivo de múltiples usuarios la mayor parte desconocidos entre sí. El manejo del sistema es muy simple. El IRC está organizado por redes, cada una de las cuales está formada por servidores que se encargan, entre otras cosas, de ofrecer canales de conversación (existiendo miles de ellos) y transmitir los mensajes entre usuarios.

2.8.8 FINGER

La mayoría de las computadoras de Internet tienen una utilidad que permite buscar información sobre un usuario particular. Este servicio es conocido como Finger (dedo).

En Internet los usuarios se conocen por su identificador. Finger se puede utilizar para encontrar el nombre de un usuario si se conoce su identificador, ya que el objetivo de este servicio es obtener información sobre una persona en particular.

El servicio Finger es un sistema Cliente/Servidor que proporciona tres tipos principales de información:

1. Información pública sobre cualquier usuario.
2. Comprobación de si un usuario está utilizando actualmente un Host determinado en Internet, pudiendo ver un resumen de información para cada usuario que está conectado.
3. Conectar con determinado Host, que se han configurado para ofrecer otros tipos de información.

2.9 AMENAZAS LOGICAS

La Entropía es una magnitud termodinámica que cuantifica el grado de desorden de un sistema; y según las leyes físicas todo sistema tiende a su máxima entropía. Si extrapolamos este concepto a la Seguridad resultaría que todo sistema tiende a su máxima inseguridad. Este principio supone decir:

- Los protocolos de comunicación utilizados carecen, en su mayoría, de seguridad o esta ha sido implementada, tiempo después de su creación, en forma de “parche”.
- Existen agujeros de seguridad en los sistemas operativos.
- Existen agujeros de seguridad en las aplicaciones.
- Existen errores en las configuraciones de los sistemas.
- Los usuarios carecen de información respecto al tema.
- Todo sistema es inseguro.

Esta lista podría seguir extendiéndose a medida que se evalúen mayor cantidad de elementos de un Sistema Informático.

2.9.1 ACCESO USO AUTORIZACION

La identificación de estas palabras es muy importante ya que el uso de algunas implica un uso desapropiado de las otras.

Específicamente “Acceso” y “Hacer Uso” no son el mismo concepto cuando se estudian desde el punto de vista de un usuario y de un intruso. Por ejemplo:

- Cuando un usuario tiene acceso autorizado, implica que tiene autorizado el uso de un recurso.
- Cuando un atacante tiene acceso desautorizado está haciendo uso desautorizado del sistema.
- Pero, cuando un atacante hace uso desautorizado de un sistema, esto implica que el acceso fue autorizado (simulación de usuario).

Luego un Ataque será un intento de acceso, o uso desautorizado de un recurso, sea satisfactorio o no. Un Incidente envuelve un conjunto de ataques que pueden ser distinguidos de otro grupo por las características del mismo (grado, similitud, técnicas utilizadas, tiempos, etc.).

John D. Howard[7] en su tesis estudia la cantidad de ataques que puede tener un incidente. Al concluir dicho estudio y basado en su experiencia en los laboratorios del CERT[8] afirma que esta cantidad varía entre 10 y 1.000 y estima que un número razonable para estudios es de 100 ataques por incidentes.

2.9.2 DETECCIÓN DE INTRUSOS

A finales de 1996, Dan Farmer (creador de una de las herramientas más útiles en la detección de intrusos: SATAN) realizó un estudio sobre seguridad analizando 2.203 sistemas de sitios en Internet. Los sistemas objeto del estudio fueron Web Sites orientados al comercio y con contenidos específicos, además de un conjunto de sistemas informáticos aleatorios con los que realizar comparaciones.

El estudio se realizó empleando técnicas sencillas y no intrusivas. Se dividieron los problemas potenciales de seguridad en dos grupos: rojos (red) y amarillos (yellow). Los problemas del grupo rojo son los más serios y suponen que el sistema está abierto a un atacante potencial, es decir, posee problemas de seguridad conocidos en disposición de ser explotados.

---

[7] HOWARD, John D. Thesis: An Analysis of security on the Internet Carnegie Institute of Technology. Carnegie Mellon University. EE.UU. *http://www.cert.org*. Capítulo 12–Página 165

[8] *http://www.cert.org*

2.9.3 IDENTIFICACIÓN DE LAS AMENAZAS

La identificación de amenazas requiere conocer los tipos de ataques, el tipo de acceso, la forma operacional y los objetivos del atacante como se muestra en la figura 1.
Las consecuencias de los ataques se podrían clasificar en:

- Data Corruption: la información que no contenía defectos pasa a tenerlos.
- Denial of Service (DoS): servicios que deberían estar disponibles no lo están.
- Leakage: los datos llegan a destinos a los que no deberían llegar.

Desde 1990 hasta nuestros días, el CERT viene desarrollando una serie de estadísticas que demuestran que cada día se registran más ataques informáticos, y estos son cada vez más sofisticados, automáticos y difíciles de rastrearse, como se muestra en la Figura II.6.

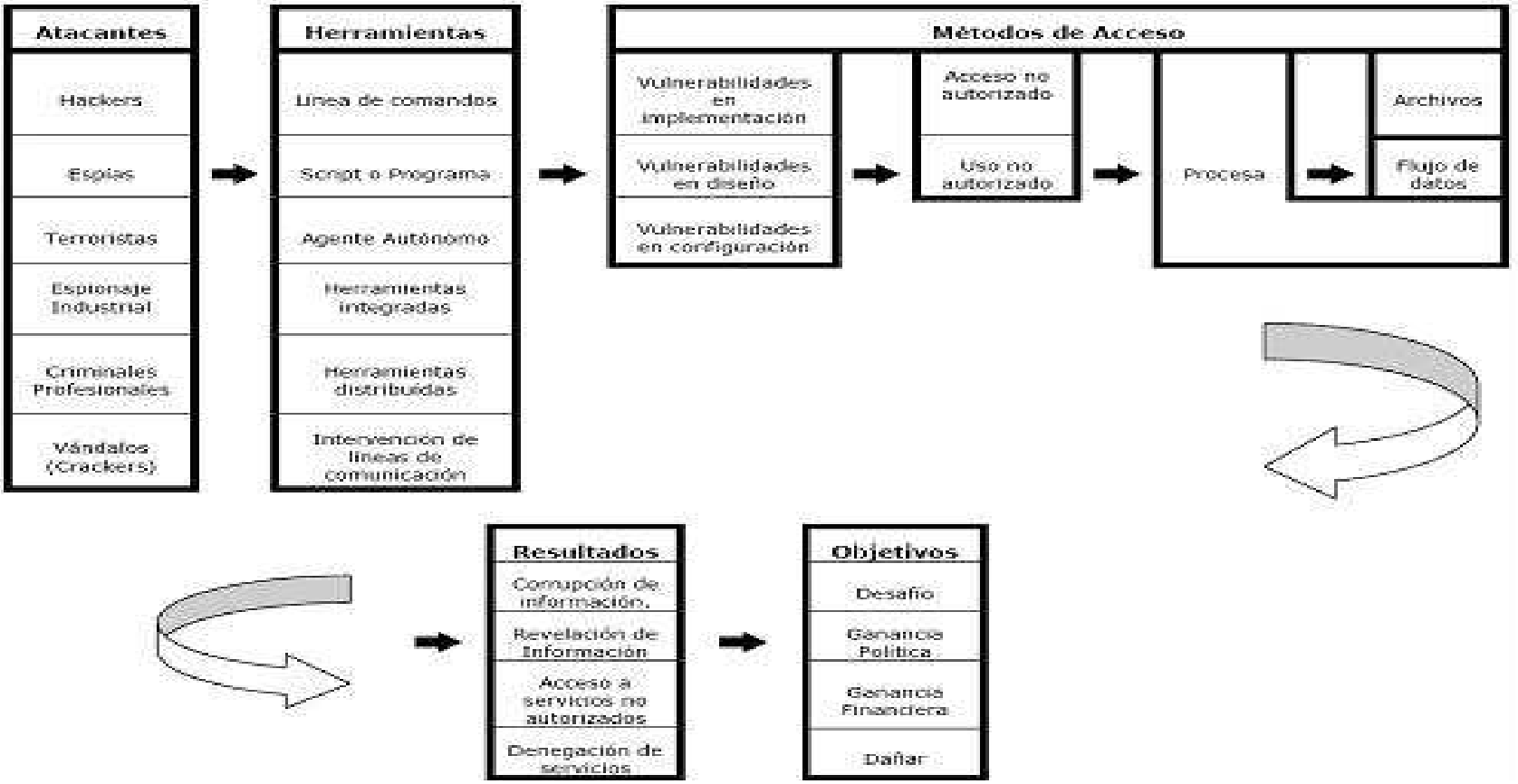


Figura II.6 Diagrama de amenazas

2.9.4 TIPOS DE ATAQUE

A continuación se expondrán diferentes tipos de ataques perpetrados, principalmente, por Hackers. Estos ataques pueden ser realizados sobre cualquier tipo de red, sistema operativo, usando diferentes protocolos, etc.

En los primeros tiempos, los ataques involucraban poca sofisticación técnica. Los Insiders (operadores, programadores, data entrys) utilizaban sus permisos para alterar archivos o registros. Los Outsiders ingresaban a la red simplemente averiguando una password válida. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar “agujeros” en el diseño, configuración y operación de los sistemas.

2.9.4.1 TRASHING (CARTONEO)

Generalmente, un usuario anota su login y password en un papelito y luego, cuando lo recuerda, lo arroja a la basura. Este procedimiento por más inocente que parezca es el que puede aprovechar un atacante para hacerse de una llave para entrar el sistema...”nada se destruye, todo se transforma”. El Trashing puede ser físico (como el caso descripto) o lógico, como analizar buffers de impresora y memoria, bloques de discos, etc.

El Trashing físico suele ser común en organizaciones que no disponen de alta confidencialidad, como colegios y universidades.

2.9.4.2 ATAQUES DE MONITORIZACIÓN

Este tipo de ataque se realiza para observar a la víctima y su sistema, con el objetivo de obtener información, establecer sus vulnerabilidades y posibles formas de acceso futuro.

2.9.4.2.1 SHOULDER SURFING

Consiste en espiar físicamente a los usuarios para obtener el login y su password correspondiente. El Surfing explota el error de los usuarios de dejar su login y password anotadas cerca de la computadora (generalmente en post–it adheridos al monitor o teclado). Cualquier intruso puede pasar por ahí, verlos y memorizarlos para su posterior

uso. Otra técnica relacionada al surfing es aquella mediante la cual se ve, por encima del hombro, al usuario cuando teclea su nombre y password.

2.9.4.2.2 DECOY (SEÑUELOS)

Los Decoy son programas diseñados con la misma interfase que otro original. En ellos se imita la solicitud de un logeo y el usuario desprevenido lo hace. Luego, el programa guardará esta información y dejará paso a las actividades normales del sistema. La información recopilada será utilizada por el atacante para futuras “visitas”.

Una técnica semejante es aquella que, mediante un programa se guardan todas las teclas presionadas durante una sesión. Luego solo hará falta estudiar el archivo generado para conocer nombres de usuarios y claves.

2.9.4.2.3 SCANNING (BUSQUEDA)

El Escaneo, como método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo. La idea es recorrer (scanear) tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular. Muchas utilidades de auditoría también se basan en este paradigma.

Para el escaneo de puertos se lo puede realizar por los siguientes métodos que se describen a continuación.

A) TCP CONNECT SCANNING

Esta es la forma básica del scaneo de puertos TCP. Si el puerto está escuchando, devolverá una respuesta de éxito; cualquier otro caso significará que el puerto no está abierto o que no se puede establecer conexión con él.

Las ventajas que caracterizan esta técnica es que no necesita de privilegios especiales y su gran velocidad.

Su principal desventaja es que este método es fácilmente detectable por el administrador del sistema. Se verá un gran número de conexiones y mensajes de error para

los servicios en los que se ha conseguido conectar la máquina, que lanza el scanner, y también se verá su inmediata desconexión.

B) TCP SYN SCANNING

Cuando dos procesos establecen una comunicación usan el modelo Cliente/Servidor para establecerla. La aplicación del Servidor "escucha" todo lo que ingresa por los puertos.

La identificación del Servidor se efectúa a través de la dirección IP del sistema en el que se ejecuta y del número de puerto del que depende para la conexión. El Cliente establece la conexión con el Servidor a través del puerto disponible para luego intercambiar datos como se muestra en la Figura II.7.

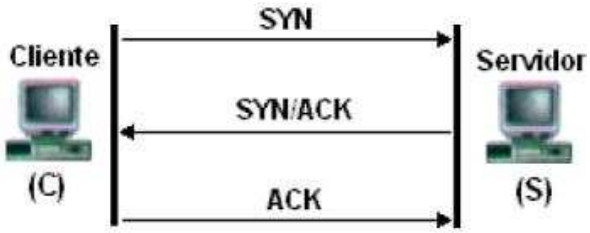


Figura II.7 SYS SCANNING

1. El programa Cliente (C) pide conexión al Servidor (S) enviándole un segmento SYN. Este segmento le dice a S que C desea establecer una conexión.
2. (si está abierto y escuchando) al recibir este segmento SYN (activa el indicador) y envía una autentificación ACK de manera de acuse de recibo a C. Si S está cerrado envía un indicador RST.
3. C entonces ACKea (autentifica) a S. Ahora ya puede tener lugar la transferencia de datos.

C) TCPFIN SCANNING–STEALTH PORT SCANNING

Hay veces en que incluso el scaneo SYN no es lo suficientemente "clandestino" o limpio. Algunos sistemas (Firewalls y filtros de paquetes) monitorizan la red en busca de paquetes SYN a puertos restringidos.

Para subsanar este inconveniente los paquetes FIN, en cambio, podrían ser capaces de pasar sin ser advertidos. Este tipo de scaneo está basado en la idea de que los puertos

cerrados tienden a responder a los paquetes FIN con el RST correspondiente. Los puertos abiertos, en cambio, suelen ignorar el paquete en cuestión.

Este es un comportamiento correcto del protocolo TCP, aunque algunos sistemas, entre los que se hallan los de Microsoft, no cumplen con este requerimiento, enviando paquetes RST siempre, independientemente de si el puerto está abierto o cerrado. Como resultado, no son vulnerables a este tipo de scaneo. Sin embargo, es posible realizarlo en otros sistemas Unix.

"Muchos de los problemas globales de vulnerabilidades son inherentes al diseño original de algunos protocolos". [9]

D) FRAGMENTATION SCANNING

Esta no es una nueva técnica de scaneo como tal, sino una modificación de las anteriores. En lugar de enviar paquetes completos de sondeo, los mismos se particionan en un par de pequeños fragmentos IP. Así, se logra partir una cabecera IP en distintos paquetes para hacerlo más difícil de monitorizar por los filtros que pudieran estar ejecutándose en la máquina objetivo.

Sin embargo, algunas implementaciones de estas técnicas tienen problemas con la gestión de este tipo de paquetes tan pequeños, causando una caída de rendimiento en el sistema del intruso o en el de la víctima. Problemas de esta índole convierte en detectables a este tipo de ataque.

2.9.4.3 EAVESDROPPING –PACKET SNIFFING

Muchas redes son vulnerables al Eavesdropping, o a la pasiva intercepción (sin modificación) del tráfico de red.

Esto se realiza con Packet Sniffers, los cuales son programas que monitorean los paquetes que circulan por la red. Los Sniffers pueden ser colocados tanto en una estación de trabajo conectada a la red, como a un equipo Router o a un Gateway de Internet, y esto puede ser

[9] GONCALVES, Marcus. Firewalls Complete. Beta Book. McGraw Hill. EE.UU. Página 25

realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

Cada máquina conectada a la red (mediante una placa con una dirección única) verifica la dirección destino de los paquetes TCP. Si estas direcciones son iguales asume que el paquete enviado es para ella, caso contrario libera el paquete para que otras placas lo analicen. Un Sniffers consiste en colocar a la placa de red en un modo llamado promiscuo, el cual desactiva el filtro de verificación de direcciones y por lo tanto todos los paquetes enviados a la red llegan a esta placa (computadora donde está instalado el Sniffer).

2.9.4.4 SNOOPING –DOWNLOADING

Los ataques de esta categoría tienen el mismo objetivo que el Sniffing: obtener la información sin modificarla.

Sin embargo los métodos son diferentes. Aquí, además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de correo electrónico y otra información guardada, realizando en la mayoría de los casos un downloading (copia de documentos) de esa información a su propia computadora, para luego hacer un análisis exhaustivo de la misma.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos más resonantes de este tipo de ataques fueron: el robo de un archivo con más de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

2.9.5 ATAQUES DE AUTENTIFICACIÓN

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

2.9.5.1 SPOOFING –LOOPING

Spoofing puede traducirse como “hacerse pasar por otro” y el objetivo de esta técnica, justamente, es actuar en nombre de otros usuarios, usualmente para realizar tareas de Snooping o Tampering (ver a continuación Ataques de Modificación y Daño).

Una forma común de Spoofing es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y así sucesivamente. Este proceso, llamado Looping, tiene la finalidad de “evaporar” la identificación y la ubicación del atacante.
El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país.

2.9.5.2 SPOOFING

Este tipo de ataques (sobre protolocos) suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Los ataques tipo Spoofing bastante conocidos son el IP Spoofing, el DNS Spoofing y el Web Spoofing

2.9.5.2.1 IP SPOOFING

Con el IP Spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete. Su utilización más común es enviar los paquetes con la dirección de un tercero, de forma que la víctima “ve” un ataque proveniente de esa tercera red, y no la dirección real del intruso. El esquema con dos puentes como se muestra en la Figura II.8 es el siguiente:

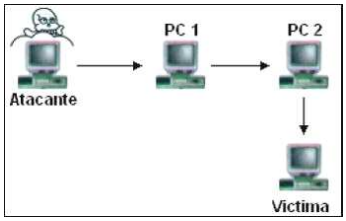


Figura II.8 Spoofing

Nótese que si la Victima descubre el ataque verá a la PC_2 como su atacante y no el verdadero origen. Este ataque se hizo famoso al usarlo Kevin Mitnick (ver Anexo I).

2.9.5.2.2 DNS SPOOFING

Este ataque se consigue mediante la manipulación de paquetes UDP pudiéndose comprometer el servidor de nombres de dominios (Domain Name Server–DNS) de Windows NT©. Si se permite el método de recursión en la resolución de "Nombre↔Dirección IP" en el DNS, es posible controlar algunos aspectos del DNS remoto. La recursión consiste en la capacidad de un servidor de nombres para resolver una petición de dirección IP a partir de un nombre que no figura en su base de datos. Este es el método de funcionamiento por defecto.

2.9.5.2.3 WEB SPOOFING

En el caso Web Spoofing el atacante crea un sitio web completo (falso) similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante, permitiéndole monitorear todas las acciones de la víctima, desde sus datos hasta las passwords, números de tarjeta de créditos, etc.
El atacante también es libre de modificar cualquier dato que se esté transmitiendo entre el servidor original y la víctima o viceversa.

2.9.5.3 IPSPLICING –HIJACKING

Se produce cuando un atacante consigue interceptar una sesión ya establecida. El atacante espera a que la victima se identifique ante el sistema y tras ello le suplanta como usuario autorizado. Ver Anexo 2.

2.9.5.4 UTILIZACIÓN DE BACKDOORS

"Las puertas traseras son trozos de código en un programa que permiten a quien las conoce saltarse los métodos usuales de autentificación para realizar ciertas tareas. Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo". Esta situación se convierte en una falla de

seguridad si se mantiene, involuntaria o intencionalmente, una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control normales.

2.9.5.5 UTILIZACIÓN DE EXPLOITS

Es muy frecuente ingresar a un sistema explotando agujeros en los algoritmos de encriptación utilizados, en la administración de las claves por parte la empresa, o simplemente encontrando un error en los programas utilizados.
Los programas para explotar estos "agujeros" reciben el nombre de Exploits y lo que realizan es aprovechar la debilidad, fallo o error hallado en el sistema (hardware o software) para ingresar al mismo. Nuevos Exploits (explotando nuevos errores en los sistemas) se publican cada día por lo que mantenerse informado de los mismos y de las herramientas para combatirlos es de vital importancia.

2.9.5.6 OBTENCIÓN DE PASSWORDS

Este método comprende la obtención por "Fuerza Bruta" de aquellas claves que permiten ingresar a los sistemas, aplicaciones, cuentas, etc. atacados.
Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario y, además, esta nunca (o rara vez) se cambia. En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la password correcta.

2.9.6 DENIAL OF SERVICE (DOS)

Los protocolos existentes actualmente fueron diseñados para ser empleados en una comunidad abierta y con una relación de confianza mutua. La realidad indica que es más fácil desorganizar el funcionamiento de un sistema que acceder al mismo; así los ataques de Negación de Servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.

Más allá del simple hecho de bloquear los servicios del cliente, existen algunas razones importantes por las cuales este tipo de ataques pueden ser útiles a un atacante:

1. Se ha instalado un troyano y se necesita que la víctima reinicie la máquina para que surta efecto.
2. Se necesita cubrir inmediatamente sus acciones o un uso abusivo de CPU. Para ello provoca un “crash” del sistema, generando así la sensación de que ha sido algo pasajero y raro.
3. El intruso cree que actúa bien al dejar fuera de servicio algún sitio web que le disgusta. Este accionar es común en sitios pornográficos, religiosos o de abuso de menores.
4. El administrador del sistema quiere comprobar que sus instalaciones no son vulnerables a este tipo de ataques.
5. El administrador del sistema tiene un proceso que no puede “matar” en su servidor y, debido a este, no puede acceder al sistema. Para ello, lanza contra sí mismo un ataque DOS deteniendo los servicios.

2.9.6.1 JAMMINGO FLOODING

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más pueda utilizarla.

Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP usando Spoofing y Looping. El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Muchos Hosts de Internet han sido dados de baja por el “ping de la muerte” (una versión-trampa del comando ping). Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte

causa el bloqueo instantáneo del equipo. Esta vulnerabilidad ha sido ampliamente utilizada en el pasado pero, aún hoy pueden encontrarse sistemas vulnerables.

2.9.6.2 SYN FLOOD

Como ya se explicó en el TCP SYN Scanning el protocolo TCP se basa en una conexión en tres pasos. Pero, si el paso final no llega a establecerse, la conexión permanece en un estado denominado “semiabierto”.

El SYN Flood es el más famoso de los ataques del tipo Denial of Service, publicado por primera vez en la revista under Phrack; y se basa en un “saludo” incompleto entre los dos hosts. El Cliente envía un paquete SYN pero no responde al paquete ACK ocasionando que la pila TCP/IP espere cierta cantidad de tiempo a que el Host hostil responda antes de cerrar la conexión. Si se crean muchas peticiones incompletas de conexión (no se responde a ninguna), el Servidor estará inactivo mucho tiempo esperando respuesta. Esto ocasiona la lentitud en los demás servicios.

SYN Flood aprovecha la mala implementación del protocolo TCP, funcionando de la siguiente manera:

Se envía al destino, una serie de paquetes TCP con el bit SYN activado, (petición de conexión) desde una dirección IP Spoofeada. Esta última debe ser inexistente para que el destino no pueda completar el saludo con el cliente.

2.9.6.3 CONNECTION FLOOD

La mayoría de las empresas que brindan servicios de Internet (ISP) tienen un límite máximo en el número de conexiones simultáneas. Una vez que se alcanza ese límite, no se admitirán conexiones nuevas. Así, por ejemplo, un servidor Web puede tener, por ejemplo, capacidad para atender a mil usuarios simultáneos. Si un atacante establece mil conexiones y no realiza ninguna petición sobre ellas, monopolizará la capacidad del servidor. Las conexiones van caducando por inactividad poco a poco, pero el atacante sólo necesita intentar nuevas conexiones, (como ocurre con el caso del SYN Flood) para mantener fuera de servicio el servidor.

2.9.6.4 NET FLOOD

En estos casos, la red víctima no puede hacer nada. Aunque filtre el tráfico en sus sistemas, sus líneas estarán saturadas con tráfico malicioso, incapacitándolas para cursar tráfico útil.

Un ejemplo habitual es el de un teléfono: si alguien quiere molestar, sólo tiene que llamar, de forma continua. Si se descuelga el teléfono (para que deje de molestar), tampoco se puede recibir llamadas de otras personas. Este problema es habitual, por ejemplo, cuando alguien intenta mandar un fax empleando el número de voz: el fax insiste durante horas, sin que el usuario llamado pueda hacer nada al respecto.

En el caso de Net Flooding ocurre algo similar. El atacante envía tantos paquetes de solicitud de conexión que las conexiones auténticas simplemente no pueden competir.

2.9.6.5 LAND ATTACK

Este ataque consiste en un Bug (error) en la implementación de la pila TCP/IP de las plataformas Windows. El ataque consiste en mandar a algún puerto abierto de un servidor (generalmente al NetBIOS 113 o 139) un paquete, maliciosamente construido, con la dirección y puerto origen igual que la dirección y puerto destino.

Por ejemplo se envían un mensaje desde la dirección 10.0.0.1:139 hacia ella misma. El resultado obtenido es que luego de cierta cantidad de mensajes enviados–recibidos la máquina termina colgándose.

Existen ciertas variantes a este método consistente, por ejemplo, en enviar el mensaje a una dirección específica sin especificar el puerto.

2.9.6.6 SMURFO BROADCAST STORM

Este ataque es bastante simple y a su vez devastador. Consiste en recolectar una serie de direcciones BroadCast para, a continuación, mandar una petición ICMP (simulando un

Ping) a cada una de ellas en serie, varias veces, falsificando la dirección IP de origen (máquina víctima). Para mayor detalle revisar el Anexo 2.

2.9.6.7 OBSUPERNUKE O WINNUKE

Un ataque característico, y quizás el más común, de los equipos con Windows© es el Nuke, que hace que los equipos que escuchan por el puerto NetBIOS sobre TCP/UDP 137 a 139, queden fuera de servicio, o disminuyan su rendimiento al enviarle paquetes UDP manipulados.
Generalmente se envían fragmentos de paquetes Out Of Band, que la máquina víctima detecta como inválidos pasando a un estado inestable. OOB es el término normal, pero realmente consiste en configurar el bit Urgente (URG) en los indicadores del encabezamiento TCP, lo que significa que este bit es válido.

Este ataque puede prevenirse instalando los parches adecuados suministrado por el fabricante del sistema operativo afectado. Un filtro efectivo debería garantizar la detección de una inundación de bits Urgentes.

2.9.6.8 TEARDROP I Y II–NEWTEAR –BONK -BOINK

Al igual que el Supernuke, los ataques Teardrop I y Teardrop II afectan a fragmentos de paquetes. Algunas implementaciones de colas Ip no vuelven a armar correctamente los fragmentos que se superponen, haciendo que el sistema se cuelgue. Windows NT© 4.0 de Microsoft® es especialmente vulnerable a este ataque. Aunque existen Patchs (parches) que pueden aplicarse para solucionar el problema, muchas organizaciones no lo hacen, y las consecuencias pueden ser devastadoras. Los ataques tipo Teardrop son especialmente peligrosos ya que existen multitud de implementaciones (algunas de ellas forman paquetes), que explotan esta debilidad. Las más conocidas son aquellas con el nombre Newtear, Bonk y Boink.

2.9.6.9 E–MAIL BOMBING–SPAMMING

El e-mail Bombing consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando así el mailbox del destinatario. El Spamming, en cambio se refiere a

enviar un e–mail a miles de usuarios, hayan estos solicitados el mensaje o no. Es muy utilizado por las empresas para publicitar sus productos. El Spamming está siendo actualmente tratado por las leyes europeas (principalmente España) como una violación de los derechos de privacidad del usuario.

2.9.7 ATAQUES DE MODIFICACIÓN –DAÑO

2.9.7.1 ATAQUES MEDIANTE JAVA APPLETS

Java es un lenguaje de programación interpretado, desarrollado inicialmente por la empresa SUN. Su mayor popularidad la merece por su alto grado de seguridad. Los más usados navegadores actuales, implementan Máquinas Virtuales Java (MVJ) para ser capaces de ejecutar programas (Applets) de Java.

2.9.7.2 ATAQUES CON JAVA SCRIPT Y VBSCRIPT

JavaScript (de la empresa Netscape) y VBScript (de Microsoft) son dos lenguajes usados por los diseñadores de sitios Web para evitar el uso de Java. Los programas realizados son interpretados por el navegador. Aunque los fallos son mucho más numerosos en versiones antiguas de JavaScript, actualmente se utilizan para explotar vulnerabilidades específicas de navegadores y servidores de correo ya que no se realiza ninguna evaluación sobre si el código.

2.9.7.3 ATAQUES MEDIANTE ACTIVE X

ActiveX es una de las tecnologías más potentes que ha desarrollado Microsoft. Mediante ActiveX es posible reutilizar código, descargar código totalmente funcional de un sitio remoto, etc. Esta tecnología es considerada la respuesta de Microsoft a Java. ActiveX soluciona los problemas de seguridad mediante certificados y firmas digitales. Una Autoridad Certificadora (AC) expende un certificado que acompaña a los controles activos y a una firma digital del programador.

2.9.7.4 VULNERABILIDADES EN LOS NAVEGADORES

Generalmente los navegadores no fallan por fallos intrínsecos, sino que fallan las tecnologías que implementan, aunque en este punto analizaremos realmente fallos intrínsecos de los navegadores, como pueden ser los “Buffer Overflow”49.

Los “Buffer Overflows” consisten en explotar una debilidad relacionada con los buffers que la aplicación usa para almacenar las entradas de usuario. Por ejemplo, cuando el usuario escribe una dirección en formato URL ésta se guarda en un buffer para luego procesarla.Si no se realizan las oportunas operaciones de comprobación, un usuario podría manipular estas direcciones.

2.9.8 ERRORES DE DISEÑO IMPLEMENTACIÓN Y OPERACIÓN

Muchos sistemas están expuestos a “agujeros” de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de “puertas invisibles” son descubiertas cada día en sistemas operativos, aplicaciones de software, protocolos de red, browsers de Internet, correo electrónico y todas clase de servicios informáticos disponibles.

Los Sistemas operativos abiertos (como Unix y Linux) tienen agujeros mas conocidos y controlados que aquellos que existen en sistemas operativos cerrados (como Windows). La importancia y ventaja del código abierto radica en miles de usuarios analizan dicho código en busca de posibles bugs y ayudan a obtener soluciones en forma inmediata.

Constantemente se encuentran en Internet avisos de nuevos descubrimientos de problemas de seguridad, herramientas de Hacking y Exploits que los explotan, por lo que hoy también se hace indispensable contar con productos que conocen esas debilidades, puedan diagnosticarlas y actualizar el programa afectado con el parche adecuado.

CAPITULO III

ANALIZAR LA VULNERABILIDAD, LIMITACIONES DEL ENTORNO INFORMATICO Y SUS DIFERENTES NIVELES DE SEGURIDAD DE PETROPRODUCCION

3.1 PETROPRODUCCIÓN

PETROPRODUCCIÓN es la Empresa Estatal de exploración y producción de Petróleos del Ecuador, filial de PETROECUADOR, fue creada el 26 de septiembre de 1989 con el objetivo de explorar, explotar las cuencas sedimentarias o yacimientos hidrocarburíferos, operar los campos hidrocarburíferos asignados a PETROECUADOR y transportar el petróleo y gas hasta los principales centros de almacenamiento.

3.1.1 MISIÓN

Realizar la exploración y explotación de hidrocarburos de manera sustentable, en armonía con los recursos socio-ambientales, para contribuir al desarrollo económico y al progreso social del Ecuador.

3.1.2 VISIÓN

Mantener y proyectar su liderazgo en el país con talento humano competitivo, motivado y comprometido que cumpla estándares internacionales de gestión y se apoye en la tecnología de punta y en los recursos provenientes de la comercialización de hidrocarburos.

3.1.3 OBJETIVOS

- Perforar pozos exploratorios en los prospectos detectados por sísmica.
- Incrementar el volumen de reservas recuperables de crudo del país, en las áreas que se encuentren bajo la responsabilidad directa de la Empresa.
- Mantener e incrementar los volúmenes de producción de petróleo, mediante la perforación de nuevos pozos de desarrollo en los campos de explotación.
- Desarrollar las actividades de la Empresa, con estricto respeto a la ecología y velar por la protección y prevención ambiental, cumpliendo con la ley Ambiental Nacional y normas internacionales.
- Optimizar los recursos que dispone la Empresa y la estandarización de equipos.

3.1.4 ESTRATEGIAS

- Licitar, adjudicar y suscribir nuevos contratos de operación, buscando la mayor rentabilidad del país, para continuar con la exploración y explotación de hidrocarburos mediante la utilización de recursos propios o a través de modalidades permitidas por la Ley.
- Explorar nuevas áreas a fin de determinar trampas estructurales y estratigráficas con posibilidad de contener hidrocarburos.
- Recuperación mejorada y simulación matemática para compensar la declinación natural de los campos en producción.

- Reposicionar la imagen institucional mediante la certificación de procesos y procedimientos con normas internacionales.
- Optimizar y fortalecer el empleo de los recursos: humanos, económicos, tecnológicos y materiales, de forma que permitan elevar los niveles de eficiencia y eficacia de la Empresa, a través de la implementación de mecanismos de evaluación de gestión[10].

3.2 INFRAESTRUCTURA

PETROPRODUCCIÓN realiza la exploración y explotación de los recursos hidrocarburíferos en la región Amazónica del Ecuador; en campos ubicados en Lago Agrio, Sacha, Coca, Auca, Cuyabeno, Guarumo, etc. denominado a este sector como el Distrito Amazónico. Para la gestión y operación administrativa, PETROPRODUCCIÓN dispone de dos Edificios ubicados en la ciudad de Quito; en el sector del Valle de los Chillos específicamente en San Rafael se sitúa el Laboratorio de Geología y Yacimientos; por último, en la ciudad de Guayaquil está localizado el Centro de Investigaciones Geológicas.

Una de las funciones más críticas que posee PETROPRODUCCIÓN es la de brindar comunicaciones eficientes de voz y datos entre los empleados de la empresa que se encuentran ubicados en las diferentes dependencias. PETROPRODUCCIÓN cuenta con una gran infraestructura de comunicaciones de la cual la Unidad de Telecomunicaciones se encarga de la red de microondas y telefónica, mientras que la Unidad de Sistemas se encarga de las aplicaciones y la red de datos.

3.2.1 INFORMACIÓN DEL SITIO

En la ciudad de Quito se encuentran las dependencias administrativas principales de la empresa aquí se concentra la mayor parte de la información que es distribuida hacia todas las dependencias del país. En el Edificio Villafuerte ubicado en la Av. 6 de Diciembre N34-290 y Gaspar Cañero, se encuentran los Departamentos Administrativos, la Unidad de Sistemas y la Unidad de Telecomunicaciones como se muestra en la Figura III.1.

[10] http://www.petroproduccion.com.ec

Figura III.1 Edificio Villafuerte

En el Edificio La Tribuna ubicado en la Av. De Los Shirys N34-382 y Portugal, se encuentran los Departamentos de Operación e Investigación, adicionalmente en este edificio se sitúa la Vicepresidencia de PETROPRODUCCIÓN como se muestra en la Figura III.2.

Figura III.2 Edificio La Tribuna

En la Tabla III.1 se presenta la ubicación geográfica en latitud y longitud del Edificio Villafuerte y el Edificio La Tribuna.

Edificio	Latitud	Longitud	Elevación
VILLAFUERTE	00º 10’ 58.90’’ S	78º 28’ 42.95’’ W	2781 m.
LA TRIBUNA	00º 10’ 56.55’’ S	78º 28’ 54.29’’ W	2775 m.

Tabla III.1 Ubicación Geográfica del Ed. VILLAFUERTE y Ed. LA TRIBUNA.[11]

[11] Fuente Google Earth

La separación entre los 2 edificios en línea recta en de 345 metros aproximadamente. Como se muestra en la Figura III.3

Figura III.3 Separación Geográfica entre los dos Edificios.[12]

3.3 RED DE DATOS DE PETROPRODUCCIÓN

En la ciudad de Quito se encuentra la mayor parte de la infraestructura tecnológica de PETROPRODUCCIÓN, para el Distrito Amazónico la base principal de la infraestructura tecnológica se sitúa en la cuidad de Lago Agrio.

Para la interconexión de las diferentes dependencias, PETROPRODUCCIÓN cuenta con una infraestructura de Red de Área Extendida (Wide Area Network, WAN), la cual utiliza enlaces vía microonda para la transmisión y recepción de voz y datos.

Para la comunicación entre los Edificios Villafuerte y La Tribuna se dispone de un enlace vía microonda desde el Edificio Villafuerte al Cerro del Pichincha y desde el Cerro del Pichincha hacia el Edificio La Tribuna, de esta forma se tiene 8 canales de 64 Kbps para datos (un total de 512 Kbps) y 22 canales de 64 Kbps para voz (un total de 1408 Kbps).

Las comunicaciones desde Quito hacia el Distrito Amazónico se realizan a través de un backbone de microondas desde el Cerro del Pichincha hacia la torre principal de transmisión y recepción en la cuidad de Lago Agrio, este enlace utiliza 8 canales de 64 Kbps para datos y 22 canales de 64 Kbps para voz.

[12] Fuente Google Earth

El la Figura III.4 y la Figura III.5 se esquematiza los enlaces microondas para datos de PETROPRODUCCIÓN hacia las diferentes dependencias del país.

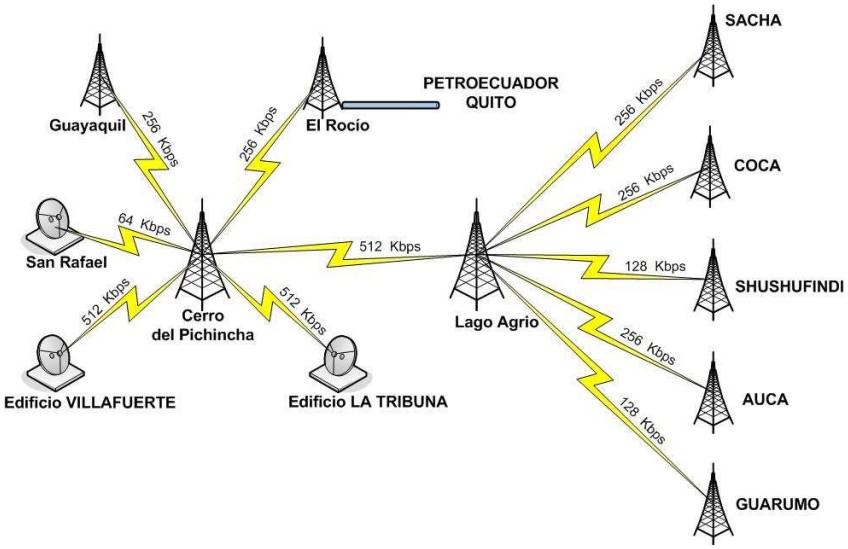


Figura III.4 Enlaces Microonda de PETROPRODUCCIÓN.

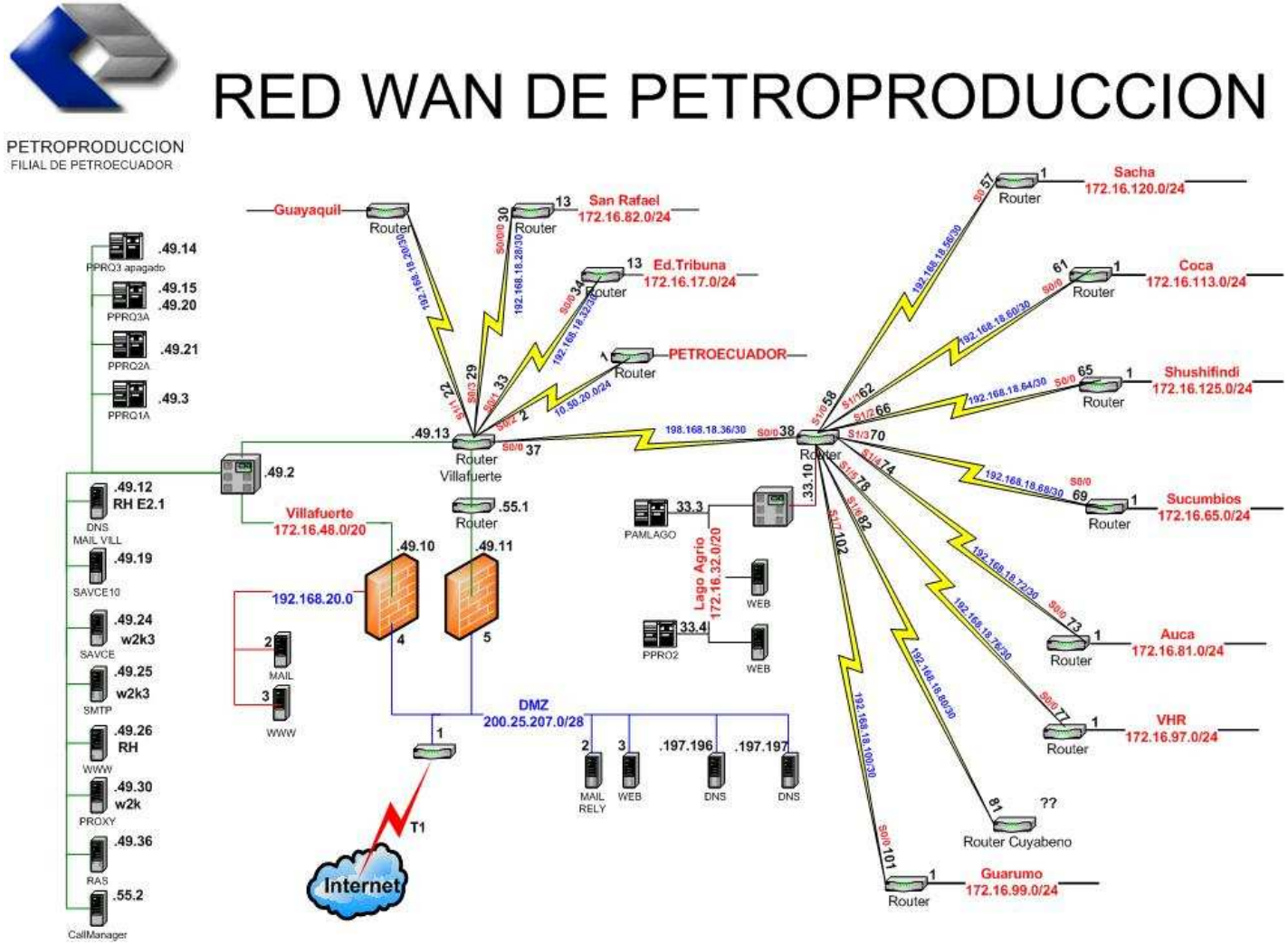


Figura III.5 Red de Datos de PETROPRODUCCION.

3.3.1 RED DE DATOS PARA EL EDIFICIO VILLAFUERTE

El Edificio Villafuerte tiene 1 Subsuelo, Panta Baja, Mezanine y 10 Pisos, la red de datos para este edificio es de tipo red Ethernet en topología tipo bus.

3.3.1.1 RED DE AREA LOCAL

La red de área local para el Edificio Villafuerte es de tipo Ethernet en topología bus con velocidades de transmisión de 10/100 Mbps para los usuarios y 1000 Mbps para los servidores.

Se tienen varias categorías para el cableado estructurado: CAT 5 y CAT5e para la mayoría de los usuarios y CAT6 para el Departamento de Sistemas y el Cuarto de Servidores. El Edificio Villafuerte cuenta con alrededor de 280 puntos de red distribuidos para todo el edificio.

Para la Capa de Core se disponen de dos equipos: un CISCO Catalyst 4507 y un IBM 8274 con velocidades de 10/100/1000 Mbps, de esta forma la capa de distribución cuenta con Switch Cisco Catalyst 2900 de 48 y 24 puertos.

Se tiene un Router 2600 para la comunicación serial V.35 con el equipo de microonda Truepoint 5200, que permite la comunicación con el Edificio Tribuna, Lago Agrio, San Rafael, PETROECUADOR y Guayaquil.

La telefonía IP CISCO CALLMANAGER utiliza un Router 2600 con tarjetas para voz que soportan el protocolo H.323 para la comunicación con la Central Telefónica Meridian 1 de Nortel Opción 61 C, de esta forma los teléfonos IP CISCO IP PHONE 7960[13]y PCs con CISCO IP SoftPhone[14] se comunican con cualquier extensión digital y analógica dentro de la empresa.

La Tabla III.2 muestra los dispositivos de interconectividad para el Edificio Villafuerte.

[13] Teléfono IP que soporta protocolos H.323, MGCP, SCCP, SIP de VoIP. Integra un conmutador Ethernet y tiene 2 puertos Ethernet de 10/100 Base-TX.
[14] Es un software que permite la simulación de un teléfono convencional en un computador.

No Equipos	Tipo de Equipo	Marca	Modelo	Capacidad
1	SWITCH ROUTER	CISCO	Catalyst 4507	10/100/1000 Base-TX X2 MOD
1	SWITCH ROUTER	IBM	IBM 8274	10/100/1000 Base-TX, X4 MOD
6	SWITCH	CISCO	Catalyst 2950	10/100 Base-TX 48x 1000 Base-T 2x
7	SWITCH	CISCO	Catalyst 2950	10/100 Base-TX 24x
4	SWITCH	CISCO	Catalyst 2900 XL	10/100 Base-TX 24x
1	SWITCH	3COM	OfficeConnect	10/100 Base-TX 8x 1000 Base-T 1x
2	ROUTER	CISCO	CISCO 2600	10/100 Base-TX SERIAL port
1	ROUTER	CISCO	CISCO 1700	10/100 Base-TX SERIAL port
2	MODEM G.SHSL	CISCO	CISCO 800	10 Base-T 4x XSDL 1x
2	MODEM ROUTER	TELLABS	TELLABS 8110	SERIAL V.35 1x 10 Base-T 1x
2	FIREWALL	CISCO	CISCO PIX 515E	10/100 Base-TX x6 SERIAL x1
1	BANDWIDTH MANAGEMENT	Net Enforce	AC-202	10/100 Base-TX 3x

Tabla III.2 Equipos de Interconectividad para el Edificio Villafuerte.

Figura III.6 Equipos de interconectividad en el Edificio Villafuerte - Mezanine.

Figura III.7 Equipos de interconectividad en el Edificio Villafuerte - Cuarto de Servidores.

A. FIREWALL

Quizás uno de los elementos más publicitados a la hora de establecer seguridad, sean estos elementos. Aunque deben ser uno de los sistemas a los que más se debe prestar atención, distan mucho de ser la solución final a los problemas de seguridad. Un Firewall es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

Puede consistir en distintos dispositivos, tendientes a los siguientes objetivos:

1. Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él.
2. Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido como se muestra en el Figura III.8

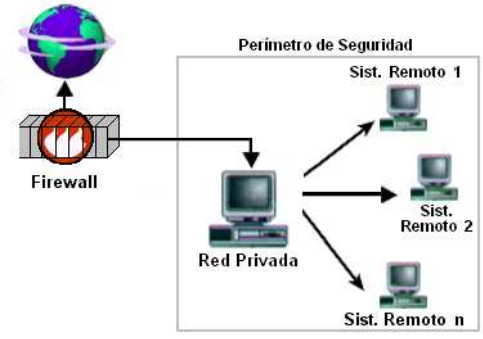


Figura III.8 – Firewall

Como puede observarse, el Muro Cortafuegos, sólo sirven de defensa perimetral de las

redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Algunos Firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red. Se entiende que si dos Firewalls están conectados, ambos deben "hablar" el mismo método de encriptación–desencriptación para entablar la comunicación.

B. ROUTERS Y BRIDGES

Cuando los paquetes de información viajan entre su destino y origen, vía TCP/IP, estos pasan por diferentes Routers (enrutadores a nivel de Red).

Los Routers son dispositivos electrónicos encargados de establecer comunicaciones externas y de convertir los protocolos utilizados en las LAN en protocolos de WAN y viceversa. En cambio, si se conectan dos redes del tipo LAN se utilizan Bridges, los cuales son puentes que operan a nivel de Enlace

La evolución tecnológica les ha permitido transformarse en computadoras muy especializadas capaz de determinar, si el paquete tiene un destino externo y el camino más corto y más descongestionado hacia el Router de la red destino. En caso de que el paquete provenga de afuera, determina el destino en la red interna y lo deriva a la máquina correspondiente o devuelve el paquete a su origen en caso de que él no sea el destinatario del mismo. Los Routers "toman decisiones" en base a un conjunto de datos, regla, filtros y excepciones que le indican que rutas son las más apropiadas para enviar los paquetes.

C. VPN–REDES PRIVADAS VIRTUALES

La tecnología de VPN proporciona un medio para usar el canal público de Internet como un canal apropiado para comunicar los datos privados. Con la tecnología de encriptación y encapsulamiento, una VPN básica, crea un pasillo privado a través de una red insegura. Es decir que la red pública sólo proporciona la infraestructura para enviar los datos.

El objetivo fundamental de una VPN es proteger los datos durante la transmisión a través de la red, permitiendo el uso de redes públicas como si fueran privadas (virtualmente privadas). Esta protección previene el mal uso, modificación, uso no autorizado e interrupciones de acceso a la información mientras atraviesa los distintos segmentos de la red (o redes).

Una VPN no protege la información mientras está alojada en el origen, o cuando llega y se aloja en su destino. También puede dejar expuesto los datos durante alguno de los procesos de encriptación en la red (redes internas antes de la encriptación o redes externas después de la desencriptación). Una VPN solo protege los aspectos de protección en la comunicación, no protege la información alojada en el disco, en pantalla, o impresas.

D. L2TP

Layer To Tunneling Protocol es un protocolo estándares del IETF que ha sido ampliamente implementado. L2TP encapsula las tramas del protocolo punto a punto (PPP Point to Point Protocol) que van a enviarse a través de redes.

Cuando está configurado para utilizar IP como su transporte, L2TP se puede utilizar como protocolo de túnel VPN en Internet. Las tramas PPP encapsuladas se pueden cifrar o comprimir. Cuando los túneles L2TP aparecen como paquetes IP, aprovechan la seguridad IPSec estándar para obtener una fuerte protección de integridad, reproducción, autenticidad y privacidad. L2TP se diseñó específicamente para conexiones Cliente–Servidor de acceso a redes y para conexiones Gateway a Gateway

E. PPTP

Point to Point Tunneling Protocol (antecesor de L2TP) fue diseñado para proporcionar comunicaciones autenticadas y cifradas entre un cliente y un Gateway o entre dos Gateways (sin necesitar una infraestructura de clave pública) utilizando un ID de usuario y una contraseña. Apareció por primera vez en 1996, dos años antes de la disponibilidad de IPSec y L2TP y su objetivo era la simplicidad en su diseño, la compatibilidad multiprotocolo y la capacidad de cruzar una amplia gama de redes IP.

3.3.1.2 SERVIDORES

Existen varios servidores instalados en la intranet de PETROPRODUCCIÓN para satisfacer las necesidades computacionales de los empleados de esta empresa. En el Edificio Villafuerte se encuentran ubicados la mayoría de los servidores e infraestructura tecnológica, sin embargo en el Edificio Tribuna se sitúan servidores generales de correo, DNS y Antivirus.

A. SERVIDORES WEB

PETROPRODUCCIÓN dispone de varios servidores WEB[15], siendo el de mayor importancia el servidor de la página WEB de la Intranet y el servidor de la página WEB Externa.

A través de la página Web de la Intranet los empleados pueden acceder a varias aplicaciones como: El Sistema Integrado de Gestión, Base de Datos Técnica, Indicadores de Gestión e Información Empresarial. Existe un servidor dedicado a la Página WEB externa accesible desde Internet[1].

B. SERVIDOR FTP

PETROPRODUCCIÓN tiene un solo servidor FTP integrado con el servidor WEB de la página de la Intranet. Este servidor se encuentra dedicado para la transferencia de paquetes de programas y no para la documentación empresarial.

C. SERVIDOR MICROSOFT EXCHANGE

PETROPRODUCCIÓN dispone de tres servidores de correo electrónico y un servidor Web-Mail utilizando la plataforma de Microsoft Exchange Server, de esta forma los usuarios pueden acceder al correo electrónico empresarial desde la intranet mediante el Microsoft Office Outlook y desde el Internet mediante el Outlook Web Access (OWA).

[15] Programa que implementa el protocolo HTTP (Hypertext Transfer Protocol) para transferencia de páginas de hipertexto o páginas HTML.

Microsoft Exchange Server es una aplicación de la familia Microsoft Server que proporciona un sistema de mensajería confiable, correo electrónico con protección integrada contra virus y spam[16], calendarios, contactos, tareas compartidas, etc.

Los usuarios pueden tener acceso al correo electrónico, el correo de voz, los calendarios y los contactos desde una amplia variedad de dispositivos electrónicos y desde cualquier ubicación.

D. SERVIDOR MICROSOFT E-LEARNING

PETROPRODUCCIÓN tiene a disposición un servidor de aprendizaje virtual mediante Microsoft E-Learning, permitiendo un aprendizaje integral de Productos Microsoft al incorporar evaluaciones, laboratorios, asesoría especializada de manera flexible.

E. SERVIDOR ACTIVE DIRECTORY Y NOMBRES DE DOMINIO

PETROPRODUCCIÓN dispone de un servidor de Active Directory (AD) integrado con un servidor de Nombres de Dominio (DNS) para el Edificio Villafuerte.

Active Directory es un software que incluye un conjunto de aplicaciones que permiten almacenar y organizar la información sobre los usuarios de la red de computadores y sobre los recursos de red, permitiendo a los administradores gestionar el acceso de usuarios a los recursos de red. Active Directory utiliza distintos protocolos como LDAP, DNS, DHCP, kerberos, etc.

Kerberos es un sistema de seguridad que provee autentificación a través de redes inseguras. Su objetivo es restringir los accesos sólo a usuarios autorizados y poder autentificar los requerimientos a servicios, asumiendo un entorno distribuido abierto, en el cual los usuarios en las estaciones de trabajo acceden a estos servicios a través de una red.

Kerberos fue creado para mitigar este problema de forma tal que el usuario necesita autorización para comunicarse con el servidor (y esta es confiable), se elimina la necesidad

[16] Correo no solicitado o correo basura habitualmente de tipo publicitario, enviados en cantidades masivas.

de demostrar el conocimiento de información privada y de que esta viaje a través de la red.

Kerberos provee un servidor de autenticación centralizado, cuya función es autentificar a los usuarios frente a servidores y a este frente a los usuarios.

Un Servidor KDC (Kerberos Distribution Center) alojado en el AS mantiene una base de datos de sus clientes (usuarios y servicios) y sus respectivas claves simétricas privadas utilizando DES (aunque actualmente se encuentra en desarrollo versiones de Kerberos empleando RSA):

F. SERVIDOR CISCO CALLMANAGER Y DHCP

PETROPRODUCCIÓN cuenta con la versión 3.3 del Cisco CallManager integrado con el servicio de DHCP en un solo servidor. Se disponen de varios teléfonos IP CISCO IP PHONE 7960, además varios usuarios utilizan el CISCO IP SoftPhone para realizar llamadas.

El Cisco CallManager es un producto basado en el Software Cisco IOS que ofrece servicios de procesamiento de llamadas. El Cisco CallManager ofrece un conjunto extenso de servicios de Comunicaciones IP, los cuales generalmente están disponibles en sistemas de telefonía y en los PBXs (Private Branch Exchange), como el tomar llamadas, seguimiento de llamadas, servicio día/noche, grupos de búsqueda, servicios de beepers, comunicaciones internas, etc.

G. SERVIDOR PROXY Y FIREWALL

PETROPRODUCCIÓN dispone de un servidor Proxy[17] integrado con un Symantec Web Security para la protección de ataques externos de Internet sobre la red LAN, WAN y la red DMZ.

Con Symantec Web Security versión 3.0 que es un software especializado de Proxy que permite la filtración de contenido (http, ftp, https) e inspección de paquetes de acuerdo con las políticas de seguridad implementadas en la empresa.

[17] Software y/o Hardware que permite el acceso a Internet a todos los equipos de una organización cuando sólo se dispone de una única dirección IP.

La Figura III.9 muestra cada una de las interfaces de los Firewall

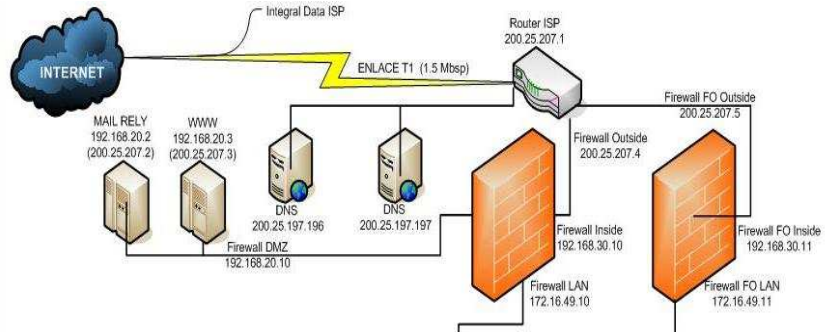


Figura III.9 Interfaces del Proxy-Firewall Astaro Security Gateway.

Para evitar las debilidades asociadas al filtrado de paquetes, los desarrolladores crearon software de aplicación encargados de filtrar las conexiones. Estas aplicaciones son conocidas como Servidores Proxy y la máquina donde se ejecuta recibe el nombre de Gateway de Aplicación o Bastion Host.

El Proxy, instalado sobre el Nodo Bastión, actúa de intermediario entre el cliente y el servidor real de la aplicación, siendo transparente a ambas partes.

Cuando un usuario desea un servicio, lo hace a través del Proxy. Este, realiza el pedido al servidor real devuelve los resultados al cliente. Su función fue la de analizar el tráfico de red en busca de contenido que viole la seguridad de la misma.

H. SERVIDOR SYMANTEC

PETROPRODUCCIÓN dispone de 2 servidores de antivirus: uno en el Edificio Villafuerte y otro en el Edificio Tribuna. Mediante estos servidores se puede dar protección contra amenazas de virus y spyware[18].

Symantec Anti-Virus es un programa antivirus destinado a proteger los servidores, estaciones de trabajo y computadores de archivos y programas maliciosos.

[18] Software que recopila información de un computador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del computador.

I. SERVIDORES AS/400

La base fundamental del manejo de información de PETROPRODUCCIÓN se encuentra ubicada en los servidores AS/400.

PETROPRODUCCIÓN cuenta con varios servidores AS/400 los que permiten el manejo de facturas, memorandos, oficios, roles de pago, información del personal, etc. Se tiene 3 servidores en la ciudad de Quito y 2 en la ciudad de Lago Agrio.

J. CUADRO COMPARATIVO DE SERVIDORES

La Tabla III.3 muestra los servidores para el Edificio Villafuerte, detallando el sistema operativo S.O. y software que implementa el servicio especificado.

Equipo	Marca	Servicio	S.O.	Software
Blade Center HS20 Slot 1	IBM	Correo Electrónico	W2k3s	Microsoft Exchange 2003
Blade Center HS20 Slot 2	IBM	Directorio Activo y Nombres de Dominio	w2k3s	Active Directory y DNS Microsoft
Blade Center JS21 Slot 3	IBM	WEB Interna	RH E4	Apache
Blade Center HS21 Slot 4	IBM	Anti-Virus	w2k3s	Symantec Anti-Virus 6.0
Blade Center HS21 Slot 5	IBM	BizAgi	w2k3s	BizAgi
Blade Center HS21 Slot 6	IBM	SMS	w2k3s	Microsoft Systems Management Server
Blade Center HS21 Slot 7	IBM	FTP	w2k3s	File Server
OpenPower	IBM	DataWareHouse	RH E4	IBM DB2
xSeries 366	IBM	B.O.	w2k3s	Business Objects XI Release 2

xSeries 366	IBM	Resolve IT	w2k3s	Resolve IT ver. E.E CSM build 1.07
Router	DELL	Firewall	Unix	
System x3550	IBM	WEB Externa	RH E4	Apache
System x3550	IBM	WEBMAIL	w2k3s	Outlook Web Access OWA
HP 370	HP	Aprendizaje On-Line	w2k3s	Microsoft E-Learning
MCS 7800 Series	CISCO	VoIP y DHCP	w2ks	Call Manager 3.3 y DHCP Microsoft
xSeries 235	IBM	WEB Interna de RR.HH.	RH E4	Apache
eServer i5	IBM	AS/400	i5	i5 ver 5.7

Tabla III.3 Servidores para el Edificio Villafuerte.

3.3.2 RED DE DATOS PARA EL EDIFICIO LA TRIBUNA

El Edificio La Tribuna tiene 2 Subsuelos, Panta Baja, Mezanine y 14 Pisos, la red de datos para este edificio es de tipo red Ethernet en topología tipo bus.

3.3.2.1 RED DE AREA LOCAL

La red de área local para el Edificio La Tribuna es de tipo Ethernet en topología bus con velocidades de transmisión de 10/100 Mbps para los usuarios y servidores.

Se tienen varias categorías para el cableado estructurado: CAT 5 y CAT5e para la mayoría de los usuarios, CAT6 y Fibra Óptica para el Departamento de Yacimientos y Geofísica. El Edificio La Tribuna cuenta con alrededor de 260 puntos de red distribuidos para todo el edificio.

Se tiene un Router 2600 para la comunicación serial V.35 con el equipo de microonda Urbanet 18Z, que permite la comunicación con el Edificio Villafuerte, desde el cual se realiza la comunicación para las diferentes dependencias del País.

La Tabla III.4 muestra los dispositivos de interconectividad para el Edificio La Tribuna.

No Equipos	Tipo de Equipo	Marca	Modelo	Capacidad
3	SWITCH	CISCO	Catalyst 2950	10/100 Base-TX 48x 1000 Base-T 2x
4	SWITCH	CISCO	Catalyst 2950	10/100 Base-T 24x
2	SWITCH	CISCO	Catalyst 2950	10/100 Base-TX 12x
4	SWITCH	INTEL	Express 460T Stardalone	10/100 Base-T 24x
1	SWITCH	CNET	PowerSwitch	10/100 Base-T 24x
1	ROUTER	CISCO	CISCO 2600	10/100 Base-TX SERIAL port
1	HUB	IBM	Stackable Ethernet 8237	10 Base-T 16x

Tabla III.4 Equipos de ínter conectividad para el Edificio La Tribuna.

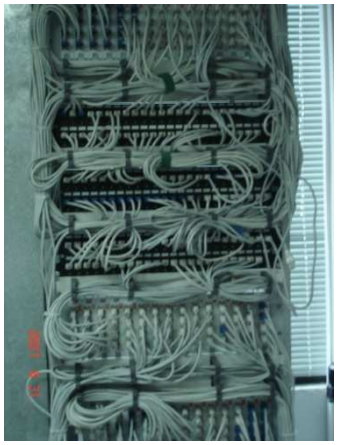


Figura III.10 Equipos de ínter conectividad en el Edificio La Tribuna – Piso 7.

3.3.2.2 SERVIDORES

En este Edificio se encuentran servidores especializados para el monitoreo, administración y control de pozos petroleros, tasa de producción, búsqueda de nuevas cuencas sedimentarias, etc.

Estos servidores especializados son utilizados por el personal del Departamento de Geofísica, Yacimientos y Geología, los servidores se encuentran en redes locales de fibra óptica de alto rendimiento y disponibilidad.

El Edificio La Tribuna cuenta con los siguientes servidores generales:

- Servidor Symantec.
- Servidor de Nombres de Dominio DNS integrado con el Servidor Microsoft Exchange.

3.3.2.2.1 CUADRO COMPARATIVO DE SERVIDORES

La Tabla III.5 muestra los servidores para el Edificio La Tribuna, detallando el sistema operativo S.O. y software que implementa el servicio especificado.

Equipo	Marca	Servicio	S.O.	Software
System x3550	IBM	Correo Electrónico Nombres de Dominio	w2k3s	Microsoft Exchange 2003 y DNS Microsoft
Precision 690	DELL	Anti-Virus	w2k3s	Symantec Anti-Virus 6.0
Precision 690	DELL	SMS	w2k3s	Microsoft Systems Management Server

Tabla III.5 Servidores para el Edificio La Tribuna.

3.4 ANÁLISIS DE TRÁFICO DE RED

Para el análisis de tráfico de datos de PETROPRODUCCIÓN se dispone de Astaro Security Gateway y de Astaro Reporter Manager.

Mediante estas dos herramientas se puede analizar el tráfico de datos para las interfases Interna, Externa y DMZ del Proxy-Firewall Astaro. (ver Figura 2.9)

Además se puede generar reportes de uso del ancho de banda AB (Bandwidth) por red, por día de la semana, por hora, por protocolo, etc.

El número de días procesados es de 186 desde el 5/28/2007 hasta el 12/13/2007, los datos nos dan a conocer que al estar sin la protección de Astaro la infección por virus entrante por navegación y correo electrónico causaría un gran daño sobre equipos de usuarios finales, causando un retraso de actividades y procesos que PPR.

3.4.1 INTERFASE INTERNA

La interfase interna corresponde el enlace con la red de datos de PETROPRODUCCIÓN, es decir todas las redes de área local (LAN) de cada dependencia conectadas mediante la red de área extendida (WAN).

Se tiene un máximo de 4,61 Mbps de tráfico local que atraviesa el Firewall en un día normal de funcionamiento.

3.4.2 INTERFASE EXTERNA.

La interfase externa corresponde la salida hacia Internet. Cabe mencionar que Integral Data proporciona el servicio de Internet con una velocidad de transmisión de 1,987 Mbps mediante un enlace de cobre dedicado.
Se tiene un máximo de 1,54 Mbps de tráfico externo que atraviesa el Firewall en un día normal de funcionamiento. Además existen picos de tráfico para las 09:00 y 14:00 horas.

3.4.3 INTERFASE DMZ

La interfase DMZ (Demilitarized Zone, Zona Desmilitarizada) permite la salida hacia Internet del servidor WEB Externo de la empresa.

3.4.4 ANCHO DE BANDA

El ancho de banda (AB) es un factor crítico para el buen rendimiento de la red de datos, sin embargo muy pocos administradores de red realizan un análisis exhaustivo de qué tipo de

tráfico circula por la red y qué porcentaje de AB consume cada subred, aplicación, protocolo, etc.

3.4.4.1 AB POR PROTOCOLO

La Tabla III.6 muestra los distintos protocolos y su respectivos eventos (Hits) generados.

Protocolo	Hits	% de Hits
http	12018692	26.08
Tcp	18487654	40.12
Udp	5741021	12.46
Dns	5785543	12.55
Icmp	3375979	7.33
https	261398	0.57
telnet	9552	0.02
ftp	87380	0.19
pop3	776	0.00
Smtp	269062	0.58
Total	46037056	99.90

Tabla III.6 Eventos generados por cada protocolo.

La Figura III.11 muestra los principales protocolos usados con su respectivo AB utilizado (bytes transferidos).

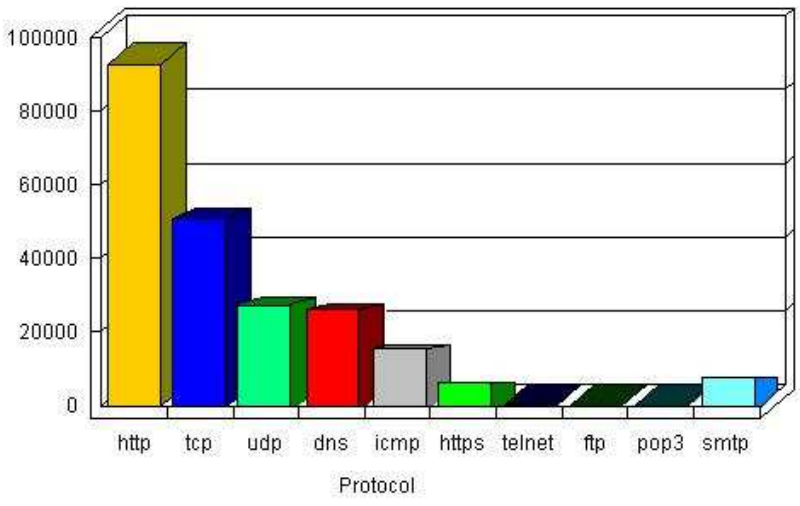


Figura III.11 AB utilizado por cada protocolo.

3.4.4.2 AB POR SUBRED

La Tabla III.7 muestra en detalle cada subred o departamento conjuntamente con el número de eventos y los bytes transferidos.

No	Subred Departamento	Hits	% de Hits	Bytes Transferidos	% de Bytes Transferidos
1	Lago Agrio	5519950	3.32	35.48 GB	11.29
2	Villafuerte	16047167	9.65	11.02 GB	3.51
3	Sacha120	1297716	0.78	10.52 GB	3.35
4	Tribuna17	2309815	1.39	7.79 GB	2.48
5	Auca	584082	0.35	4.79 GB	1.52
6	Shushufindi125	10381634	6.24	3.94 GB	1.25
7	Libertador	1507422	0.91	3.71 GB	1.18
8	Coca	270208	0.16	2.71 GB	0.86
9	VHR	236863	0.14	2.64 GB	0.84
10	Guarumo	382939	0.23	2.20 GB	0.70
	Total	38537796	23.17	84.80 GB	26.98

Tabla III.7 AB y eventos generados por subred.

La Figura III.12 muestra el ancho de banda utilizado por cada subred o dependencia.

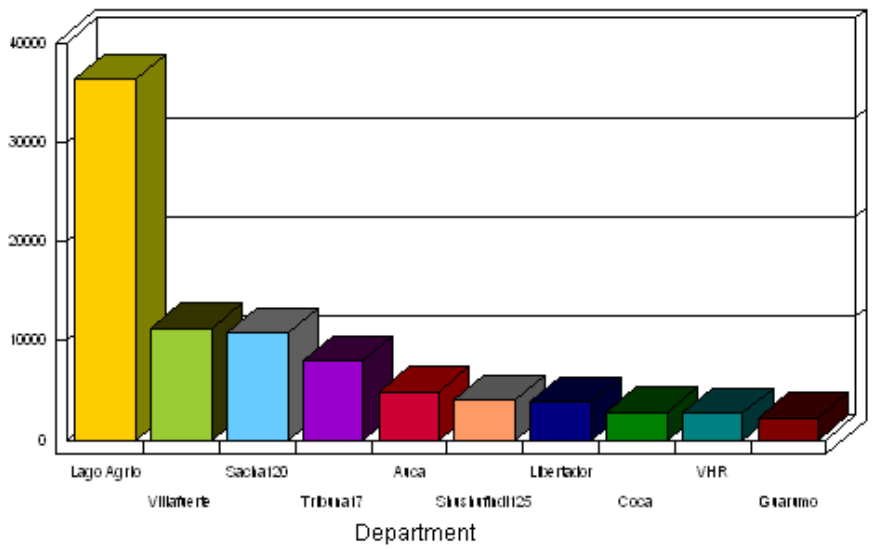


Figura III.12 AB utilizado por subred o departamento.

3.4.4.3 AB POR DIA DE LA SEMANA

La Tabla III.8 muestra en detalle el uso del ancho de banda utilizado por cada día de la semana.

Día	Hits	% de Hits	Bytes Transferidos	% de Bytes Transferidos
Domingo(Sun)	6658497	14.45	13.77 GB	15.20
Lunes (Mon)	9092213	19.73	20.89 GB	23.06
Martes (Tue)	7573995	16.43	18.18 GB	20.07
Miércoles (Wed)	5132579	11.14	11.95 GB	13.19
Jueves(Thu)	4832209	10.49	7.58 GB	8.37
Viernes (Fri)	5191681	11.27	9.23 GB	10.19
Sábado (Sat)	7603572	16.50	8.98 GB	9.91
Total	46084744	100.00	90.58 GB	99.99

Tabla III.8 AB y eventos generados por día de la semana.

La Figura III.13 muestra el ancho de banda utilizado por cada día de la semana.

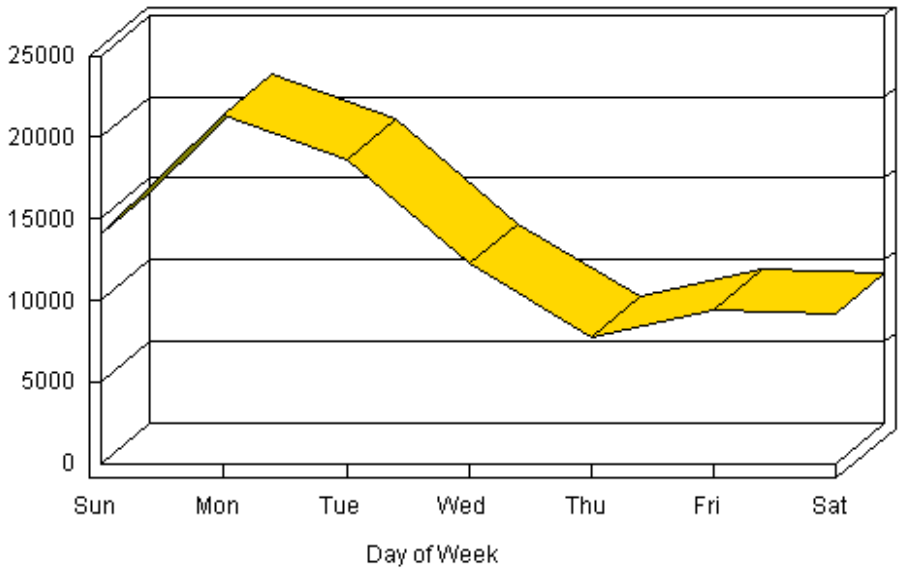


Figura III.13 AB utilizado por día de la semana.

La Figura III.14 muestra los bytes enviados por cada día de la semana.

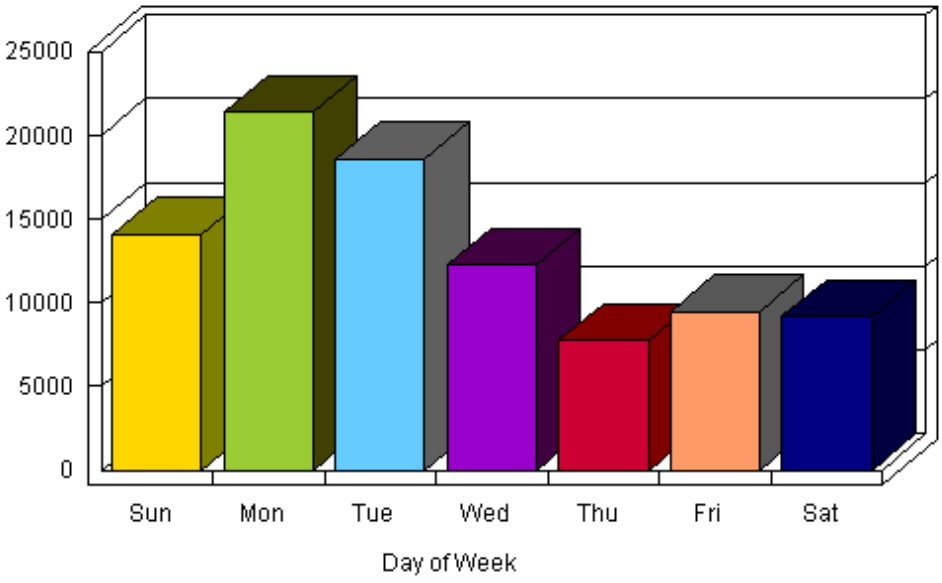


Figura III.14 AB saliente utilizado por día de la semana.

3.4.4.4 AB POR HORA DEL DIA

La Figura III.15 muestra el uso del ancho de banda con respecto a cada hora del día, se tiene un acumulado para todos los días procesados (Historical) y una para un día en particular (Daily).

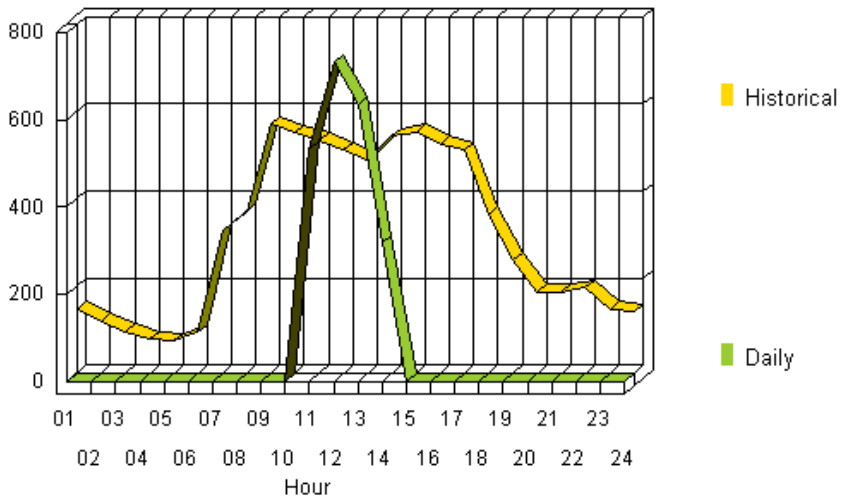


Figura III.15 AB utilizado por hora del día.

3.4.5 ATAQUES Y SEGURIDAD

Es imprescindible que las redes de información manejen criterios y políticas de seguridad de esta forma la confiabilidad, disponibilidad, integridad y autenticación del usuario sea efectiva y eficiente.

Uno de los principales parámetros de control es el número de ataques que soporta la red.

La Figura III.16 muestra el número de ataques bloquedos y filtrados dependiendo de cada hora del día.

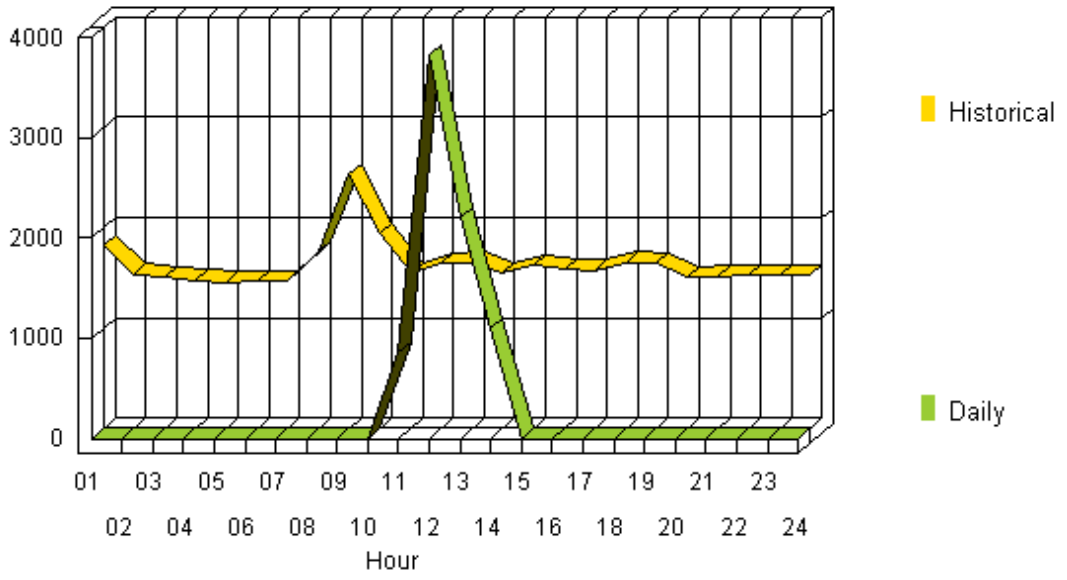


Figura III.16 Número de Ataques por hora del día.

El Firewall permite la categorización de páginas Web sospechosas y maliciosas de tal forma que bloquea al usuario el acceso a este tipo de páginas y genera un reporte del número de eventos (páginas, imágenes, videos, banners, etc.) que han sido bloqueados se muestra en la Tabla III.9.

	Categorías y Bloqueo de Páginas Web	# de Hits	Bytes Transferidos
1	Bloqueadas por Pornografía pornography(0)	53793	32.33 KB
2	Bloqueadas por Relaciones de Amistad (hi5,msn, lycos, etc.)	38699	7.86 KB

	Dating_/_relationships(42)		
3	Bloqueadas por Páginas Personales (blogger, geocities, weblogs, etc.) personal_homepages(49)	37816	2.86 KB
4	Bloqueadas por Erótico/Sexo Erotic_/_sex(1)	23414	13.13 KB
5	Bloqueadas por Chat (Messenger,google chat, latin chat, etc.) chat(28)	15244	3.25 KB
6	Bloqueadas por Spyware (programas espías) malware(60)	14087	6.05 KB
7	Bloqueadas por Proxy Anónimos anonymous_proxies(37)	8678	6.00 KB
8	Bloqueadas por Phishing (correos electrónicos engañosos con finalidad de obtener información) web_mail(27)	7081	0.02 KB
9	Bloqueadas por Juegos de computadoras. computer_games(18)	2789	0.04 KB
10	Bloqueadas por Juegos de lotería. gambling_/_lottery(17)	1842	0.02 KB
	Total	203443	71.56 KB

Tabla III.9 Categorías y Bloqueos de páginas Web.

Finalmente, la Figura III.17 muestra el número de eventos bloqueados dependiendo del filtro de contenido y de la categorización del Proxy-Firewall.

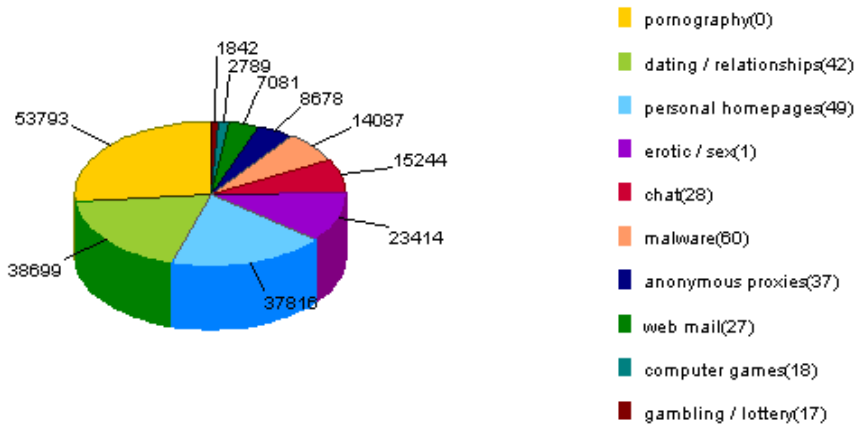


Figura III.17 Porcentaje de bloqueos de páginas Web.

CAPITULO IV

ESTUDIO DE LAS PLATAFORMAS TÍPICAS DE SEGURIDAD EN LOS SERVICIOS DE INTERNET

Para brindar una mejor seguridad se ha adquirido software como Astaro, Systems Management Server y Antivirus Kaspersky las cuales han sido seleccionadas dentro de un gran numero plataformas tanto software como hardware.

Uno de los grandes inconvenientes que se afronta al momento de gestionar la seguridad informática es encontrar las herramientas adecuadas acorde a la infraestructura de la Organización, además de tomar muy en cuenta los costos que representan dichas herramientas, así como también el soporte técnico. Por tal razón, es esencial la necesidad de buscar mecanismos y herramientas que ayuden a mejorar la seguridad del ambiente informático.

4.1 CARACTERÍSTICAS DE LAS PLATAFORMAS DE SEGURIDAD

4.2 CARACTERÍSTICAS DE ASTARO

Todos los dispositivos Astaro Security Gateway cuentan con funcionalidad completa de Gestión Unificada de Amenazas (UTM) y son extremadamente fáciles de utilizar.

Astaro Security Linux es una solución única para la seguridad en las redes, fácil de manejar. Incluye una combinación de las siguientes aplicaciones de seguridad:
Proteje todo tipo de redes – Windows, Linux, Unix y otros.

- Proporciona características comprensivas a bajo coste.
- Alta eficacia. Ha ganado numerosos premios de la industria. Supera a Cisco y Checkpoint en la comparativa de productos de la revista, gana a IBM y Computer Associates en Linux World a la mejor aplicación de seguridad.
- La plataforma integrada de manejo, la interfaz basada en web y las actualizaciones proporciona una rápida implantación y fàcil manejo.
- Puede instalarse en menos de 15 minutos o bien adquirirse en dispositivos pre-instalados.
- Puede iniciarse con firewall, VPN y protección contra spam, así como añadir otras aplicaciones de seguridad si se necesitan.
- Funciona como servidor dedicado encima de un sistema operativo robusto, que elimina quebraderos de los administradores del sistema operativo.
- Puede ser utilizado tanto pequeñas como grandes redes, así como en sistemas multiprocesador con gigabytes de memoria.
- Puede configurarse la alta disponibilidad en caso de fallos del sistema.
- El balanceo de carga le permite asignar prioridades al tráfico por red, por servicio y protocolo.

A) FACILIDAD DE USO

Los dispositivos Astaro Security Gateway se instalan y configuran a través de una interfaz de usuario basada en navegador, configuración por https.
La configuración de Astaro Security Gateway se efectúa a través de una interfaz basada en web. No es necesario ningún software adicional.

- Asistentes de instalación y configuraciones por defecto simplifican el despliegue de información como la configuración.
- Tiene una ayuda sensible al contexto incluye ejemplos para cada función.
- Las opciones y textos de los menús son flexibles de entender para cualquier administrador de red.

Las características de seguridad en Astaro Security Gateway están completamente integradas, de manera que el esfuerzo administrativo se reduce y la protección se incrementa.

Es posible administrar de forma eficiente grandes implantaciones de Astaro Security Gateways desde una localización central mediante Astaro Command Center.

B) WEB SECURITY

Con los dispositivos Astaro Security Gateway PETROPRODUCCION puede administrar y filtrar el acceso a Internet de sus empleados, y hacer cumplir las políticas empresariales de seguridad con el fin de aumentar la productividad general.

Los dispositivos Astaro Security Gateway proporcionan protección en tiempo real para redes de cualquier tamaño mediante:

- Defensa frente a ataques y sondas a nivel perimetral;
- Filtrado del tráfico permitido en busca de riesgos ocultos y amenazas;
- Dotando a los empleados de acceso remoto seguro; y
- Conectando de forma segura las delegaciones.

C) NETWORK SECURITY

Las funcionalidades integradas de firewall, protección de intrusos y VPN permiten una mejor protección perimetral y control de acceso a la red.

Astaro Security Gateway consigue proteger su red empleando múltiples tecnologías integradas, incluyendo:

- Un firewall de alto rendimiento con inspección de paquetes stateful;

- Detección y prevención de intrusos, mediante continuas actualizaciones para detectar y repeler miles de intrusiones diferentes;
- Pasarela de Red Privada Virtual (VPN), soportando una gran variedad de protocolos de conexión y encriptación estándares del mercado; y
- control del ancho de banda, permitiendo la priorización de ciertos canales de tráfico frente a otros.

D) EMAIL SECURITY

Con Astaro Security Gateway los administradores pueden limpiar en tiempo real todos los E-mails de Virus, Spam y Ataques Phising, tanto entrantes, como salientes.

La protección total del email se consigue mediante la integración de varias técnicas:

- Escaneado dual anti-virus cada mensaje ha de pasar a través de dos sofisticados motores anti-virus;
- Ocho técnicas anti-spam en serie con posibilidad de auto-liberación de cuarentena permiten una fácil administración;
- Combinación de filtros URL y patrones de texto para detectar de forma efectiva los ataques de tipo phising
- Proxy de alto rendimiento para el filtrado transparente de múltiples protocolos de correo, tanto entrantes como salientes.

4.2.1 PUNTOS CLAVE ACERCA DE ASTARO SECURITY LINUX

- Proteje todos tipo de redes - Windows, Linux, Unix y cualquier red sobre IP.
- Proporciona características avanzadas a bajo costo maximizando el Retorno de la Inversión (ROI).
- Altamente eficaz. Ha ganado numerosos premios de la industria. Venció a Cisco y Checkpoint en el análisis de productos de InfoWorld, Ha ganado a IBM y Computer Associates en Linux World como mejor aplicación de seguridad.
- La plataforma integrada de administración ofrece una interfaz intuitiva basada en navegador Web y actualizaciones de un solo paso para una instalación rápida y fácil gestión.

- Se puede instalar en menos de 15 minutos o comprarlo previamente instalado en dispositivos de seguridad.
- Puede comenzar con el cortafuego, VPN y la protección contra Spam y agregar posteriormente otras aplicaciones de seguridad según las vaya necesitando, sin problemas.
- Se ejecuta como servidor de aplicaciones dedicado sobre un sistema operativo fortificado, evitando los quebraderos de cabeza asociados con la gestión del sistema operativo.
- Funciona sobre toda clase de sistemas: desde dispositivos pequeños hasta grandes servidores multiprocesador y con múltiples gigabytes de memoria RAM.
- Configure sistemas redundantes para proporcionar alta disponibilidad y failover automático en el caso de fallos hardware o de red.
- Mejore el rendimiento con el balanceo de carga - Establezca prioridades de tráfico según red, servicio y protocolo con la opción de calidad de servicio (QoS).
- Consiga el más alto grado de fiabilidad mediante los históricos, copia de seguridad automatizada y herramientas de diagnóstico integradas.
- Talleres de evaluación online gratuitos para que empiece ya

4.3 COMPATIBILIDAD HARDWARE Y SOFTWARE DE ASTARO

4.3.1 REQUISITOS DE SISTEMA PARA LA INSTALACIÓN DEL SERVIDOR

El propósito de esta lista es darle cierta ayuda e información sobre el hardware para ser usado con Astaro Security Linux.

- Requisitos Mínimos de Hardware:
    - Pentium II o compatible (hasta 100 usuarios LB)
    - Pentium III o compatible (más de 100 usuarios LB)
    - 256 MB RAM
    - 8GB IDE o SCSI de Disco Duro
    - CD ROM IDE
    - 2 o más tarjetas de Red (Interna, Externa, DMZ)
- Software: Revisar compatibilidad de hardware en HCL de Astaro en el **Anexo 3**

4.3.2 LIMITACIONES DE SEGURIDAD EN ASTARO

Las limitaciones de Astaro están dadas por su sistema operativo cerrado puesto que no nos permite realizar modificaciones en cuanto a su interfaz como a encontrar nuevas vulnerabilidades y poder incrementar reglas de seguridad. Por lo cual Astaro está siempre en constante actualización para poder incrementar los nuevos recursos.

4.4. UTILIZACIÓN DE HERRAMIENTAS DE SEGURIDAD DE LICENCIA

4.4.1 UTILIZACIÓN DE ASTARO

Astaro Security Linux es una solución de seguridad de red única en su categoría y presentada en un conjunto integrado y fácil de usar. Se compone de las siguientes aplicaciones de seguridad:

- Firewall con inspección de paquetes “stateful” y proxies de aplicación que protege todo el tráfico de comunicaciones de su empresa, tanto entrante como saliente.
- Pasarela de Red Privada Virtual (VPN): garantiza comunicaciones seguras con oficinas y sedes remotas, usuarios móviles y teletrabajadores.
- Protección Antivirus defiende sus ordenadores de virus, tanto en el correo electrónico, como procedentes de la web.
- Protección de Intrusos detecta y detiene sondas hostiles y ataques basados en aplicaciones.
- Protección contra el Spam, eliminando la pérdida de productividad producida por la apertura y borrado de correos no solicitados.
- Protección de la Navegación (Filtrado de Contenidos): mejora la productividad bloqueando actividades inapropiadas en la red.

4.4.1.1 SEGURIDAD DE LA RED PETROPRODUCCION

El firewall de Astaro**.** Maneja la comunicación que ingresa y sale, así como el tráfico entre redes internas. Los administradores pueden bloquear el acceso para cada protocolo, a cada red de órganos internos, servidor, servicio, y grupo de usuario. El firewall inspecciona ambas información de red (cabeceras de paquetes) e información sobre la aplicación (carga útil) para detectar y bloquear tráfico sospechoso, tal como se muestra en la Figura 3.1.

Figura IV.1 Firewall de Astaro

4.4.1.2 RED PRIVADA VIRTUAL (VPN)

La Pasarela VPN Astaro Security Linux emplea un amplio abanico de métodos de cifrado de datos para crear un "túnel" de comunicaciones seguro sobre la Internet pública, este modulo de Network Security contiene VPN, Intrusión Protection y Firewall como se denota en la Figura IV.2.

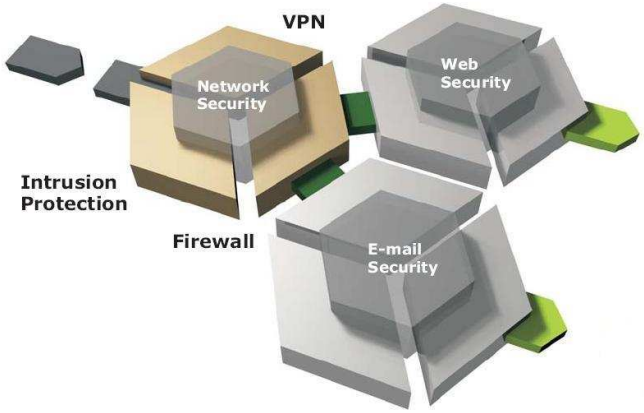


Figura IV.2 Network Security

A. CARACTERÍSITICAS DE LA PASARELA VPN ASTARO SECURITY LINUX VERSION 6.03

La Pasarela VPN Astaro Security Linux soporta una variedad de arquitecturas VPN para acomodarse a las necesidades del ambiente de trabajo de PETROPRODUCCION. Las configuraciones soportadas incluyen: Red-a-Red | Host-a-Red | Host-a-Host

4.4.1.3 CIFRADO AVANZADO

Los sofisticados algoritmos de cifrado incluyen: como muestra en la tabla IV.1

•	AES (Rijndael)	•	Serpent 128-bit
•	DES	•	Twofish 128-bit
•	3DES	•	MPPE (40 y 128 bit)
•	Blowfish		

Tabla IV.1 Algoritmos de cifrado

A. VPNS IPSEC Y PPTP

La Pasarela VPN Astaro Security Linux establece VPNs mediante PPTP e IPSec. Algunos de los clientes soportados los podemos ver en la Tabla IV.2:

•	Cliente nativo PPTP de Windows
•	Cliente nativo IPSec de Windows
•	Cliente nativo IPSec de Astaro
•	Otros clientes VPN que siguen el estándar IPSec
•	Cliente VPN de Mac OS X

Tabla IV.2 Clientes que soportan VPNS

B. MÉTODOS DE AUTENTICACIÓN

Se ofrecen una variedad de métodos de autenticación con los que pueden utilizarse las VPNS como se puede ver en la Tabla IV.3

•	Clave Privada Compartida (PSK)
•	Certificados (X.509v3)
•	Claves RSA tipo Raw
•	CHAP, MSCHAP, MSCHAPv2, y PAP
•	RADIUS (para L2TP IPSec y PPTP)

Tabla IV.3 Métodos de Autentificación

C. PROTOCOLOS IPSEC

Los protocolos soportados por Astaro Gateway 6.0 son los que se muestran en la siguiente Tabla IV.4

✚	Internet Key Exchange (IKE)
✚	Encapsulated Security Payload (ESP)
✚	Layer 2 Tunneling Protocol (L2TP)
✚	NAT-Traversal

Tabla IV.4 Protocolos Soportados

Las formas de utilización de la VPN se lo realizan por medio de conexión a Internet desde cualquier parte del planeta a través de protocolo PPTP como se muestra en la Figura IV.3

Figura IV.3 Conexión por VPN

4.4.1.4. AUTORIDAD DE CERTIFICACIÓN

Astaro Security Linux VPN incluye una Autoridad de Certificación interna cuya utenticación se encuentra basada en la cadena de confianza PKI. Esto permite el uso de certificados digitales sin requerir que los certificados precisen ser generados centralmente y distribuidos a las delegaciones remotas.

A. TÚNELES VPN DE IP DINÁMICA

Los túneles VPN se pueden crear basados en direcciones IP dinámicas en ambos extremos de la conexión (túnel dyn-dyn). Esto proporciona flexibilidad a la hora de elegir distintos Proveedores de Internet (ISP), tipos de redes y enlaces de Internet para las oficinas y usuarios remotos.

4.4.1.5. ACCESO REMOTO SIMPLIFICADO

Las direcciones IP dinámicas y las direcciones de servidores DNS y WINS se configuran automáticamente en el equipo cliente para simplificar el acceso remoto. Las configuraciones de cliente de IPSec se pueden generar y distribuir desde un punto central, simplificando despliegues en masa de VPNs IPSec.

A. INTEGRACIÓN EN ARQUITECTURAS EXISTENTES

- Authenticación de usuarios VPN contra una base de datos local, Servidores Radius, o Directorio Activo.
- Aplicación de políticas de acceso basadas en usuarios y grupos, así como IPs y redes.
- Aplicación de políticas de acceso según grupos de usuarios IPSec basados en PKI.
- Soporte total de VPNs Nativas Windows y Mac OS X usando L2TP sobre IPSec.

4.4.1.6 INTEGRACIÓN CON EL FIREWALL

La Pasarela VPN se integra a la perfección con el firewall de Astaro Security Linux. Las VPNs de tipo IPSec soportan NAT-Traversal y direcciones IP virtuales. Las reglas de filtrado de paquetes del firewall se generan automáticamente a medida que se van configurando los clientes de VPN. Las políticas de filtrado de paquetes se pueden especificar a nivel de cada usuario individual. Los grupos de usuarios de VPN pueden ser creados y utilizados para conceder derechos de acceso.

4.4.1.7 PROTECCIÓN DE INTRUSOS

Astaro Security Linux Intrusión Protección escanea todo el tráfico de red entrante y emplea tecnología de reconocimiento de patrones para detectar más de 1.500 tipos de sondas,

taques de denegación del servicio (DoS), e intentos de explotación de vulnerabilidades de aplicación. Los administradores pueden fijar los umbrales para ser notificados acerca de incidentes, bloquear el tráfico sospechoso, y activar y desactivar reglas para conseguir el mayor rendimiento.

A. AMPLIO ABANICO DE REGLAS DE DETECCIÓN

Astaro Intrusion Protection usa una base de datos de más de 2.000 reglas para detectar patrones:

- Ataques premeditados que explotan vulnerabilidades en tráfico de mensajería y chat, así como redes Peer-2-Peer (P2P).
- Sondeos hostiles, escaneo de puertos, búsqueda de puertas traseras (backdoor probes), interrogaciones ilegítimas, barridos de Host y otras actividades sospechosas.
- Ataques de Denegación del Servicio (DoS) como los SYN flood.
- Previene los exploits de protocolo, corrigiendo debilidades en los servicios de DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, x11 y otros protocolos de red.
- Ataques de aplicación, explotando errores de programación en software desarrollado internamente y scripts CGI. También defiende de ataques conocidos en aplicaciones y bases de datos populares tales como Oracle, MySQL server, Coldfusion y Frontpage.

El proceso de detección de intrusos actúa como se muestra en la Figura IV.4

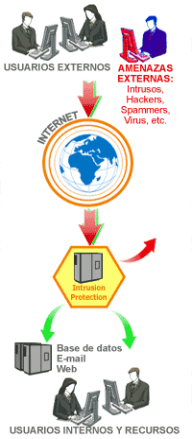


Figura IV.4 Intrusión Protection

4.4.1.7.1 DETECCIÓN Y PREVENCIÓN DE INTRUSOS

Astaro Security Linux detecta la intrusión identificando los comportamientos sospechosos y notificando al administrador de sistema sobre incidentes concretos. El software también proporcionar prevención de la intrusión trabajando conjuntamente con el cortafuegos para bloquear inmediatamente el tráfico entrante asociado al intento de intrusión.

A. LA DETECCIÓN Y LA PREVENCIÓN DE INTRUSOS SE PUEDEN EMPLEAR SIMULTÁNEAMENTE.

Los nuevos patrones de amenazas se instalan frecuentemente mediante el servicio de actualizaciones Up2Date a través de Internet. Astaro monitoriza y aprende los nuevos patrones de amenazas publicados en la base de datos del proyecto Snort, el proyecto basado en código abierto más importante dedicado a la detección de intrusos.

B. RENDIMIENTO Y CONTROL

Implantando la protección de intrusos en línea con el firewall, Astaro asegura que todo el tráfico de Internet y VPN es inspeccionado ágilmente, y evita los retrasos en el flujo de la información que existen en otras soluciones basadas en el desvío del tráfico a un sensor separado.

El administrador tiene la posibilidad de configurar a medida cada tipo de inspección según cada red y servidor de las siguientes formas:

- Activando o desactivando cualquiera de más de 1.500 reglas.
- Customizando reglas existentes o creando reglas nuevas.
- Realizando ciertas clases de pruebas solamente en redes o tráfico específico o proveniente de servidores específicos (por ejemplo, ejecutando pruebas relacionadas con email solamente sobre el tráfico hacia y desde los servidores de correo).

C. CLASES DE REGLAS DE DETECCIÓN DE INTRUSOS

Astaro Security Linux Intrusión Protección escanea todo el tráfico de red entrante y emplea tecnología de reconocimiento de patrones para detectar más de 1.500 tipos de sondas, ataques de denegación del servicio (DoS), e intentos de explotación de vulnerabilidades de aplicación. Las clases de reglas las podemos ver en la tabla IV.5.

El administrador tiene la posibilidad de configurar a medida cada tipo de inspección según cada red y servidor de las siguientes formas:

- Activando o desactivando cualquiera de más de 1.500 reglas.
- Customizando reglas existentes o creando reglas nuevas.
- Realizando ciertas clases de pruebas solamente en redes o tráfico específico o proveniente de servidores específicos (por ejemplo, ejecutando pruebas relacionadas con email solamente sobre el tráfico hacia y desde los servidores de correo).

Sondas y Ataques	Aplicaciones y Servicios	Protocolos
Software de Puerta Trasera	Mensajería y Chat	DNS
Denegación de servicio	Base de datos MySQL Server	FTP
DoS Distribuído	Base de datos Oracle	ICMP
Escaneo de Redes	Scripts CGI	IMAP
Tráfico NO Deseado	Redes P2P (Napster, Kazaa, ...)	NetBIOS
	Coldfusion	NNTP
	FrontPage	P2P
	Microsoft IIS	POP2
	Software de Streaming Multimedia	POP3
		RPC
		SMTP
		SQL

Tabla IV.5 Clases de reglas de intrusion protection

4.4.1.8 SEGURIDAD WEB

La red (Internet) es un lugar peligroso**.** Como los usuarios de computadoras navegan en la red y descargan archivos, pueden infectar sus computadoras y la red con spyware y virus. Y las organizaciones necesitan saber si los usuarios de computadoras están creando obligaciones legales accediendo sitios Web inadecuados y descargando los materiales derechos de autor. Las amenazas pueden robar la información confidencial, inhabilitan computadoras,

desborde la capacidad de red, y llegue sobrepasar los costos de soporte.

La seguridad web consta de Virus Protection, Surf Protection y Spyware Protection como se muestra en la Figura IV.5

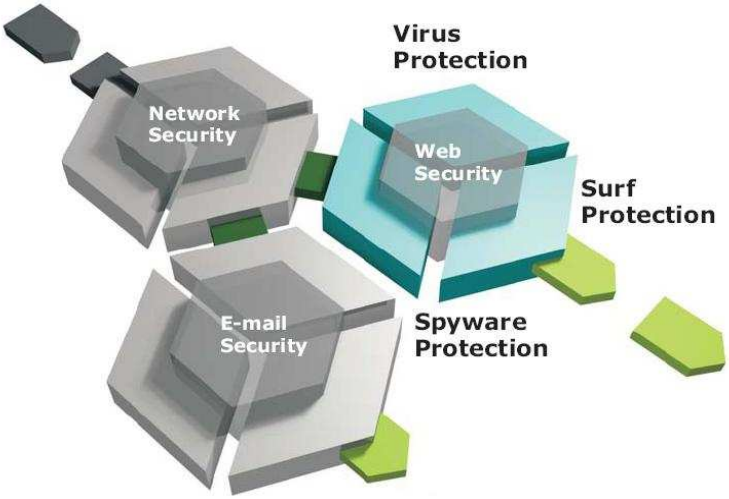


Figura IV.5 Web Security

4.4.1.9 PROTECCIÓN ANTIVIRUS

Virus, gusanos y todo tipo de software maligno, son amenazas que pueden penetrar en organizaciones pasando a través de los servidores de correo, o directamente a los usuarios que descargan emails y ficheros a través de sus navegadores. El antivirus de Astaro puede protegerle contra todo ello.

4.4.1.9.1 ANTIVIRUS PARA EMAIL

Astaro Security Linux Virus Protection para Email escanea los mensajes de correo entrante y saliente así como los archivos adjuntos que se transmiten mediante los protocolos estándares (SMTP y POP3).

4.4.1.9.2 ANTIVIRUS PARA LA WEB

Virus Protection for the Web escanea emails, archivos adjuntos, y archivos descargados por los usuarios que usan servicios web email, así como los archivos descargados mediante sus navegadores conforme a los protocolos estándares (HTTP, FTP).

Astaro Security Linux Virus Protection complementa los paquetes antivirus de escritorio proporcionando un único punto de control donde los virus descubiertos recientemente pueden ser bloqueados con rapidez, antes de que infecten su red interna.

4.4.1.10 ALTA EFECTIVIDAD

El Antivirus de Astaro utiliza tres métodos de detección independientes para detectar el rango más amplio posible de amenazas víricas:

- Firmas de virus**.** Los mensajes de email y sus adjuntos, así como el tráfico Web, se comparan con los modelos conocidos contenidos en una extensa base de datos de virus.
- Heurística**.** Sofisticadas reglas detectan patrones y comportamientos que se asemejan a tipos conocidos de virus.
- Emulación**.** Todo código sospechoso es ejecutado en un ambiente protegido, por ejemplo desempaquetando ficheros archivados y ejecutando los scripts y las macros.

El software es capaz de abrir e inspeccionar más de 700 formatos de ficheros adjuntos y comprimidos como se muestra en la Figura IV.6.

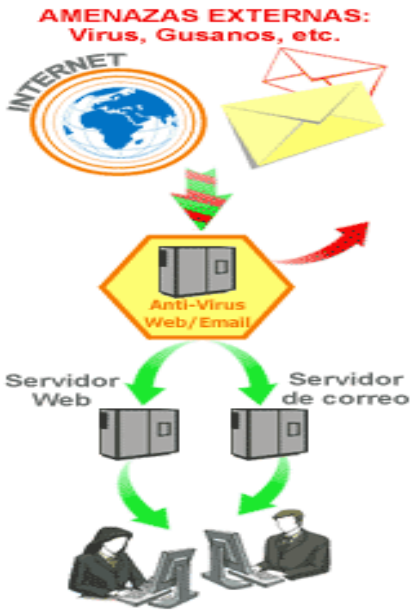


Figura IV.6 Anti-Virus Web/Email

4.5 E-MAIL SECURITY

La aplicación Protection de correos electrónicos no deseados de Astaro detecta y bloquea correos electrónicos no solicitados. Usa métodos de detección múltiples para apuntar con precisión los tipos de correos electrónicos no deseados. Ello ejecuta una serie de pruebas y asignan un “spam score” a cada mensaje que indica el |ity| de probabilidad. Los mensajes cuya cuenta exceden los umbrales puestos por el administrador son eliminados, retornados al remitente, pasado al receptor con una advertencia, o puso en cuarentena el modulo de E-mail Security consta con Virus Protection, Phshing Protection y Spam Protection como se muestra en la Figura IV.7.

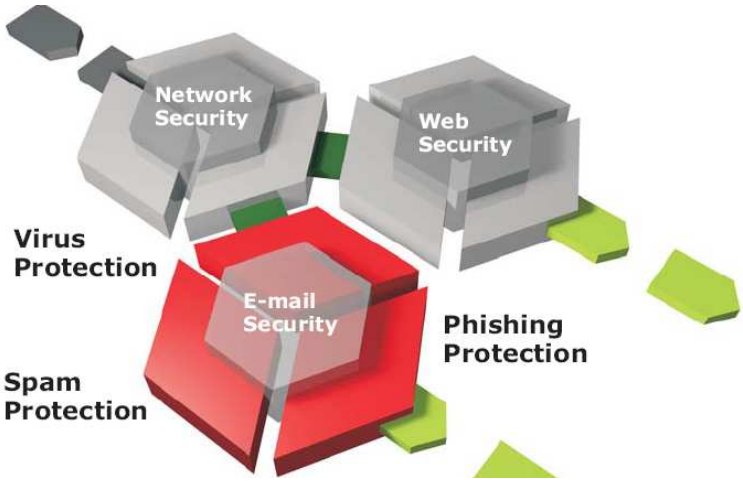


Figura IV.7 E-mail Security

A. VIRUS PROTECTION FOR E-MAIL

La protección de virus de Astaro para la aplicación E-mail detecta y bloquea los virus en tráfico de correo electrónico. Ello examina correos que ingresan y mensajes de correo electrónico que salen y adjuntos de correo electrónico de PETROPRODUCCION el correo electrónico estándar (SMTP y POP3). La protección de virus para el correo electrónico emplea métodos de detección múltiples y una base de datos de más de 280,000 firmas de virus para asegurar exactitud alta y ejecución excelente.

B. PHISHING PROTECTION

Phishing envia por correo electrónico imite legitiman los mensajes de instituciones, comerciantes en la red financieras, y otras fuentes a fin de engañar al usuarios en enviar la

información confidencial a criminales. Mientras que la mayor parte de los ataques son diseñados para capturar información de personal, esté aumentando allí potencial para los métodos de phishing para estar acostumbrado a capturar usuario
ids, contraseñas, y otra información confidencial que puede ayudar al intrusos a penetrar bases de datos corporativas. El Phishing Protection de Astaro detecta y bloquea los correos electrónicos que intente capturar información confidencial que puede ser usada para hurto de identidad, fraude, y ataques en redes corporativas.

4.6 ALIANZA TECNOLÓGICA

El antivirus de Astaro utiliza la base de datos de más de 100.000 firmas de virus mantenida por Kaspersky Labs, un líder global en el sector de la protección antivirus. Con más de 250 empleados, los laboratorios Kaspersky monitorizan Internet en busca de virus nuevos 24 horas al día desde tres sedes a nivel mundial.
Con los servicios de suscripción de Astaro Security Linux Virus Protection, las firmas de virus se pueden mantener al día automáticamente, con una frecuencia de incluso cada hora.

4.7 ADMINISTRACIÓN FLEXIBLE

Los administradores pueden adaptar la protección antivirus a las necesidades y a las preferencias de su empresa de la siguiente manera:

- Seleccionando qué formatos de archivo bloquear en los archivos adjuntos.
- Indicando cadenas de texto para identificar mensajes no deseados.
- Especificando la forma de actuar frente a los mensajes sospechos:
    - Eliminarlos
    - Devolverlos al remitente original con una notificación de error
    - Permitir el paso adjuntando un mensaje de alerta

Mantenerlos en cuarentena para una evaluación y posterior decisión manual. Los informes y los históricos (logs) detallados ayudan a los administradores a solucionar e identificar patrones de actividad recurrentes.

4.7.1 RENDIMIENTO Y ESCALABILIDAD

El antivirus de Astaro incluye características que proporcionan un funcionamiento y escalabilidad excepcionales:

- Reglas inteligentes que seleccionan el mecanismo de la detección más rápido o la combinación de mecanismos para cada tipo de archivo.
- Integración del escaneado de virus con la protección de cortafuegos y spam elimina retardos a la hora de enviar archivos a sistemas adyacentes.
- El software no impone límites al tamaño de archivos escaneados, al número de archivos escaneados en paralelo, o la cantidad de memoria usada para el proceso de exploración de virus, más que los propios de la máquina hardware en cuestión.

Astaro Security Gateway V6 tiene una presentación como se muestra en la figura IV.8

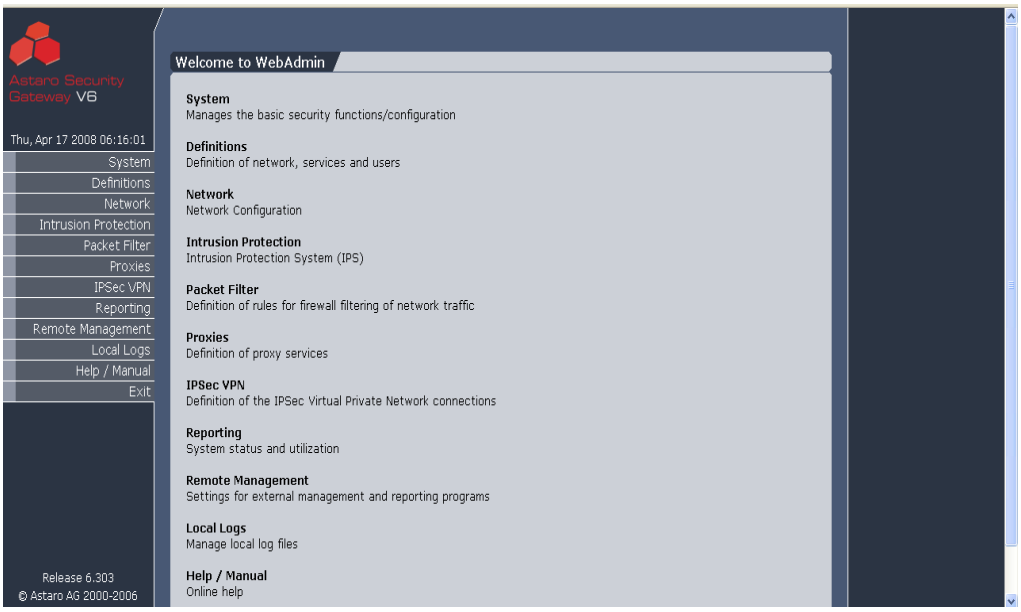


Figura IV.8 Astaro Security Gateway

4.8 CARACTERÍSTICAS PRINCIPALES DE SYSTEMS MANAGEMENT SERVER 2003

4.8.1 IMPLANTACIÓN DE APLICACIONES

- Planificación detallada de la implantación de aplicaciones**.** Los informes detallados disponibles en SMS 2003 facilitan el proceso de implantación de aplicaciones. Con una planificación detallada, resulta sencillo obtener la base de hardware que tiene actualmente el cliente objetivo, las aplicaciones existentes y la información de versión, así como el paquete de servicios actual y los niveles hotfix del sistema.

- Orientación racional de la distribución. La distribución de software y otras tareas de administración pueden orientarse específicamente a equipos a través de una amplia variedad propiedades como la configuración de red o de hardware, la unidad de organización de Active Directory® y un conjunto de estados de instalación de software y de grupos de miembros autorizados.
- Distribución Delta entre servidores de site y puntos de distribución**.** Cuando se efectúan cambios en paquetes de recursos software previamente instalados, estos cambios, en lugar de afectar a la imagen de la aplicación entera, únicamente afectan a los demás servidores de site SMS 2003 y puntos de distribución.
- Derechos avanzados de Windows Installer Service**.** SMS 2003, al admitir el servicio Windows Installer (.msi), es capaz de ir cambiando entre los distintos contextos de cuentas de usuario durante la instalación del paquete de software posibilitando una instalación segura en sistemas de acceso cerrado.
- Soporte para agregar o quitar programas. Las aplicaciones se pueden visualizar con facilidad en la interfaz de agregar o quitar programas, de manera que el usuario dispone de una manera coherente de instalar aplicaciones.

4.8.2 GESTIÓN DE ACTIVOS

- Control del uso de aplicaciones**.** Se pueden generar informes breves o detallados simplemente especificando qué aplicaciones utiliza el usuario, durante cuánto tiempo y en qué sistemas administrados lo hizo. El seguimiento del uso se puede hacer tomando como referencia al usuario o al ordenador y los informes se pueden generar comparando los datos de uso simultáneo con la correspondiente licencia de usuario (informes de conformidad).
- Granularidad en la búsqueda en inventario de software desde archivos**.** Ahora puede configurar SMS 2003 para que descubra por usted los recursos que necesita, y sólo los que necesita.
- Inventario de hardware detallado**.** Las mejoras incorporadas en Windows Management Instrumentation (WMI) facilitan el rendimiento del cliente durante la exploración en inventarios y proporcionan un conjunto ampliado de datos de inventario, incluyendo datos de la BIOS y de placa base y otros elementos físicos.

- Informes en formato Web mejorados**.** Se incluyen más de 120 informes previos que abordan inventarios de hardware y software y otros estados del equipo y del progreso de implantación de software.

4.8.3 GESTIÓN DE PARCHES DE SEGURIDAD

- Identificación de vulnerabilidades**.** Las herramientas estándar de seguridad de Microsoft como el analizador de inventarios Microsoft Baseline Security y la herramienta de inventario para actualizaciones de Microsoft Office le permiten inventariar su sistema para detectar vulnerabilidades y parches aplicables.
- Asistente para la implantación de parches de seguridad**.** Se proporciona un sencillo asistente para consola para facilitar a los administradores la implantación de los parches necesarios en los dispositivos administrados.
- Análisis de vulnerabilidades e informes sobre métodos de resolución**.** Una vez identificados los parches de seguridad que faltan, los resultados de estas exploraciones individuales se envían a la base de datos central para poder hacer informes y orientar la resolución. En cuanto los parches de seguridad necesarios se han implantado, estos datos se pueden actualizar en tiempo real de forma óptima.

4.8.4 MOVILIDAD

- Clientes con capacidad de adaptación al ancho de banda**.** El nuevo Advanced Client utiliza la tecnología Background Intelligent Transfer Service (BITS) para detectar de forma automática la capacidad de la conexión de red del cliente y a partir de ahí ajustar las velocidades de transferencia con eficiencia.
- Checkpoint/reinicio**.** En caso de desconexión, cualquier descarga a los ordenadores cliente que no se hubiera completado se reanudará en el punto en el que se detuvo. Ya no es necesario reiniciar las transmisiones de datos por culpa de que se desconecte la sesión. Checkpoint/reinicio actúa a nivel de byte y simplemente requiere descargar en un paquete los bytes que no se hubieran transferido.
- Descarga y ejecución**.** Una vez descargado con éxito un paquete de software en el ordenador cliente permanece en el caché del sistema cliente hasta que concluya el tiempo de instalación programado y entonces se ejecuta.

- Comportamiento adaptado a la ubicación física**.** Como los usuarios se desplazan geográficamente con frecuencia, los límites de site flexibles garantizan que reciben los paquetes de software y las actualizaciones desde la fuente de instalación adecuada más cercana con lo que resulta innecesario que la instalación de software se realice a través de la red de área extensa de la empresa (WAN).

4.8.5 INTEGRACIÓN DE SERVICIOS DE ADMINISTRACIÓN DE WINDOWS

- Directorio Activo**.** Con SMS 2003 descubrirá enseguida las propiedades de Active Directory tanto en los usuarios como en los sistemas, incluyendo el de unidades de la organización y la autorización de pertenencia en lo que respecta a grupos. Los paquetes de software se pueden distribuir de forma dirigida en base a estos atributos de Active Directory.
- Límites de site basados en Directorio Activo**.** Ahora, los límites de site se pueden basar en los nombres de site de Directorio Activo en lugar de en subredes de protocolo de Internet (IP).
- Modo de seguridad avanzada**.** Las cuentas registradas en los ordenadores y sistemas locales podrán ser utilizadas en todas las funciones de servidor (como por ejemplo para acceder a las bases de datos) con lo que se simplifica enormemente la administración de las cuentas y contraseñas en SMS 2003 y se aporta seguridad a la empresa al no tener que crearse más cuentas con derechos avanzados.
- Herramientas de estado mejoradas**.** Los datos de estado proporcionan información en tiempo real acerca del estado de los procesos de SMS 2003 en curso, tanto en los servidores como en los clientes.
- Asistencia remota para Windows XP**.** La utilidad de alto rendimiento de asistencia remota de Windows XP constituye ahora una opción para solucionar problemas en los ordenadores cliente de forma remota administrándolas de forma centralizada desde Administrator Console de SMS cuando un usuario está trabajando en un equipo remoto.

4.9 COMPATIBILIDAD HARDWARE Y SOFTWARE DE SMS

4.9.1.1 REQUISITOS DE SISTEMA PARA LA INSTALACIÓN DEL SERVIDOR

- CPU: procesador Intel Pentium/Celeron (o compatible) de 550 MHz o superior, recomendado
- Microsoft Windows 2000 Server, Windows 2000 Advanced Server, o Windows 2000 Datacenter Server con Service Pack 4 o posterior; o Windows Server™ 2003 Ed. Estándar, Windows Server 2003 Ed. Enterprise, o Windows Server 2003 Ed. Datacenter
- Internet Information Services (IIS) debe estar instalado dentro de la instalación del servidor Windows, para acceder a determinadas funciones y roles del sistema en el site SMS.
- Microsoft SQL Server 7.0 SP3 o posterior, SQL Server 2000 SP3a o posterior, o SQL Server 2005 pueden utilizarse para alojar la base de datos SMS para SMS 2003 R2.
- SMS 2003 con Service Pack 2 si se está actualizando una infraestructura existente.
- 256 MB de RAM (4 GB de RAM máximo)
- 2 GB de espacio disponible en disco, sobre una partición NTFS
- Unidad de CD-ROM o DVD-ROM
- Tarjeta de red
- Tarjeta de vídeo compatible con Windows 2000
- Teclado y ratón de Microsoft o dispositivo apuntador
- compatible, o bien un hardware que permita la redirección de la consola.

4.9.1.2 ESPECIFICACIONES PARA LA HERRAMIENTA DE PUBLICACIÓN DE ACTUALIZACIONES PERSONALIZADAS

- CPU: procesador Intel Pentium/Celeron (o compatible) de 600 MHz o superior, recomendado
- Microsoft Windows XP Profesional con Service Pack 2 o posterior, o Windows Server™ 2003 Ed. Estándar, Windows Server 2003 Ed. Enterprise o Windows Server 2003 Ed. Datacenter con Service Pack 1 o superior
- 256 MB de RAM; recomendado 512 MB o más

- 10 MB de espacio disponible en disco, y 350 Mb adicionales si se instala SQL Server Express Edition para la Herramienta de Publicación de Actualizaciones Personalizadas.
- Tarjeta de red.
- Microsoft Internet Explorer 5.0 o superior
- Pantalla y tarjeta gráfica Super VGA (800 × 600) o con resolución superior
- Teclado y ratón de Microsoft o dispositivo apuntador compatible

4.9.1.3 ESPECIFICACIONES PARA INSTALACIÓN DE CLIENTE SMS 2003 R2

- PC con procesador Intel Pentium/Celeron o compatible, de 133 Mhz mínimo; recomendado procesador de 300 MHz o superior
- Microsoft Windows 98; Windows 2000 Profesional, Windows 2000 Server, Windows 2000 Advanced Server, o Windows 2000 Datacenter Server con Service Pack 4 o posterior; o Windows XP Profesional; o Windows XP Embedded con Service Pack 1 o posterior; o Windows Server 2003 Ed. Estándar, Windows Server 2003 Ed. Enterprise, o Windows Server 2003 Ed. Datacenter
- Soporta equipos con 64 Mb de RAM, pero puede limitar el rendimiento y uso de ciertas funcionalidades. Se recomienda 128 Mb o más de memoria.
- 80 MB de espacio disponible en disco
- Tarjeta de red
- Microsoft Internet Explorer 5.0 o posterior
- Pantalla y adaptador de gráficos Super VGA (800 × 600) o resolución superior
- Teclado y ratón de Microsoft o dispositivo apuntador compatible
    - Sistemas operativos obsoletos: la instalación del Cliente Legacy de SMS 2003 R2 no está soportado en ningún sistema operativo de cliente con capacidad para la instalación de Cliente Avanzado. Microsoft Windows 98 es el único sistema operativo soportado para los Clientes Legacy.
    - Sistemas Operativos de Cliente Avanzado: SMS 2003 R2 no soporta la instalación del Cliente Avanzado en plataformas de cliente anteriores a Windows 2000 Service Pack 4 o Windows XP
      Service Pack 1.

4.10 LIMITACIONES DE SEGURIDAD DE SMS

- Limitación en sistemas operativos**.** las limitaciones de sms en el ámbito de seguridad se dan para los sistemas que no pertenecen a los productos que no son Microsoft, como son los sistemas operativos:
    - Linux
    - As/400
    - Sun

  Como también para las aplicaciones que son para cada uno de estos sistemas operativos.
- Limitación en Pcs que no estén dentro de un directorio Activo**.** Los pcs deben estar dentro de un directorio activo para poder realizar actualizaciones del sistema operativo como de las aplicaciones
- Limitaciones por la versión del sistema operativo de los Pcs.

  Los sistemas operativos como:
    - Windows 9x
    - Windows 2000 con SP menor que el 4

  No podrán ser actualizados por que el soporte para este tipo de sistemas se ha dejado de realizar, además el sistema de SMS es con SP 2 por lo cual no actualiza estos sistemas.

4.10.1 UTILIZACIÓN DE SMS

4.10.1.1 INVENTARIO DE HARDWARE

El agente de inventario de hardware recolecta una amplia variedad de propiedades de hardware del cliente, como por ejemplo: información del disco como el espacio usado y el espacio disponible; memoria, video, procesador y datos del sistema operativo; programas registrados en adicionar y remover programas; y MAC, IP y dirección de las subredes.

El proceso de inventario de hardware está diseñado para consultar el Windows Management Instrumentation (WMI) que es lo que utiliza la instalación del cliente de SMS para obtener sus datos. Windows Management expone una vasta cantidad de información acerca del cliente, obteniéndola de varios proveedores, incluyendo el subsistema WIN32 de Windows, el registry, la BIOS entre otros.

También se pueden adicionar datos al inventario que es recolectado normalmente. Por ejemplo se podría agregar la placa de activo fijo del computador, nombres de contactos, información sobre la compra, entre otros. Esta tarea se lleva a cabo mediante la creación de archivos de texto conocidos como Management Information Format (MIF) que se presentan ante SMS como una actualización a los registros de la base de datos para cada cliente especifico.

A. CONFIGURACIÓN DEL AGENTE

En la pestaña "General", habilitar el agente para recolectar inventarios cada mes. Configurar para que el inventario se tome cada jueves a las 12:30 p.m.

En la pestaña "MIF Collection", no habilitar ninguna opción. Esta se habilitaría en caso que se requiera adicionar datos como la placa de activo fijo, contactos u otros que defina Petroproducción como se muestra en la Figura IV.9.

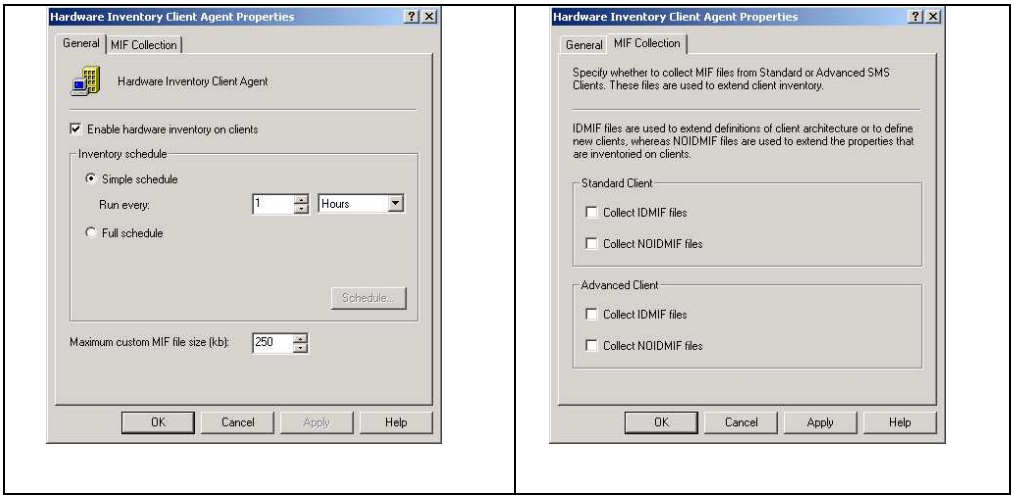


Figura IV.9 Configuración del Agente

4.10.1.2 INVENTARIO DE SOFTWARE

El agente de inventario de software recolecta información acerca de los aplicativos que incluye:

- Nombre de archivo, versión y tamaño
- Nombre del fabricante
- Nombre del producto, versión y lenguaje

- Fecha y hora de creación (presumiblemente en la instalación)

El agente de inventario de software también puede recolectar copia de archivos específicos, como por ejemplo el autoexec.bat o algún .ini especifico de una aplicación.

A diferencia del inventario de hardware, el agente de inventario de software revisa los discos locales en vez de consultar los datos al WMI.

A. CONFIGURACIÓN DEL AGENTE

- En la pestaña "General", habilitar el agente para recolectar inventarios quincenalmente. Configurar para que el inventario se tome los días viernes a las 12:30 p.m.

- En la pestaña "Inventory Collection", habilitar para revisar los archivos .exe en todos los discos duros. Configure para que excluya los archivos comprimidos, encriptados y los que están bajo el directorio Windows, esto con el fin de reducir la búsqueda y centrarse en las rutas donde más se encuentra información. En caso que se requiera algún archivo específico del directorio Windows se puede adicionar el nombre del archivo o un wildcard que lo identifique.

- En la pestaña "File Collection", no adicione ningún archivo. Se agregarán archivos cuando PETROPRODUCCION defina que es necesario recolectar alguno en especial.

- En la pestaña "Inventory Names", adicione tipos de nombres que se quieran estandarizar para los inventarios. Esta lista se ira construyendo a medida que se vaya operando el producto y se requieran estandarizar los nombres de los fabricantes o de los productos inventariados por el agente como se muestra en la Figura 3.8.

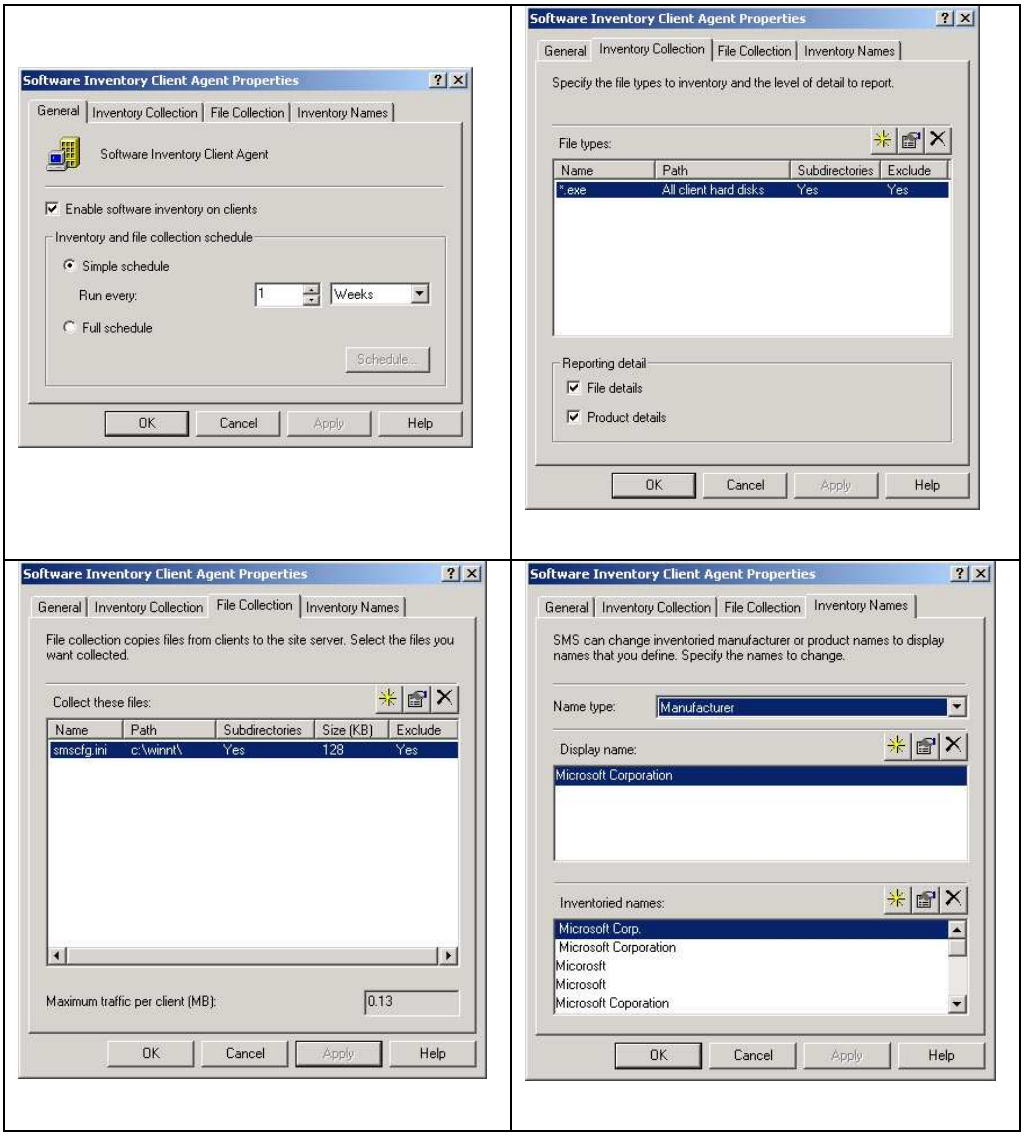


Figura IV.10 Configuración del agente de Inventario de Software

4.10.1.3 DISTRIBUCIÓN DE SOFTWARE

Una de las principales características de SMS 2003 es su habilidad para distribuir paquetes y correr programas en los clientes de SMS. Este proceso consiste de tres elementos básicos:

- Crear y distribuir el paquete
- Avisar un programa del paquete a una colección
- Recibir un aviso y ejecutar un programa en el cliente

A. CONFIGURACIÓN DEL AGENTE

En la pestaña "General", habilitar el agente para distribución de software y colocar un valor de 60 minutos tanto para el cliente legacy como para el cliente avanzado. Habilitar la opción para que los clientes no puedan modificar la configuración del agente.
En la pestaña "Notification", deshabilite todas las opciones que vienen por defecto, ya que no se quiere que se muestre ningún mensaje al usuario al momento de hacer distribuciones como se muestra en la Figura IV.11.

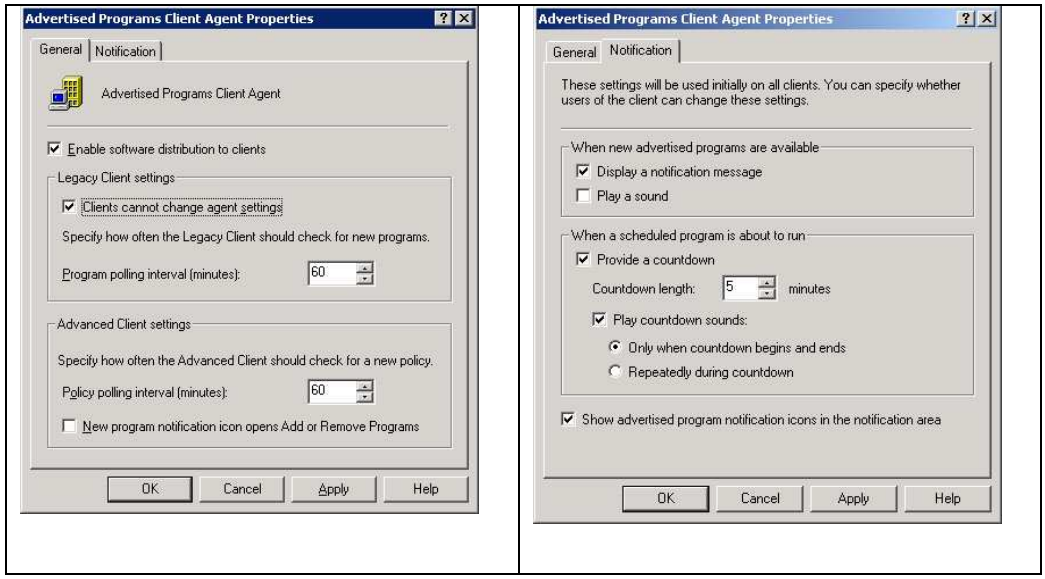


Figura IV.11 Configuración del Agente de Distribución de Software

B. TIEMPO ESTIMADO DE TRANSFERENCIA DE PAQUETES EN ENLACES LENTOS

Transferir grandes paquetes desde un sitio a otro, desde el servidor de sitio a un distribution point o desde un distribution point hacia el cliente, puede tomar una gran cantidad de tiempo. Esto es especialmente cierto cuando el enlace es lento, o está muy ocupado. En tales casos es importante estimar cuánto tiempo puede tomar la transferencia del paquete. Esta estimación le permite a PETROPRODUCCION resolver dos problemas:
Decidir cuándo comenzar a solucionar un problema de transferencia que no ha sido completada
Decidir cuándo transferir un paquete por la noche o un fin de semana.

Ancho de banda disponible	128 Kbps	28.8 Kbps	9.6 Kbps
Bits/Sec	131,072	29,941	9,830
Bytes/Sec	16,384	3,686	1,229
Bytes/Tour	58,982,400	13,271,040	4,423,680

C. MECANISMO PARA DETENER EL PAQUETE CUANDO AFECTA ALGUNA OFICINA

Cuando el paquete está siendo copiado desde el servidor de sitio hacia el distribution point, no existe un address que regule el uso de ancho de banda, para poder detener la distribución hacia los distribution point se debe detener el componente llamado SMS_DISTRIBUTION_MANAGER, como se observa en el siguiente gráfico. Para continuar con la distribución basta con iniciar de nuevo el componente como se muestra en la Figura IV.12.

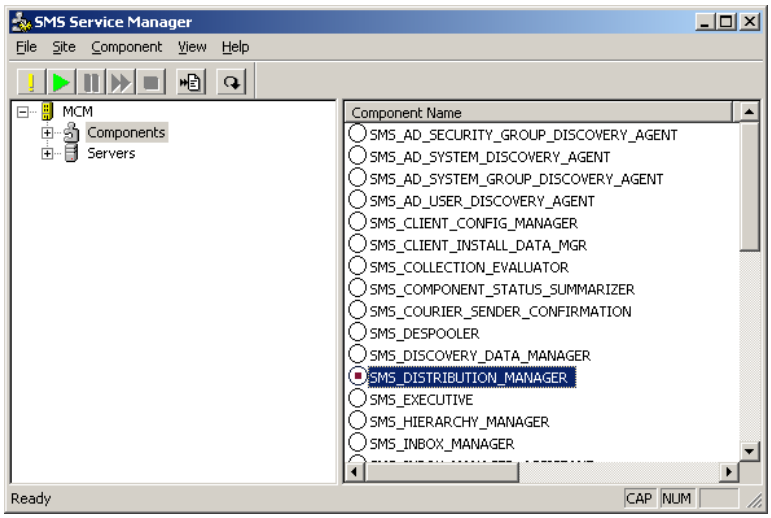


Figura IV.12 SMS Service Manager

D. INVENTARIO DE HARDWARE, INVENTARIO DE SOFTWARE Y DISTRIBUCIÓN DE SOFTWARE POR DEMANDA

El inventario de hardware y software esta configurado para recolectar la información periódicamente. La distribución de software esta configurada para revisar si existen nuevos paquetes cada hora. En ocasiones es necesario tomar un inventario de hardware o software por

demanda, por fuera de la programación original. Para este requerimiento se recomienda utilizar una herramienta llamada SMSUtilities, la cual proporciona los medios para tomar el inventario de hardware, inventario de software y distribución de software (ver gráfico, opciones remarcadas) inmediatamente a un grupo de maquinas especificadas en un archivo, colección de SMS o a una maquina individual. Esta utilidad puede ser ejecutada en el servidor de SMS o en una estación de trabajo como se muestra en la Figura IV.13.

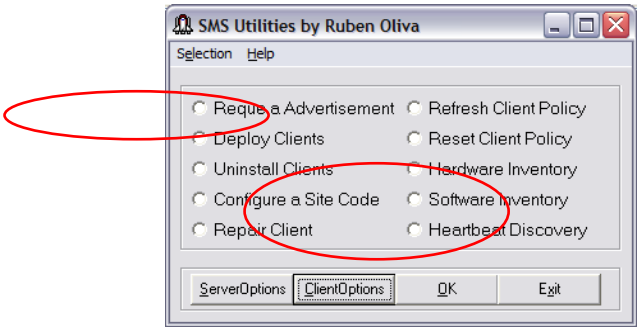


Figura IV.13 SMS Utilities para inventarios

Para obligar a todas las estaciones se selecciona la opción de "Configure a List" y luego el uso de una colección de SMS que para todas las maquinas sería "All Systems", para lo cual hay que configurar las opciones como muestran las Figuras IV.14, Figura IV.14.1 y Figura IV.14.2

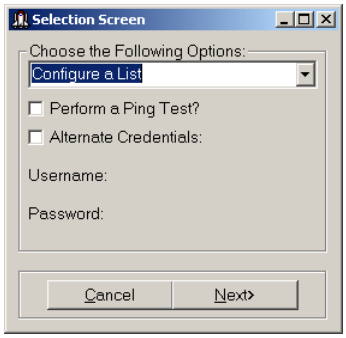


Figura IV.14

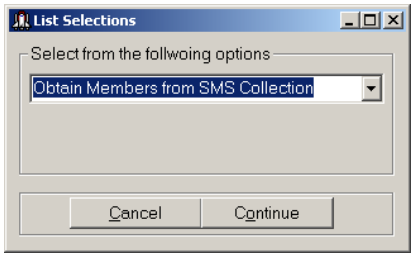


Figura IV.14.1

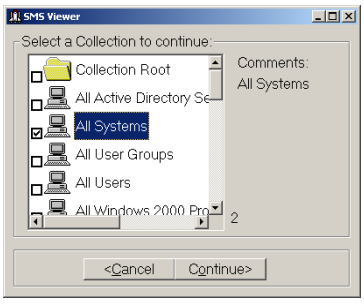


Figura IV.14.2

4.10.1.4 HERRAMIENTAS REMOTAS

Con las herramientas remotas, el administrador de SMS puede remotamente diagnosticar un cliente, iniciar o detener servicios, ver el escritorio del usuario, ejecutar programas, y transferir archivos. El usuario también tiene la habilidad para determinar quién puede acceder al cliente y qué tipo de funciones están permitidas.

La recomendación dada en el diseño exige que para habilitar este agente se cumpla con la condición de que los usuarios no sean administradores locales de las estaciones. Cuando se cumpla la condición se puede habilitar el control remoto con la siguiente configuración:

A. CONFIGURACIÓN DEL AGENTE

En la pestaña "General", habilitar el agente para herramientas remotas y seleccionar la opción para que los usuarios no puedan cambiar la configuración del agente. No habilite ninguna opción de Remote Assistance.

En la pestaña "Security", agregar a las lista de Permitted Viewers el grupo: "UIO\SMS_Helpdesk".

En la pestaña "Policy", seleccionar en las opciones de SMS Remote Tools un nivel de acceso Full y la opción de solicitar permiso del usuario.

En la pestaña "Notification", seleccione la opción de desplegar un indicador visual, con la subopción de mostrar un icono de estado en la barra de tareas. Deshabilite la opción de sonido.

En la pestaña "Advanced", deje las opciones por defecto como se muestra en la Figura IV.15.

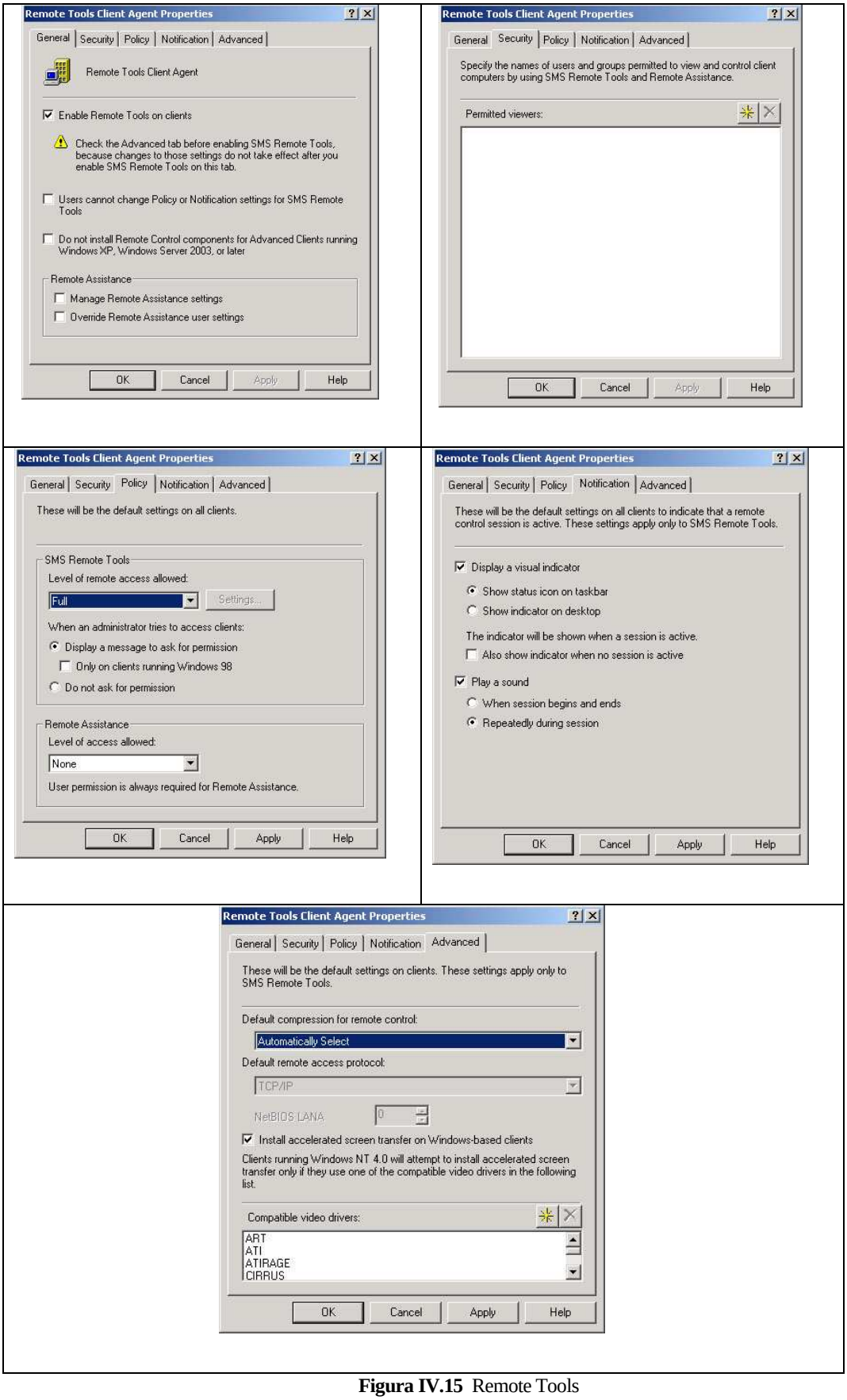


Figura IV.15 Remote Tools

B. CONFIGURACIÓN PARA NO SOLICITAR PERMISO EN SERVIDORES

Debido a que el PETROPRODUCCION tiene una aplicación sobre los servidores que tiene que correr en el contexto de un usuario logueado, se hace necesario que para dichas maquinas no se solicite permiso al momento de tomar control remoto. Para lograr esta configuración se debe modificar en los servidores, el valor llamado “Permission Required” ubicado en la siguiente clave del registro

HKLM\Software\Microsoft\SMS\Client\Client Components\Remote Control

Y colocando como valor el número cero (0).

Para facilitar la tarea de implementación se creará durante la instalación un paquete que se encarga de modificar automáticamente el valor, este paquete será aplicado a la colección que contiene los servidores del PETROPRODUCCION.

4.10.1.5 MEDICIÓN DE USO DE SOFTWARE

La medición de uso de software recolecta y monitorea información sobre el uso de programas en los computadores clientes de SMS, incluyendo datos sobre los usuarios que ejecutan el programa, cuando el programa fue iniciado, y cuando el programa fue detenido. Un programa es un archivo ejecutable que puede correr en la memoria del computador, especialmente archivos .EXE y archivos .COM. Se utiliza esta información para ayudar a determinar como los programas son usados dentro de la organización, cuando y como están siendo usados y cuando se cumple con los acuerdos de licenciamiento para los programas que están siendo monitoreados. El administrador determina que programas medir creando reglas de medición de uso de software, las cuales son copiadas a cada cliente.

A. CONFIGURACIÓN DEL AGENTE

Este agente va a estar habilitado en la jerarquía, y recolectará datos de uso de software de PETROPRODUCCION. Antes de que el agente empiece a recolectar datos es necesario definir las reglas para medición de uso de software, según las necesidades de PETROPRODUCCION.

En la pestaña “General”, habilitar el agente para medición de uso de software. En la pestaña “Schedule”, habilitar con las opciones por defecto. Estas opciones cambiarán cuando por demanda se requiera información sobre el uso de software como se muestra en la Figura IV.16.

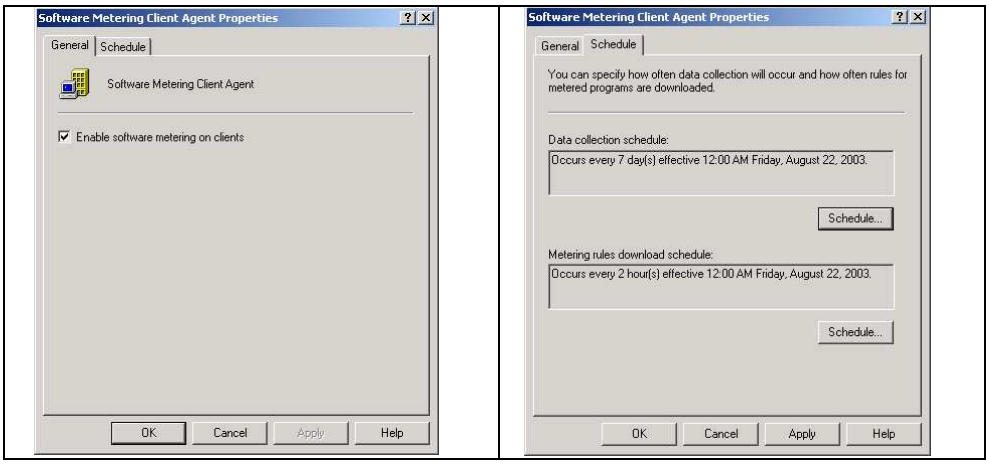


Figura IV.16 Configuración del uso de un determinado software

4.10.1.6 OTROS COMPONENTES DE SMS

A. DISTRIBUCIÓN DE ACTUALIZACIONES CRÍTICAS (INVENTORY TOOL FOR MICROSOFT UPDATE)

SMS 2003 Inventory Tool for Microsoft Updates, suministra actualizaciones de seguridad de forma confiable y flexible, despliegue de actualizaciones y sistemas de administración de service packs construidos sobre la tecnología de Windows Server Update Services. Esta versión incluye una completa instalación de una herramienta de inventario al igual que una redistribución del Windows Update Agent para detección e implementación de las ultimas actualizaciones de seguridad y service packs de Microsoft para una variedad de productos incluyendo Windows, Office, SQL y Exchange.

En la instalación de este componente se debe configurar el servidor de SMS como servidor de sincronización, cuya tarea será la de conectarse a Internet (específicamente el sitio de Microsoft Update) y descargar diariamente el catalogo con el listado (no descarga el ejecutable) de todos los parches definidos por sistema operativo y/o aplicación.

4.11 KASPERSKY ANTI-VIRUS 6.0

Combina detección reactiva con la más reciente tecnología proactiva para proveer a su computador con protección sólida contra los programas maliciosos.

En particular, los principiantes quedarán cómodamente sorprendidos de encontrar un producto que es simple de instalar y configurar, mientras que los usuarios avanzados encontrarán un producto que es fácil de utilizar y altamente adaptable a sus requerimientos individuales.

4.11.1 REQUERIMIENTOS DE HARDWARE Y SOFTWARE PARA INSTALAR KASPERSKY WORKSTATIONS

Los requerimientos para instalar kaspersky en estaciones de trabajo son los siguientes:

4.11.1.1 REQUERIMIENTOS GENERALES:

1. Espacio mínimo libre en el disco duro 50MB.
2. Internet Explorer 5.0 o superior.
3. Microsoft Windows 98, Windows Me, con Service Pack 6.0
4. Microsoft Windows 2000 Professional (Service Pack 2 o superior)
5. Microsoft Windows XP Home Edition, Microsoft XP professional (Service Pack 1 o superior)
6. Procesador Intel Pentium 300Mhz o superior
7. Mínimo 128 MB en RAM.

Para los servidores los requerimientos son:

4.11.1.2 REQUERIMIENTOS PARA WINDOWS 2000 SERVER:

1. Microsoft Windows 2000 Server con Service Pack 2 o superior
2. Procesador Intel Pentium
3. Espacio libre en RAM mínimo 64 MB
4. Espacio libre en disco 30 MB mínimo.

4.11.1.3 REQUERIMIENTOS PARA WINDOWS 2003 SERVER:

1. Microsoft Windows 2003 Server:
2. Procesador Intel Pentium
3. Espacio libre en RAM mínimo 128 MB
4. Espacio libre en disco 30 MB mínimo.

Para la instalación de Kaspersky **es muy importante** que en los equipos no se encuentre instalado ningún tipo de antivirus y que los requerimientos sean tomados **en cuenta.**

4.11.2 KASPERSKY ANTI-VIRUS PARA WINDOWS WORKSTATIONS

4.11.2.1 PRINCIPALES VENTAJAS

Protección para todo tipo de archivos: Kaspersky Anti-Virus provee de escaneos contra virus en tiempo real, revisando los archivos cada vez que son creados, abiertos o copiados. El anti-virus está incrustado profundamente en el sistema operativo, revisando todas las operaciones de archivos instantáneamente. Kaspersky Anti-Virus monitorea tanto los discos locales como los remotos automáticamente o según la definición del usuario.

Escaneo de todo tipo de archivos comprimidos: Los virus a menudo se esconden en archivos comprimidos, donde la mayoría de anti-virus tienen problemas para encontrarlos. No así Kaspersky Anti-Virus para Workstation. Este programa escanea más de 700 tipos de archivos, incluso desinfecta archivos tipo ZIP.

Escaneo de mensajes de correo electrónico: Kaspersky Anti-Virus escanea todos los correos electrónicos contra posibles infecciones y detecta todo tipo de malware. Soporta una variada gama de clientes de correo electrónico: Microsoft Outlook, Microsoft Outlook Express, The Bat!, Netscape Messenger, Opera mail client e IncrediMail.

Detención de virus de script: Los anti-virus clásicos, son incapaces de detener virus de script en la infección de la RAM. Kaspersky Anti-Virus puede hacerlo, debido a un chequeador incorporado de scripts, el cual filtra entre scripts y su aplicación correspondiente, lo cual significa que los scripts que corren en su PC son revisados antes de su ejecución.

Detección de todo tipo de amenazas: Kaspersky Anti - Virus para Windows Workstations protege sus estaciones de trabajo no solo de virus y programas maliciosos, sino también de programas potencialmente hostiles, tales como adware, spyware, etc.

4.11.2.2 FUNCIONES

Protección contra ataques de red: La aplicación contiene nuevos componentes que repelen ataques de red y previenen la detección de puertos vulnerables desde el exterior. Cuando un computador no posee firewall, este componente puede actuar como un nivel base de protección para la estación de trabajo.

Protección proactiva de aplicaciones de aplicaciones Microsoft Office: Kaspersky Anti - Virus para estaciones de trabajo usa el modulo Office Guard™ para monitorear todas las macros ejecutadas en documentos de Microsoft Office y bloquear cualquier acción sospechosa.

Soporte para Laptops: Kaspersky Anti - Virus para estaciones de trabajo Windows se asegura de que los laptops estén siempre completamente protegidos, incluso cuando ellos no están conectados a la red. Si la conexión es interrumpida durante la descarga de actualizaciones de la base de datos de anti - virus, las actualizaciones parciales son guardadas y las partes faltantes son descargadas automáticamente cuando la conexión se reestablezca.

4.11.3 KASPERSKY ANTI-VIRUS PARA WINDOWS FILE SERVERS

4.11.3.1 PROTECCIÓN DE DOS NIVELES

La protección eficaz para los servidores es la clave para una solución completa de seguridad de información para redes corporativas. Este producto otorga dos niveles de protección: un monitor de antivirus que escanea todos los archivos que son llamados, modificados y creados, en tiempo real, y un escáner de antivirus que escanea datos almacenados. El escáner puede ser ejecutado de acuerdo con las especificaciones del administrador.

Kaspersky Administration kit ofrece administración y manejo centralizados Kaspersky Updater asegura una fácil descarga de las actualizaciones del antivirus Protección optimizada

La tecnología iChecker™ utiliza checksumming para maximizar el escaneo y el rendimiento del sistema; al no tener que revisar todos los archivos. El escaneo está limitado a aquellos archivos que han sido modificados desde la última vez.

4.11.3.2 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

Este programa escanea más de 700 tipos de archivos, incluso desinfecta archivos tipo ZIP. El módulo ScriptCheckerT protege contra virus de script. Los objetos que son sospechosos o infectados son puestos en cuarentena esperando futuro análisis.

CAPITULO V

DESARROLLO DE GUÍA PARA EL CONTROL DE BRECHAS DE SEGURIDAD EN LOS SERVICIOS DE INTERNET APLICADA A PETROPRODUCCION.

El proponer o identificar una guía de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha guía en función del dinámico ambiente que rodea las organizaciones modernas.

Está lejos de mi intención (y del alcance del presente) proponer un documento estableciendo lo que debe hacer un usuario o una organización para lograr la mayor Seguridad Informática posible. Sí está dentro de mis objetivos proponer los lineamientos generales que se deben seguir para lograr (si así se pretendiese) un documento con estas características.

El presente es el resultado de la investigación, pero sobre todo de mi experiencia viendo como muchos documentos son ignorados por contener planes y políticas difíciles de lograr, o peor aún, de entender.

5.1 GUIA DE SEGURIDAD INFORMATICA

Esto adquiere mayor importancia aún cuando el tema abordado por esta guía es la Seguridad Informática. Sin la necesidad de extensos manuales explicando cómo debe protegerse una computadora o una red con un simple Firewall, un programa antivirus o un monitor de sucesos.

He intentado dejar en claro que la Seguridad Informática no tiene una solución definitiva aquí y ahora, sino que es y será el resultado de la innovación tecnológica, a la par del avance tecnológico, por parte de aquellos que son los responsables de nuestros sistemas.

Las fases para el desarrollo de una guía para el control de brechas de seguridades en los servicios de Internet que se realizaron son las que se muestra en el diagrama de ciclo básico que se muestra en la Figura V.1 Fases para el desarrollo de una guía.

Figura V.1 Fases para el Desarrollo de una Guía

La guía se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad del sistema; pero ante todo, una guía de seguridad es una forma de comunicarse con los usuarios siempre hay que tener en cuenta que la seguridad comienza y termina con personas.

5.2 IDENTIFICACIÓN DEL HARDWARE DE CONEXIÓN ENTRE LA RED INTERNA Y EL INTERNET

El hardware que se utilizaba para la conexión de la intranet y la internet constaba de un modem al cual se conecta el enlace del proveedor de internet y de el sale la conexión a un router el cual se conecta a dos routers de capa tres de los cuales un router se encargaba del trafico que sale desde la intranet hacia el internet y el otro se encargaba del trafico que ingresa desde el internet hacia la intranet como se muestra en la Figura V.2 conexión a internet PPR.

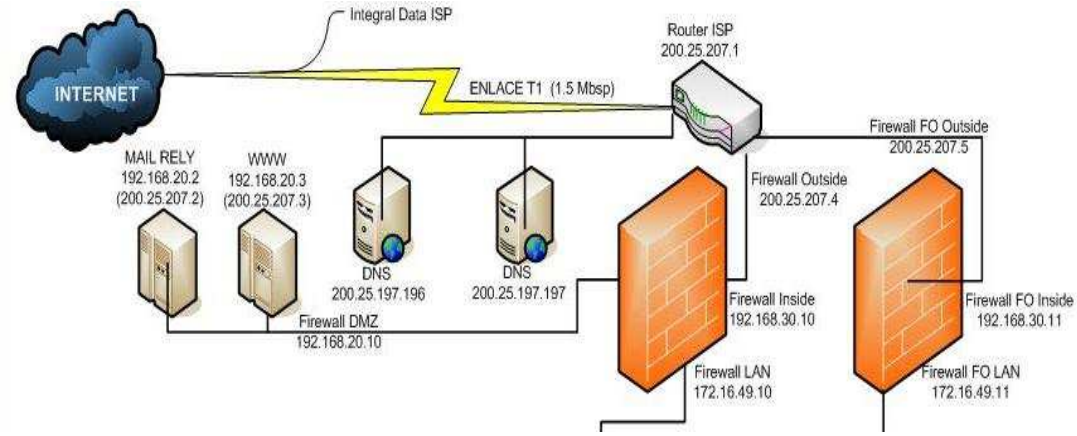


Figura V.2 Conexión a Internet PPR

Este esquema de seguridad es el que utiliza PPR para dar seguridad a toda la empresa lo cual conllevaba un gran esfuerzo al personal de sistemas realizar las configuraciones para asignar internet a determinado usuario así como también controlar que usuarios y que redes pueden tener acceso desde internet como hacia el internet, esto porque las configuraciones son manuales y directamente en los routers, lo cual se requería una persona con gran conocimiento de configuraciones sobre el router en cuanto a ACL y un profundo conocimiento de cómo esta conformada la red de PPR.

Por todo lo mencionado se busco una solución que permita realizar una configuración de una manera fácil y de una manera muy intuitiva, con un personal con conocimientos básicos en cuanto a configuraciones de conectividad, ruteo, filtrados y networking.
Para llegar a la herramienta con la cual se configurara toda la parte de seguridad, conectividad entre las redes internas de PPR y el internet se evaluó costo, licenciamiento, soporte, versiona miento, y sobre todo sea una solución completa en la cual contenga Firewall, Proxy, filtradores de Spam, filtradores de contenido WWW, Intruction Protection y antivirus para Correo Electrónico.

Una ves adquirida la solución que para PPR es Astaro Security 6.03 se realizo una renovación en cuanto a la conexión entre las redes Intranet y las Redes de Internet quedando de una manera centralizada la configuración y accesibilidad desde internet hacia PPR y desde la redes de Intranet hacia el Internet, quedando como se muestra en la Figura V.3.

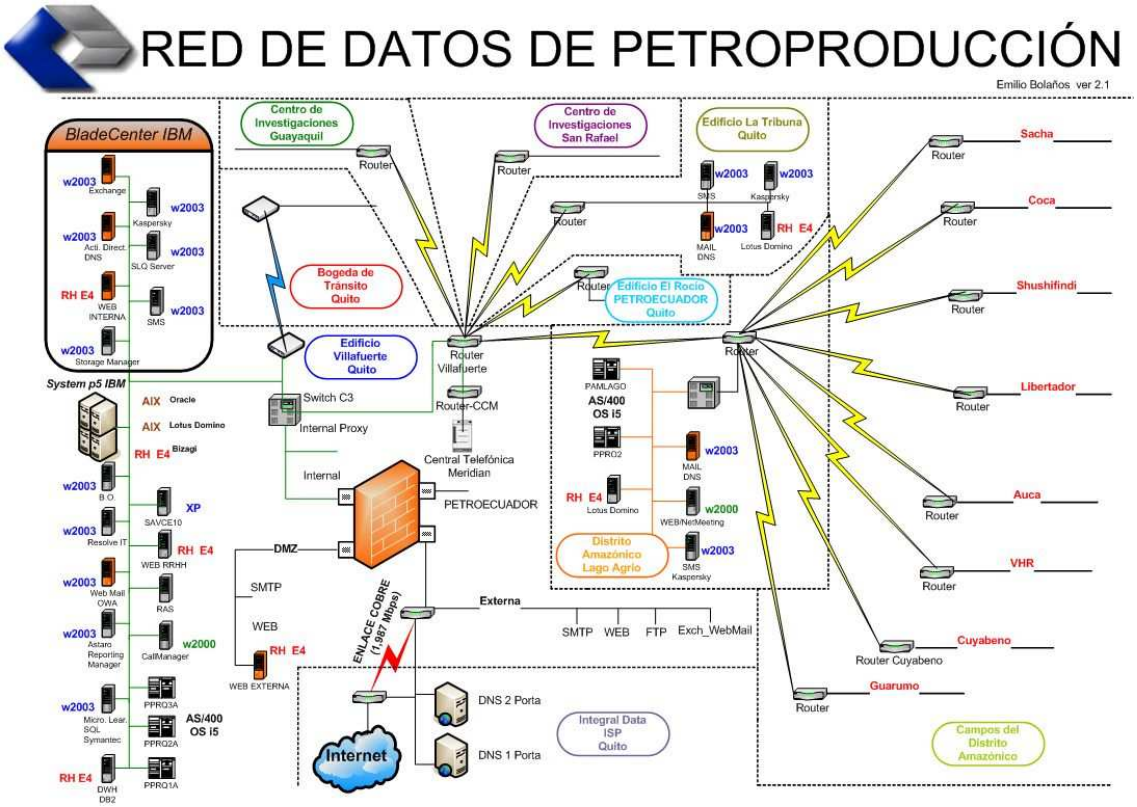


Figura V.3 Infraestructura de red con Conexión a Internet y desde Internet Anterior

Cualquier guía de seguridad ha de contemplar los elementos claves de seguridad ya mencionados: la Integridad, Disponibilidad, Privacidad y, adicionalmente, Control, Autenticidad y Utilidad

5.2.1 IDENTIFICACIÓN DE HARDWARE DE CONEXIÓN DEL PROVEEDOR DE INTERNET

Los dispositivos de conexión con el proveedor de internet (ISP) son el enlace de cobre el cual es conectado a un Patton Electronics modelo 552 desde este se conecta directamente a un Modem Tellabs 8110 y desde el modem se conecta directamente al Router Cisco 1700 y desde el se conecta a nuestro firewall Astaro. La configuración de estos equipos lo realiza el proveedor de internet (ISP), la información que llega hasta el Router puede ser de cualquier tipo hasta ahí no existe ningún tipo de bloqueo ni protección.

5.2.2 IDENTIFICACIÓN DEL ANCHO DE BANDA Y SERVICIOS DEL PROVEEDOR DE INTERNET

El enlace que proporciona el proveedor de internet es de un E1 que equivale a 2 Mbps para todo PETROPRODUCCION. Los servicios que facilita el proveedor son:

- Nombre de dominio para las aplicaciones web que están en el mundo.
- Un rango de 16 IPS públicas para la utilización que disponga PETROPRODUCCION.
- Una herramienta de monitoreo del enlace la cual se utiliza ingresando a una dirección de internet a través de Internet Explorer.

5.3 EVALUACIÓN DE RIESGOS

El análisis de riesgos supone más que el hecho de calcular la posibilidad de que ocurran cosas negativas.

- Se debe poder obtener una evaluación económica del impacto de estos sucesos. Este valor se podrá utilizar para contrastar el costo de la protección de la información en análisis, versus el costo de volverla a producir (reproducir).

- Se debe tener en cuenta la probabilidad que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.
- Se debe conocer qué se quiere proteger, dónde y cómo, asegurando que con los costos en los que se incurren se obtengan beneficios efectivos. Para esto se deberá identificar los recursos (hardware, software, información, personal, accesorios, etc.) con que se cuenta y las amenazas a las que se está expuesto.

La evaluación de riesgos y presentación de respuestas debe prepararse de forma personalizada para cada organización; pero se puede presentar algunas preguntas que ayudan en la identificación de lo anteriormente expuesto:

- "¿Qué puede ir mal?"
- "¿Con qué frecuencia puede ocurrir?"
- "¿Cuáles serían sus consecuencias?"
- "¿Se está preparado para abrir las puertas del negocio sin sistemas, por un día, una semana, cuánto tiempo?"
- "¿Cuál es el costo de una hora sin procesar, un día, una semana...?"
- "¿Cuánto, tiempo se puede estar off–line sin que los clientes se vayan a la competencia?"
- "¿Se tiene forma de detectar a un empleado deshonesto en el sistema?"
- "¿Se tiene control sobre las operaciones de los distintos sistemas?"
- "¿A que se llama información confidencial y/o sensitiva?"
- "¿La información confidencial y sensitiva permanece así en los sistemas?"
- "¿La seguridad actual cubre los tipos de ataques existentes y está preparada para adecuarse a los avances tecnológicos esperados?"
- "¿Quién es el propietario del recurso? y ¿quién es el usuario con mayores privilegios sobre ese recurso?"
- "¿Cómo se actuará si la seguridad es violada?"

Una vez obtenida la lista de cada uno de los riesgos se efectuará un resumen del tipo:

Tipo de Riesgo	Factor
Robo de hardware	Medio
Robo de información	Alto
Vandalismo	Medio
Fallas en los equipos	Medio
Virus Informáticos	Medio
Equivocaciones	Medio
Accesos no autorizados	Medio
Fraude	Bajo
Fuego	Muy Bajo
Terremotos	Muy Bajo

Tabla V.1 – Tipo de Riesgo–Factor

5.4 NIVELES DE RIESGO

Como puede apreciarse en la Tabla V.1, los riesgos se clasifican por su nivel de importancia y por la severidad de su pérdida:

1. Estimación del riesgo de pérdida del recurso (Ri)
2. Estimación de la importancia del recurso (Ii)

Para la cuantificación del riesgo de perder un recurso, es posible asignar un valor numérico de 0 a 10, tanto a la importancia del recurso (10 es el recurso de mayor importancia) como al riesgo de perderlo (10 es el riesgo más alto).

El riesgo de un recurso será el producto de su importancia por el riesgo de perderlo:

$$WRi = Ri * Ii$$

Luego, con la siguiente fórmula es posible calcular el riesgo general de los recursos de la red:

$$W_R = \frac{(WR_1 * I_1 + WR_2 * I_2 + \ldots + WR_n * I_n)}{I_1 + I_2 + \ldots + I_n}$$

Otros factores que debe considerar para el análisis de riesgo de un recurso de red son su disponibilidad, su integridad y su carácter confidencial, los cuales pueden incorporarse a la fórmula para ser evaluados.

Ejemplo: el Administrador de una red ha estimado los siguientes riesgos y su importancia para los elementos de la red que administra:

Recurso	**Riesgo (R_i)**	**Importancia (I_i)**	**Riesgo Evaluado (R_i*I_i)**
Router	6	7	42
Gateway	6	5	30
Servidor	10	10	100
PC’s	9	2	18

Tabla V.2 – Valuación de Riesgos

5.5 IDENTIFICACIÓN DE AMENAZA

Una vez conocidos los riesgos, los recursos que se deben proteger y como su daño o falta pueden influir en la organización es necesario identificar cada una de las amenazas y vulnerabilidades que pueden causar estas bajas en los recursos. Como ya se mencionó existe una relación directa entre amenaza y vulnerabilidad a tal punto que si una no existe la otra tampoco.

Se suele dividir las amenazas existentes según su ámbito de acción:

- Amenazas del sistema (Seguridad Lógica).
- Amenazas en la red (Comunicaciones).
- Amenazas de personas (Insiders–Outsiders).

Se debería disponer de una lista de amenazas (actualizadas) para ayudar a los administradores de seguridad a identificar los distintos métodos, herramientas y técnicas de ataque que se pueden utilizar. Es importante que los Administradores actualicen constantemente sus conocimientos en esta área, ya que los nuevos métodos, herramientas y técnicas para sortear las medidas de seguridad evolucionan de forma continua.

En la siguiente sección se explica una metodología para definir una estrategia de seguridad informática que se puede utilizar para implementar directivas y controles de seguridad con el objeto de aminorar los posibles ataques y amenazas. Los métodos se pueden utilizar en todos los tipos de ataques a sistemas, independientemente de que sean intencionados, no intencionados o desastres naturales.

La metodología se basa en los distintos ejemplos (uno para cada tipo de amenaza) y contempla como hubiera ayudado una guía de seguridad en caso de haber existido.

5.6 ESTRATEGIA DE SEGURIDAD

Para establecer una estrategia adecuada es conveniente pensar una guía de protección en los distintos niveles que esta debe abarcar y que no son ni más ni menos que los estudiados hasta aquí: Lógica, Humana y la interacción que existe entre estos factores.

En cada caso considerado, el plan de seguridad debe incluir una estrategia Proactiva y otra Reactiva.

La Estrategia Proactiva (proteger y proceder) o de previsión de ataques es un conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes.

En las directivas de seguridad y a desarrollar planes de contingencia. La determinación del daño que un ataque va a provocar en un sistema y las debilidades y puntos vulnerables explotados durante este ataque ayudará a desarrollar esta estrategia.

La Estrategia Reactiva (perseguir y procesar) o estrategia posterior al ataque ayuda al personal de seguridad a evaluar el daño que ha causado el ataque, a repararlo o a implementar el plan de contingencia desarrollado en la estrategia Proactiva, a documentar y aprender de la experiencia, y a conseguir que las funciones comerciales se normalicen lo antes posible.

Con respecto a la postura que puede adoptarse ante los recursos compartidos:

- Lo que no se permite expresamente está prohibido: significa que la organización proporciona una serie de servicios bien determinados y documentados, y cualquier otra cosa está prohibida.

- Lo que no se prohíbe expresamente está permitido: significa que, a menos que se indique expresamente que cierto servicio no está disponible, todos los demás sí lo estarán.

Estas posturas constituyen la base de todas las demás guías de seguridad y regulan los procedimientos puestos en marcha para implementarlas. Se dirigen a describir qué acciones se toleran y cuáles no.

Actualmente, y “gracias” a las, cada día más repetitivas y eficaces, acciones que atentan contra los sistemas informáticos los expertos se inclinan por recomendar la primera guía mencionada.

5.7 IMPLEMENTACIÓN

La implementación de medidas de seguridad, es un proceso Técnico–Administrativo. Como este proceso debe abarcar toda la organización, sin exclusión alguna, ha de estar fuertemente apoyado por el sector gerencial, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria.

Es fundamental no dejar de lado la notificación a todos los involucrados en las nuevas disposiciones y, darlas a conocer al resto de la organización con el fin de otorgar visibilidad a los actos de la administración.

Una guía informática deberá abarcar:

- Alcance de la guía, incluyendo sistemas y personal sobre el cual se aplica.
- Objetivos de la guía y descripción clara de los elementos involucrados en su definición.

5.7.1 CONTROL DE ACCESO

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

5.7.2 IDENTIFICACIÓN Y A UTENTIFICACIÓN

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos. Esta administración abarca:

1. Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y, de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación según corresponda.

2. Además, la identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.

3. Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos.

5.7.2.1 CONTROL DE ACCESO INTERNO

El acceso a Internet para los empleados de PETROPRODUCCION se administra a través de su dirección Ip por medio del Proxy que está incluido en el filtrador de contenidos Astaro Gateway 6.0 el cual contiene un esquema de usuarios con diferentes privilegios de acceso a Internet.

5.8 NORMAS DE USO DE LAS APLICACIONES DE PETROPRODUCCION

En PETROPRODUCCION el personal tiene acceso a aplicaciones tales como:

- Correo electrónico.
- As/400
- Web Interna
- Internet

Las aplicaciones aquí mencionadas cada una de ella conllevan una administración y seguridad para su ingreso, las mismas que día a día deben ser actualizadas para no tener constantes vulnerabilidades y ataques.

5.8.1 ¿CÓMO DEFENDERSE DE ATAQUES?

La mayoría de los ataques mencionados se basan en fallos de diseño inherentes a Internet (y sus protocolos) y a los sistemas operativos utilizados, por lo que no son "solucionables" en un plazo breve de tiempo.

La solución inmediata en cada caso es mantenerse informado sobre todos los tipos de ataques existentes y las actualizaciones que permanentemente lanzan las empresas desarrolladoras de software, principalmente de sistemas operativos.

Las siguientes son medidas preventivas. Medidas que toda red y administrador deben conocer y desplegar cuanto antes:

1. Mantener las máquinas actualizadas y seguras físicamente
2. Mantener personal especializado en cuestiones de seguridad (o subcontratarlo).
3. Aunque una máquina no contenga información valiosa, hay que tener en cuenta que puede resultar útil para un atacante, a la hora de ser empleada en un DoS coordinado o para ocultar su verdadera dirección.
4. No permitir el tráfico "broadcast" desde fuera de nuestra red. De esta forma evitamos ser empleados como "multiplicadores" durante un ataque Smurf.
5. Filtrar el tráfico IP Spoof.
6. Auditorias de seguridad y sistemas de detección.
7. Mantenerse informado constantemente sobre cada unas de las vulnerabilidades encontradas y parches lanzados. Para esto es recomendable estar suscripto a listas que brinden este servicio de información.

8. Por último, pero quizás lo más importante, la capacitación continúa del usuario.

5.8.2 PROTECCIÓN

Una vez conocidas las vulnerabilidades y ataques a las que está expuesto un sistema es necesario conocer los recursos disponibles para protegerlo. Mientras algunas técnicas son evidentes (seguridad física por ejemplo) otras pautas no lo son tanto e incluso algunas pueden ocasionar una sensación de falsa seguridad.
Muchas de las vulnerabilidades estudiadas son el resultado de implementación incorrecta de tecnologías, otras son consecuencias de la falta de planeamiento de las mismas pero, como ya se ha mencionado, la mayoría de los agujeros de seguridad son ocasionados por los usuarios de dichos sistemas y es responsabilidad del administrador detectarlos y encontrar la mejor manera de cerrarlos.

En el presente capítulo, después de lo expuesto y vistas la gran cantidad de herramientas con las que cuenta el intruso, es el turno de estudiar implementaciones en la búsqueda de mantener el sistema seguro.
Siendo reiterativo, ninguna de las técnicas expuestas a continuación representará el 100% de la seguridad deseado, aunque muchas parezcan la panacea, será la suma de algunas de ellas las que convertirán un sistema interconectado en confiable.

5.8.3 ADMINISTRACIÓN DE LA SEGURIDAD

Por regla general, las políticas son el primer paso que dispone a una organización para entrar en un ambiente de seguridad, puesto que reflejan su “voluntad de hacer algo” que permita detener un posible ataque antes de que éste suceda (proactividad). A continuación se citan algunos de los métodos de protección más comúnmente empleados.

- Sistemas de detección de intrusos: son sistemas que permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, sobre la base de la información con la que han sido previamente alimentados. Pueden considerarse como monitores.

- Sistemas orientados a conexión de red: monitorizan las conexiones que se intentan

establecer en una red o equipo en particular, siendo capaces de efectuar una acción sobre la base de métricas como: origen y destino de la conexión, servicio solicitado, permisos, etc. Las acciones que pueden emprender suelen ir desde el rechazo de la conexión hasta alerta al administrador. En esta categoría están los cortafuegos (Firewalls) y los Wrappers.

- Sistemas de análisis de vulnerabilidades: analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La "desventaja" de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que buscan acceso no autorizado al sistema.

- Sistemas de protección a la integridad de información: sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger. Algunos ejemplos son los programas que implementan algoritmos como Message Digest (MD5) o Secure Hash Algorithm (SHA), o bien sistemas que utilizan varios de ellos como PGP, Tripwire y DozeCrypt.

5.9. ANÁLISIS DE LA EVALUACIÓN

5.9.1 INFRAESTRUCTURA

La seguridad de la infraestructura se centra en cómo debe funcionar la red, los procesos comerciales (internos o externos) que debe favorecer, cómo se construyen y utilizan los hosts, y la administración y el mantenimiento de la red. La seguridad efectiva de la infraestructura puede ayudarle a mejorar significativamente la defensa de la red, cómo reaccionar ante un incidente, la disponibilidad de la red y el análisis de errores y fallas. Al establecer un diseño que todos puedan comprender y seguir, podrá identificar las áreas de riesgo y desarrollar métodos para reducir las amenazas. La evaluación revisa los procedimientos de alto nivel que una empresa puede seguir para mitigar los riesgos de la infraestructura centrándose en las siguientes áreas de seguridad:

- Defensa del perímetro: firewalls, antivirus, acceso remoto, segmentación
- Autenticación: políticas de contraseñas

- Administración y monitoreo: hosts de administración, archivos con la bitácora del uso
- Terminales de trabajo: configuración de la estructura

La infraestructura de red PETROPRODUCCION para la salida a Internet como para el ingreso desde Internet en la actualidad esta dada como se muestra en la Figura V.1.

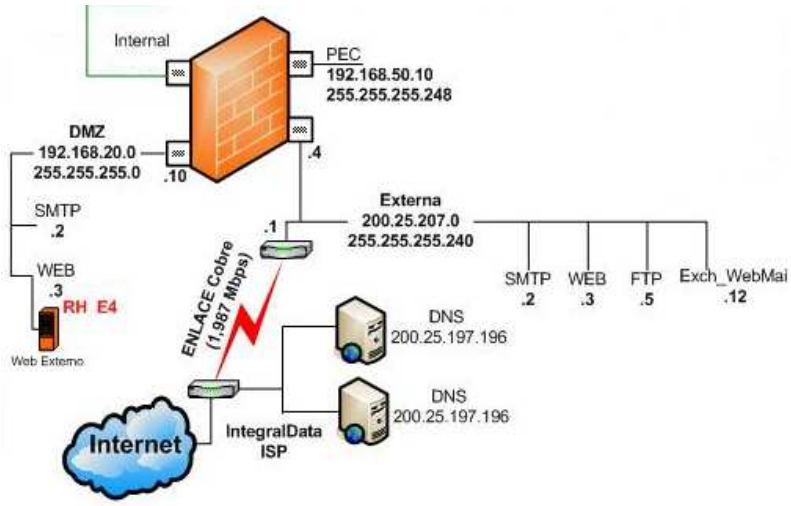


Figura V.4 Infraestructura de Red Conexión a Internet y desde Internet Actual

5.9.2 CONTROL DE ACCESO A INTERNET PARA PETROPRODUCCION.

Para el control de acceso a Internet Astaro Gateway 6.0 tiene un modulo Proxy en donde está configurado a que usuarios se les da el servicio de Internet y qué tipo de navegación pueden tener este control está basado en la dirección IP que se le asigno al computador del usuario, por lo cual se debe registrar el nombre del usuario ligado a la dirección IP que lleva el ordenador con el cual trabaja y podremos crear host, Network, DNS Hostname, grupos de Network de usuarios y de esta manera poder llevar una buena organización y control de usuarios, para la creación de usuarios y grupos de usuarios se debe ingresar a Definition-Network como se muestra en la Figura V.6.

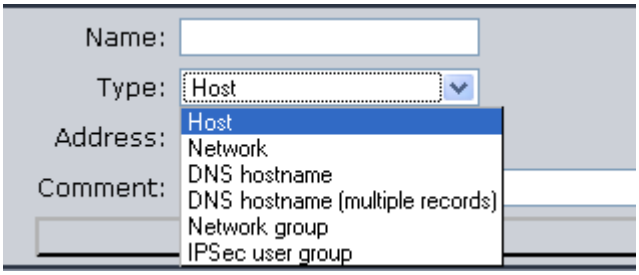


Figura V.6 Astaro Network Definition

Una vez registrados los usuarios, redes grupos de redes y usuarios debemos ingresar en Proxies-http y a habilitar la función de proxy como se muestra en la figura V.7.

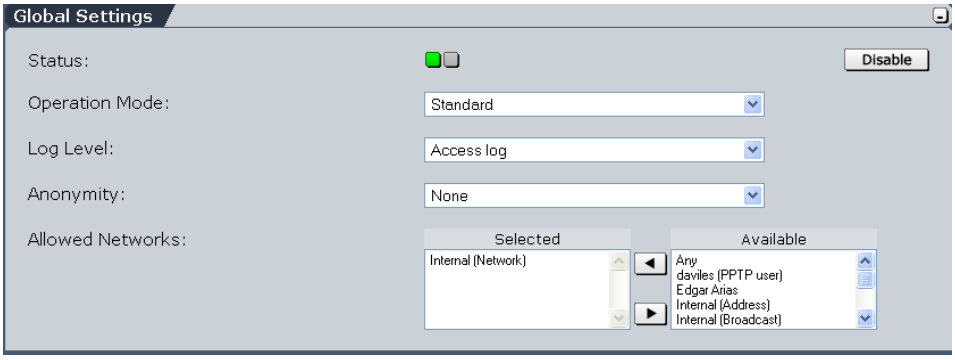


Figura V.7 Astaro Proxies http

Una ves habilitada el modulo de Proxy se configura el modo de operación el nivel de los log las redes permitidas para la salida a Internet, al terminar se debe crear y definir los filtros de navegación para PETROPRODUCCION se tiene una clasificación de usuarios como se muestra en la Figura V.8 además se tienen las listas blancas de dominios como las listas blancas y listas negras de páginas de navegación para cada una de las clasificaciones de usuarios.

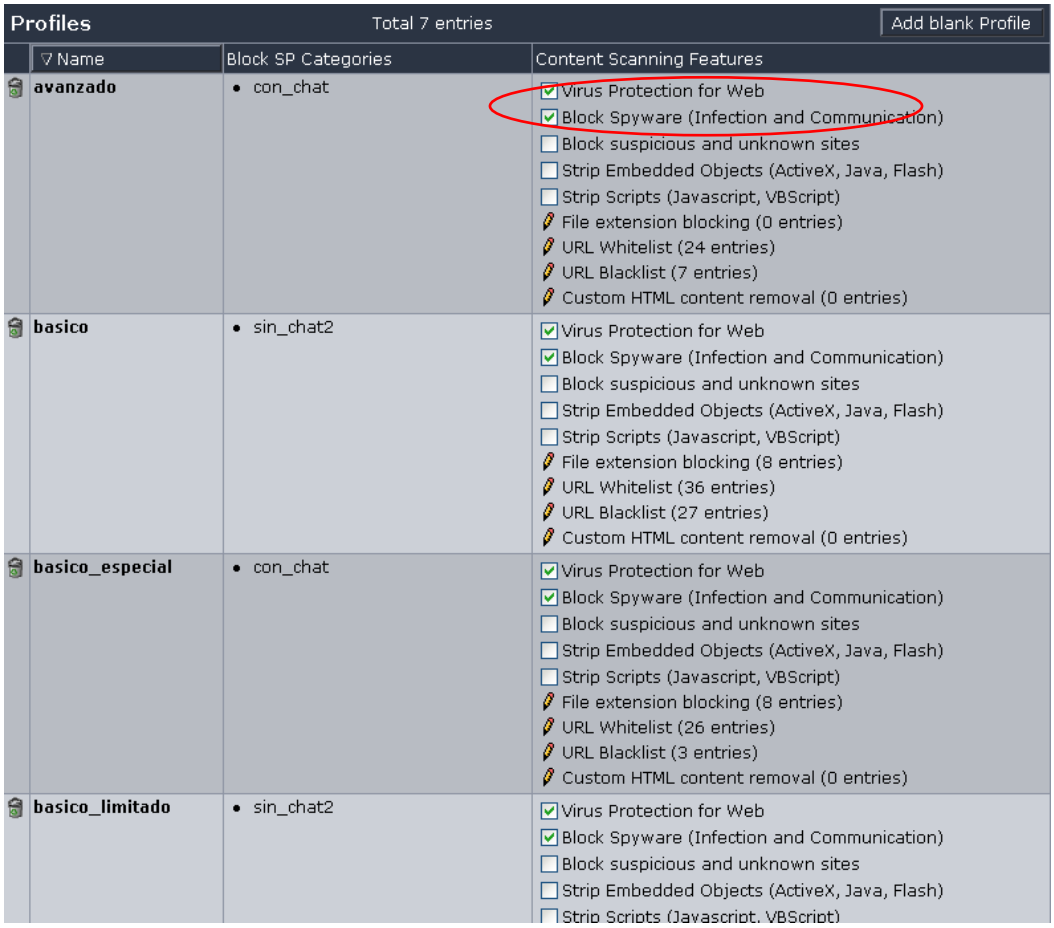


Figura V.8 Astaro Categoría de Usuarios

Cada categoría de usuario posee la posibilidad de habilitar el virus protection para la Web el bloqueo de spyware, sitios anónimos virus embebidos en Activex, Java, Flash, Javascript y VBScript, se puede bloquear archivos con extenciones tales como .mp3, .avi, .jpeg, .exe etc.

5.9.3 CONTROL DE CORREO ELECTRONICO

Para el control de correo electrónico Astaro Gateway 6.0 tiene un modulo Proxy SMTP en donde está configurado el nombre del hostname como la direccion de correo con la que se identificaran los correos que enviara Astaro Gateway 6.0, para la configuración debe ingresar a Proxies-SMTP donde se debe habilitar la opción de status y configurar los parámetros de Hostname, Postmasters Addres y Allow Relay from como se muestra en la Figura V.9.

Figura V.9 AstaroConfiguración de Proxies SMTP

El siguiente paso es de crear el dominio con el cual se van a identificar las cuentas de correo electrónico de todos los usuarios de PETROPRODUCCION y el tipo de verificaciones que realizara Astaro sobre el dominio creado está definido como se muestra en la Figura V.10

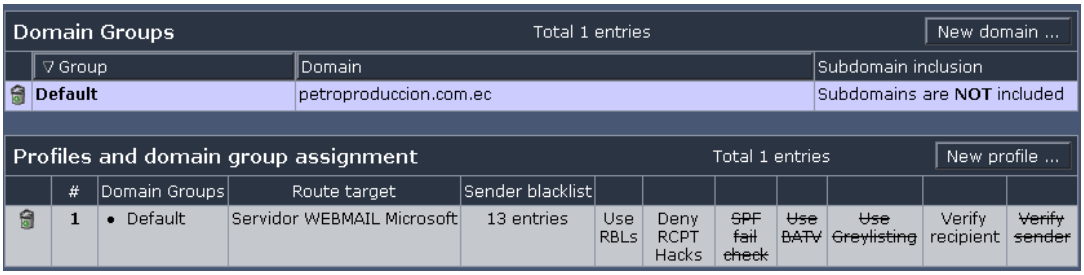


Figura V.10 Astaro Creación del Dominio de Correo Electrónico

El motor anti-spam de correo electrónicos no deseados usa heurística y verificaciones estadísticas, texto, HTML, y análisis sintáctico de URL así como ambas validación de título y cuerpo. Cada correo electrónico no deseados Astaro envía por correo electrónico incluye un hyperlink, y estos enlaces son verificados contra una base de datos central. Para mantener un alto a nivel de exactitud, los modelos fundamentales son actualizados a intervalos regulares.

Podemos establecer el rango de posibles spam y realizar una acción entre devolver, almacenar, en cuarentena, eliminarlo, enviarle una advertencia como un umbral que al ser superado tome las acciones mencionadas y podemos establecer las listas blancas de los dominios de correo electrónico como se puede ver en la Figura V.11.

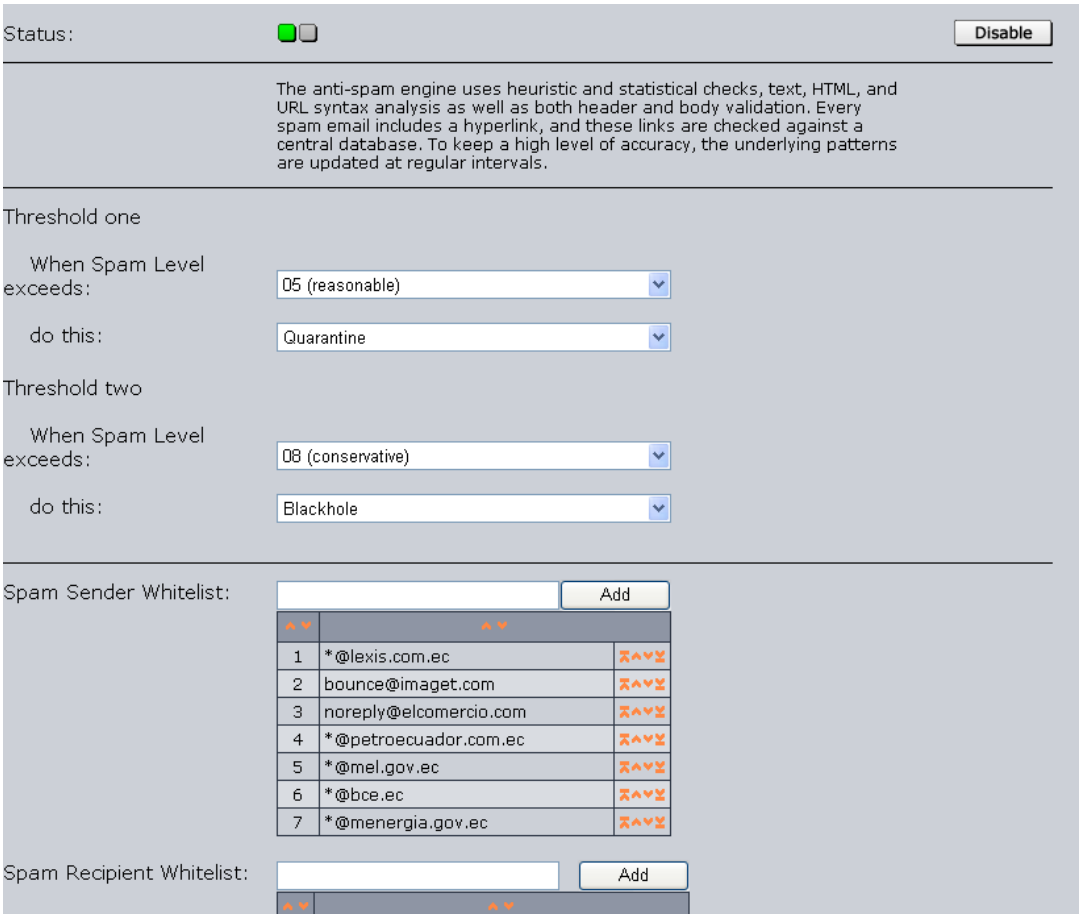


Figura V.11 Astaro Protección contra Spam

En la parte de configuraciones avanzadas podemos establecer el tamaño máximo de cada correo electrónico esto también debe estar configurado en el servidor de correo electrónico de Exchange y la activación de DOS Protección como se muestra en la Figura V.12

Figura V.12 Astaro Configuración Avanzada

5.9.4 INSTRUCTION PROTECTION

En la tabla se puede ver la lista completa de reglas para protección de intrusos. Existe un conjunto de reglas implícito que es actualizada en una base regular, y cualesquier

cambios/adiciones que se aplica aquí permanecerá después de una actualización de los reglamentos bajos. Las reglas son organizadas en grupos para proporcionar una mejor visión general. Inicialmente, verá la lista de grupos conjuntamente con una descripción corta. Al escoger un grupo específico usted verá más detalle

5.9.4.1 VISTA DE GRUPO

En este modo, que es la vista implícita, usted consigue una lista de todos los grupos actuales en el |ruleset|. Un grupo de cosa especial es también listado, nombrado "local". Si añade nuevas reglas, de forma automática serán creados en este grupo. El título de la tabla mostrará el número total de entradas. Puede ver también el número de entradas que son omitidas de la vista actual. La tabla contiene las columnas siguientes, de izquierda a derecha:

- Estatus: Puede inhabilitar o habilitar este grupo entero. Su selección es aplicada a todos los reglamentos de este grupo.
- Acción: Puede especificar si esta es una alarma (detección) o una gota (prevención) se agrupan. La acción escogida se aplica entonces a todos los reglamentos en el grupo.
- Vista: Haciendo clic en el icono de carpeta puede editar las colocaciones del individuo gobiernan dentro del grupo.
- El nombre del grupo: Nombre corto del grupo.
- Golpes: El número total de cuántos cronometran una regla de este grupo se aplicaba en realidad.
- Información: una descripción corta de este grupo.

Para ingresar a la vista de grupos de reglas de Intrusión Protection debe ingresar a Intrusión Protection-Rules como se muestra en la Figura V.13

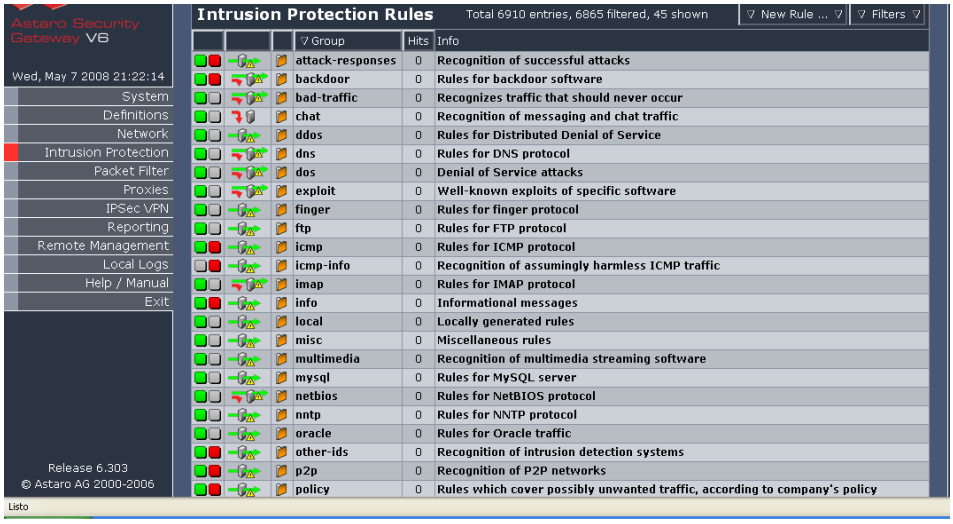


Figura V.13 Astaro Intrusión Protección Rules

5.9.4.2 VISTA DE REGLAS

En este modo consigue una lista de reglamento individual. Los reglamentos la vista pueden accederse por hacer clic sobre el icono de carpeta de cada grupo. La mesa contiene las columnas siguientes, de izquierda a derecho:

- Estatus: Puede inhabilitar o habilitar esta regla.
- Acción: Puede especificar si esta es una alarma (detección de entremetimiento) o una gota (prevención de entremetimiento) gobiernan.
- Vista: Haciendo clic

La vista de reglas de un grupo de reglas se ve como en la Figura V.14.

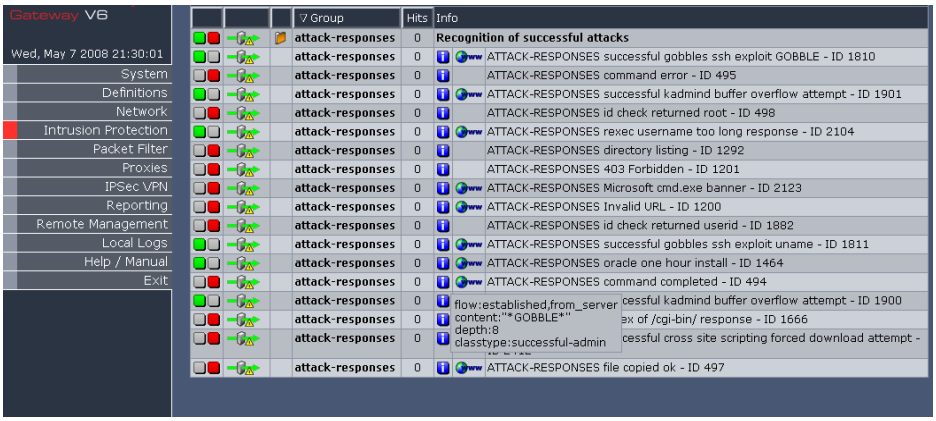


Figura V.14 Astaro Vista de Reglas de un grupo

5.9.5 PORTSCAN DETECTION

Esta pantalla le deja configurar las opciones generales del sistema Portscan Protection. Si un ataque alegado ejecuta un scan de anfitriones o servicios en su red, la característica de detección de |portscan| reconocerá este disparando una notificación sobre el evento, bloqueando de forma automática el ataque. Para habilitar esta función debemos configurar lo que se ve en la Figura V.15.

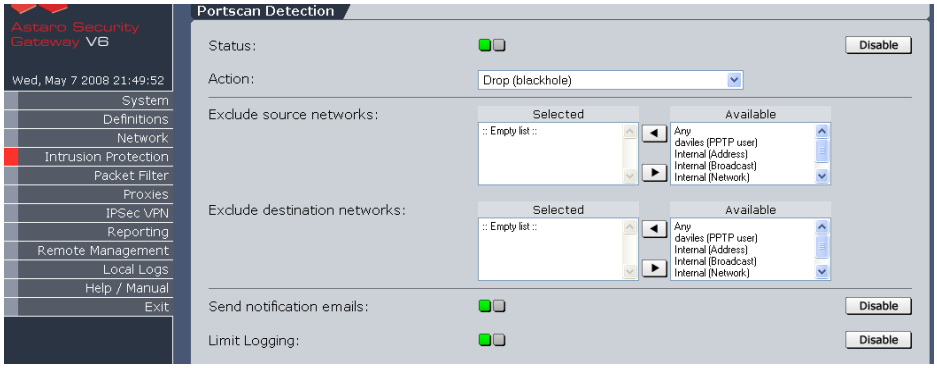
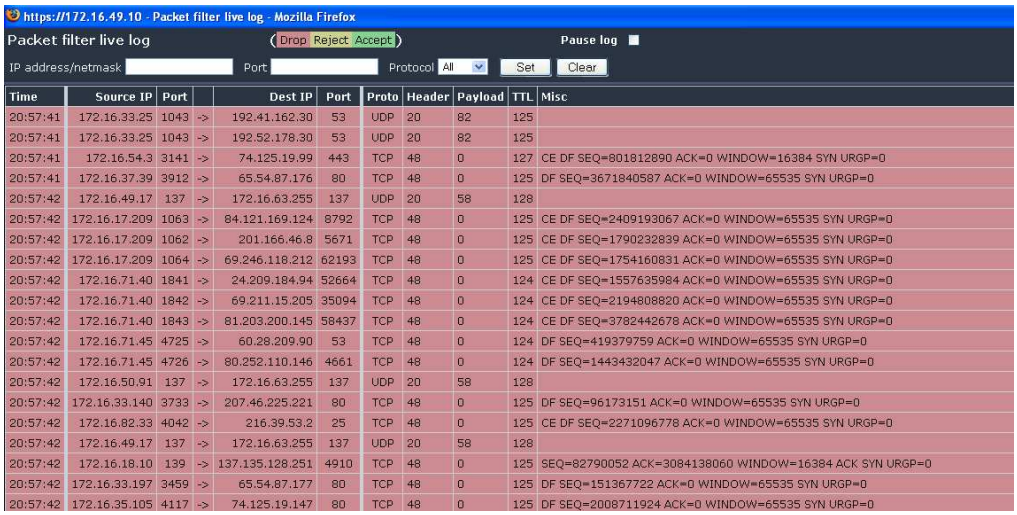


Figura V.15 Astaro Configuración de PortScan Detection

5.9.6 MONITORIZACIÓN DEL TRAFICO QUE INGRESA O SALE DE PETROPRODUCCION

Para poder monitorear el tráfico de datos que ingresa y sale de PETROPRODUCCION Astaro Gateway 6.0 cuenta con logs en línea los cuales nos ayudan para determinar trafico malicioso, así como también podemos determinar que personas de nuestra red intentan acceder a determinados servicios y puertos como se muestra en la Figura V.16



Time	Source IP	Port		Dest IP	Port	Proto	Header	Payload	TTL	Misc
20:57:41	172.16.33.25	1043	->	192.41.162.30	53	UDP	20	82	125	
20:57:41	172.16.33.25	1043	->	192.52.178.30	53	UDP	20	82	125	
20:57:41	172.16.54.3	3141	->	74.125.19.99	443	TCP	48	0	127	CE DF SEQ=801812890 ACK=0 WINDOW=16384 SYN URGP=0
20:57:41	172.16.37.39	3912	->	65.54.87.176	80	TCP	48	0	125	DF SEQ=3671840587 ACK=0 WINDOW=65535 SYN URGP=0
20:57:42	172.16.49.17	137	->	172.16.63.255	137	UDP	20	58	128	
20:57:42	172.16.17.209	1063	->	84.121.169.124	8792	TCP	48	0	125	CE DF SEQ=2409193067 ACK=0 WINDOW=65535 SYN URGP=0
20:57:42	172.16.17.209	1062	->	201.166.46.8	5671	TCP	48	0	125	CE DF SEQ=1790232839 ACK=0 WINDOW=65535 SYN URGP=0
20:57:42	172.16.17.209	1064	->	69.246.118.212	62193	TCP	48	0	125	CE DF SEQ=1754160831 ACK=0 WINDOW=65535 SYN URGP=0
20:57:42	172.16.71.40	1841	->	24.209.184.94	52664	TCP	48	0	124	CE DF SEQ=1557635984 ACK=0 WINDOW=65535 SYN URGP=0
20:57:42	172.16.71.40	1842	->	69.211.15.205	35094	TCP	48	0	124	CE DF SEQ=2194808820 ACK=0 WINDOW=65535 SYN URGP=0
20:57:42	172.16.71.40	1843	->	81.203.200.145	58437	TCP	48	0	124	CE DF SEQ=3782442678 ACK=0 WINDOW=65535 SYN URGP=0
20:57:42	172.16.71.45	4725	->	60.28.209.90	53	TCP	48	0	124	DF SEQ=419379759 ACK=0 WINDOW=65535 SYN URGP=0
20:57:42	172.16.71.45	4726	->	80.252.110.146	4661	TCP	48	0	124	DF SEQ=1443432047 ACK=0 WINDOW=65535 SYN URGP=0
20:57:42	172.16.50.91	137	->	172.16.63.255	137	UDP	20	58	128	
20:57:42	172.16.33.140	3733	->	207.46.225.221	80	TCP	48	0	125	DF SEQ=96173151 ACK=0 WINDOW=65535 SYN URGP=0
20:57:42	172.16.82.33	4042	->	216.39.53.2	25	TCP	48	0	125	CE DF SEQ=2271096778 ACK=0 WINDOW=65535 SYN URGP=0
20:57:42	172.16.49.17	137	->	172.16.63.255	137	UDP	20	58	128	
20:57:42	172.16.18.10	139	->	137.135.128.251	4910	TCP	48	0	125	SEQ=82790052 ACK=3084138060 WINDOW=16384 ACK SYN URGP=0
20:57:42	172.16.33.197	3459	->	65.54.87.177	80	TCP	48	0	125	DF SEQ=151367722 ACK=0 WINDOW=65535 SYN URGP=0
20:57:42	172.16.35.105	4117	->	74.125.19.147	80	TCP	48	0	125	DF SEQ=2008711924 ACK=0 WINDOW=65535 SYN URGP=0

Figura V.16 Astaro Monitoreo de Paquetes

5.9.7 REPORTES GENERADOS POR ASTARO GATEWAY 6.0

El reporte ejecutivo es una colección de los más importantes datos de presentación de informes, que puede enviarse por correo a las direcciones de correo electrónico escogidas diariamente. Para activar esta función, debemos ingresar al menos una dirección de correo electrónico en la lista. Puede También, mira y opcionalmente imprime un reporte actual haciendo clic sobre el botón Show en la caja de reporte actual. Hay que tener presente que el reporte generará sólo una vez todas las noches para mayor detalle del reporte los podemos ver en el **Anexo4**

CONCLUSIONES DE LA UTILIZACION DE LA GUIA

A partir de los resultados que se obtuvieron con la utilización de la guía para el control de brechas de seguridades en los servicios de internet y la utilización de Astaro Security Gateway 6.0 se puede decir que el resultante cumple con los objetivos expuestos anteriormente apoyando de manera correcta, el control de brechas de seguridad en los servicios de internet. Con base en la hipótesis de la presente tesis se puede concluir que efectivamente con la utilización de una guía se garantiza la optimización de los recursos cumpliendo un papel muy importante en el desempeño del personal de sistemas, así como brindar un mejor aseguramiento de los sistemas informáticos de Petroproducción.

NORMAS GENERALES DE SEGURIDAD

5.10 FIREWALLS

Defensa del perímetro	
Subcategoría	**Mejores prácticas recomendadas**
Reglas y filtros de firewall	Al crear las reglas para los firewalls y las listas de control de acceso (ACL) de los routers, céntrese en primer lugar en proteger los dispositivos de control de acceso y la red frente a posibles ataques. Asegúrese de que los datos sigan fluyendo mediante la utilización de ACL de red y las reglas para los firewalls. Compruebe el funcionamiento de las reglas para los firewalls y las ACL de los routers para determinar si las reglas contribuyen a ataques de negación de servicio (Denial of Service, DoS).

	Utilice uno o varios DMZ como parte del desarrollo sistemático y formal de firewalls. Sitúe en esa ubicación todos los servidores a los que se puede acceder por Internet. Limite la conectividad de los DMZ.
Recomendaciones	
Revise las políticas relativas a los firewalls con regularidad y elimine reglas obsoletas o inadecuadas. Implemente reglas que controlen el acceso de entrada y de salida, y considere poner en práctica filtros de salida para prevenir conexiones innecesarias. Limite el acceso de los usuarios internos a los segmentos DMZ, porque no es probable que éstos trabajen con los hosts del DMZ con frecuencia. Limite el acceso de la red central al segmento DMZ sólo a hosts específicos o redes administrativas.	
Recomendaciones	
Como una capa adicional de defensa, considere instalar firewalls basados en host en todos los servidores y piense también en emplear este software en todas las computadoras de escritorio y equipos portátiles de la empresa..	

5.10.1 ANTIVIRUS Y ACCESO REMOTO

Subcategoría	Mejores prácticas recomendadas
Antivirus	Utilice soluciones antivirus en todo el ambiente: tanto en los servidores como en las computadoras de escritorio. Utilice soluciones antivirus especializadas para tareas específicas, como detectores de virus para servidores de archivos, herramientas de análisis de contenido y detectores de carga y descarga de datos. Configure las soluciones antivirus para que detecten virus que entren o salgan del sistema. Estas soluciones deben instalarse primero en los servidores de archivos críticos y, a continuación, en los servidores de correo, de base de datos y de red. En el caso de las computadoras portátiles y de escritorio, debe implementar una solución antivirus en el ambiente predeterminado. Para Microsoft Exchange, utilice las funciones adicionales de antivirus y los filtros de contenido para los buzones de correo.
Subcategoría	**Mejores prácticas recomendadas**
Acceso remoto	Las terminales de trabajo son un elemento fundamental en la defensa de cualquier ambiente, sobre todo si hay usuarios remotos o itinerantes que se estén conectando. Herramientas como firewalls particulares, antivirus y software de acceso remoto son imprescindibles en todas las terminales, donde deberán configurarse correctamente. Ponga en práctica un procedimiento que exija una revisión periódica de estas herramientas para asegurarse de que la configuración refleje los cambios en las

	aplicaciones y los servicios usados y que, al mismo tiempo, garantice la solidez de la terminal de trabajo ante los ataques.

Recomendaciones
Revise con regularidad la lista de acceso de todos los usuarios en el dispositivo VPN. Considere administrar este dispositivo exclusivamente desde el interior de la red corporativa.

	Resultados	**Recomendaciones**
Acceso remoto	Se analizo que la VPN no puede limitar la conectividad para aislarla en cuarentena hasta que se realicen todas las comprobaciones de seguridad necesarias.	La mejor solución para mantener la integridad de los datos es tratar a la red inalámbrica como no segura y exigir que los usuarios utilicen VPN o tecnologías similares para conectarse a recursos corporativos; sin embargo, esto no evita que usuarios no autorizados puedan conectarse. Considere usar restricciones como la autenticación WPA y la dirección MAC para limitar el acceso a usuarios autorizados.

Subcategoría	**Mejores prácticas recomendadas**
Segmentación	Utilice segmentaciones para separar el acceso a extranet específicas para fabricantes, socios o clientes. Cada segmentación externa de la red debe permitir que el tráfico sólo se dirija a los hosts y puertos de aplicaciones determinadas que proporcionan servicios a los clientes. Asegúrese de que existan controles de red que permitan sólo el acceso necesario para cada conexión de terceros. Limite el acceso de los servicios de red suministrados, así como el acceso entre los segmentos de red.

Recomendaciones
Asegúrese de que los firewalls, la segmentación y los sistemas de detección de intrusos permitan proteger la infraestructura de la empresa de los ataques desde Internet. Siga empleando la segmentación de la red para mejorar la administración del tráfico de la red y limitar el acceso a los recursos en función de los requisitos del usuario.

Subcategoría	Mejores prácticas recomendadas
Usuarios de acceso remoto	Ponga en práctica controles de contraseñas complejas para todos los usuarios de acceso remoto, independientemente de si el acceso se concede mediante tecnologías de marcación telefónicas o VPN. Se considera que una contraseña es compleja si cumple estas condiciones: + Alfanumérica + Mayúsculas y minúsculas + Contiene al menos un carácter especial + Contiene como mínimo 8 caracteres
Recomendaciones	
Si aún no lo ha hecho, utilice un sistema de autenticación de factores múltiples de acceso remoto y limite el acceso únicamente a aquellos empleados que deban conectarse en forma remota por motivos laborales.	

Subcategoría	Mejores prácticas recomendadas
Sistema de detección de intrusos (IDS)	Los sistemas de detección de intrusos del host y de la red deben implementarse para detectar y notificar cualquier ataque que se produzca contra los sistemas corporativos.
Recomendaciones	
Siga implementando sistemas de detección de intrusos en la red. Asegúrese de que las definiciones de virus se mantengan actualizadas y averigüe sobre tecnologías de prevención de intrusiones a medida que estén disponibles.	

5.10.2 AUTENTIFICACIÓN

Autenticación	
Subcategoría	**Mejores prácticas recomendadas**
Usuarios administrativos	Ponga en práctica una política estricta para las cuentas administrativas mediante el uso de contraseñas complejas que cumplan estas condiciones: Alfanumérica Mayúsculas y minúsculas Contiene al menos un carácter especial Contiene como mínimo 12 caracteres Para limitar más los riesgos de ataques a las contraseñas, ponga en práctica los controles siguientes: Vencimiento de contraseñas Bloqueo de la cuenta después de entre 7 y 10 intentos de registro fallidos Registro del sistema Además de las contraseñas complejas, puede recurrir a la autenticación de factores

	múltiples. Utilice controles avanzados para la administración de las cuentas y el registro de acceso a las cuentas (no permita que se compartan cuentas).

5.10.3 ADMINISTRACIÓN Y CONTROL

Administración y control	
Subcategoría	**Mejores prácticas recomendadas**
Creación	Mantenga procesos de armado mediante los parches y configuraciones cerradas recomendadas del fabricante. Compruebe este proceso periódicamente. Utilice procedimientos para robustecer los hosts con el objeto de corregir y configurar correctamente los servicios y las aplicaciones de cada host. Desactive todos los servicios y las aplicaciones que no necesite. Deben robustecerse las terminales de trabajo instalando los parches recomendados, retirando también todos los paquetes y servicios que no sean necesarios y evaluando los permisos de los archivos. Incluya medidas de robustecimiento de los hosts en los procedimientos estándar de creación de terminales de trabajo.
Recomendaciones	
Elabore una estructura segura para cada tipo de estación. Actualícela con regularidad con los service pack más recientes, revisiones de emergencia y otras técnicas de robustecimiento.	

Subcategoría	**Mejores prácticas recomendadas**
Registros	Debe activar el archivo de registro en todas las aplicaciones del ambiente. Los datos de los archivos con la bitácora del uso son importantes para los análisis de incidentes, tendencias y auditorías. Las aplicaciones deben registrar los intentos de autenticación correctos e incorrectos, además de los cambios de datos de la aplicación, incluidas las cuentas de usuarios, los errores graves de la aplicación y los accesos correctos e incorrectos a los recursos. Cuando grabe datos en la bitácora de la aplicación, deberá evitar grabar información sensible en ésta.

Almacenamiento de datos y comunicaciones	
Subcategoría	**Mejores prácticas recomendadas**
Encripción	Los datos sensibles deben encriptarse o codificarse mediante hash en la base de datos y en el sistema de archivos. La aplicación debe diferenciar entre los datos que podrían estar expuestos a la divulgación y que deben encriptarse, los datos sensibles que podrían llegar a manipularse y para los que es necesario un valor de claves hash, y los datos que se pueden transformar irreversiblemente (hash) sin ninguna pérdida de funcionalidad, como las contraseñas. La aplicación debe guardar las claves para desencriptar datos en un lugar distinto al de la información encriptada. Los datos sensibles se deben encriptar antes de transmitirlos a otros componentes. Verifique que los componentes intermedios que controlan los datos en un formato de texto sin encripción, antes o después de la transmisión, no representan una amenaza indebida. La aplicación debe sacar partido de las funciones de autenticación disponibles con el mecanismo de transmisión segura. Algunos de los tipos de encripción más comunes y confiables son: 3DES, AES, RSA, RC4 y Blowfish. Utilice claves de 128 bits (1024 bits para RSA) como mínimo.

Ambiente	
Subcategoría	**Mejores prácticas recomendadas**
Protocolos y servicios	Documente los estándares normas y las prácticas donde se establecen los protocolos y servicios que permite la organización. Se deben verificar las listas de control de acceso para garantizar que los servicios permitidos tienen necesidades empresariales acordes con su nivel de acceso. Utilice direcciones IP y rangos de direcciones IP específicos donde sea posible. Limite los servicios de los servidores a los que necesita la empresa. En las pautas también se debe detallar aspectos específicos relativos a la versión de protocolo y la seguridad mínima de la encripción. Implemente el uso de protocolos establecidos con dispositivos del perímetro (como routers, gateways, firewalls, etc.), sistemas de autenticación segura y comunicaciones encriptadas.

5.10.4 ADMINISTRACIÓN DE ACTUALIZACIÓN DE PARCHES

Administración de actualizaciones y parches	
Subcategoría	**Mejores prácticas recomendadas**
Documentación de la red	Los diagramas actuales y precisos de las relaciones físicas y lógicas de las redes internas y externas tendrán que estar disponibles en todo momento.

	Actualice estos diagramas conforme se produzcan cambios en el ambiente. Limite el acceso a los diagramas a sólo el equipo de TI.
Recomendaciones	
Revise la política sobre actualizaciones de los diagramas de red. Si hubiera una política de control de cambios para la red, incluya actualizaciones de los diagramas como paso formal. Asegúrese de que los diagramas más recientes estén disponibles sólo a un grupo limitado de empleados, principalmente los equipos de TI y de seguridad.	

Subcategoría	**Mejores prácticas recomendadas**
Administración de parches	Los parches de seguridad y cambios de configuración se deben aplicar en forma oportuna (según lo dispuesto en la política de seguridad de la empresa) cuando estén disponibles. Estos parches y actualizaciones se deben comprobar exhaustivamente en un ambiente de laboratorio antes de instalarlos definitivamente, independientemente de que se hayan desarrollado en la empresa o por terceros. Por otra parte, una vez instalado el parche, se debe probar cada uno de los sistemas para detectar conflictos específicos que podrían significar tener que desinstalar el parche. Debe clasificar los sistemas para permitir una programación basándose en agrupaciones: los sistemas críticos y los que tienen más tráfico tienen preferencia a la hora de aplicar los parches.
Subcategoría	**Mejores prácticas recomendadas**
Definición de virus	Visite regularmente los sitios de los fabricantes para obtener actualizaciones de definiciones de virus y descárguelas en un sitio aislado para probarlas en un ambiente de laboratorio. Verifique que las actualizaciones no causan problemas con ningún sistema operativo ni aplicaciones antes de utilizarlas. Debe desactivar las funciones de actualización automática de las soluciones antivirus en todos los sistemas para evitar el uso de archivos potencialmente peligrosos antes de probarlos. Puede utilizar una consola central para las aplicaciones antivirus y así facilitar la creación de informes sobre los sistemas obsoletos o con funciones de software desactivadas. Para los usuarios remotos que no se conectan regularmente a la red de la empresa, puede usar la función de actualización automática.
Subcategoría	**Mejores prácticas recomendadas**

Medios de copia de respaldo	Deben seguirse políticas detalladas relativas al almacenamiento y la manipulación de los dispositivos de copias de respaldo. Estas políticas deben abordar temas como: Almacenamiento en las instalaciones o fuera de ellas Rotación de los medios Controles de seguridad Controles de acceso para empleados Los dispositivos extraíbles para copias de respaldo deben almacenarse en armarios cerrados, a prueba de fuego, a los que sólo tengan acceso empleados autorizados. El almacenamiento fuera de las instalaciones debe usarse como sistema adicional para recuperar datos en caso de que producirse algún desastre.

5.10.5 REQUISITOS Y EVALUACIONES

Requisitos y evaluaciones		
Subcategoría	**Mejores prácticas recomendadas**	
Requisitos de seguridad	La empresa debe identificar a individuos con experiencia en el campo de la seguridad para incluirlos en todas las reuniones y decisiones relativas a este tema. Además, debe señalar qué debe protegerse, teniendo en cuenta el valor del recurso y el nivel de seguridad que se requiere. El análisis incluye todas las amenazas posibles. La estrategia desarrollada debe equilibrar los costos y los beneficios de las protecciones, e incluir como opciones el traslado o la aceptación de los riesgos. Los requisitos de seguridad, definidos por representantes comerciales y técnicos, se deben documentar y publicar para que todo el personal los pueda consultar y usar en diseños futuros. Las diferencias entre los tipos de aplicaciones y tipos de datos pueden dar como resultado requisitos finales diferentes.	
	Resultados	**Recomendaciones**
Requisitos de seguridad	No hay ningún individuo ni equipo de seguridad que desempeñe un papel fundamental en la definición de los requisitos de seguridad dentro de la empresa.	Considere asignar a una persona con experiencia en soluciones de seguridad la definición de los requisitos de seguridad para las tecnologías utilizadas en el ambiente. Es importante que los requisitos sean obligatorios para todas las iniciativas tecnológicas. El equipo de seguridad toma parte en todos los aspectos del desarrollo y utilización de tecnologías, desde la fase inicial de planificación y diseño hasta del desarrollo, la utilización y las pruebas. Se deben establecer requisitos claros para las especificaciones de funcionamiento.

	Resultados	Recomendaciones
Requisitos de seguridad	El equipo de seguridad no participa en la fase de planificación y diseño del ciclo de vida de la tecnología.	El equipo de seguridad debe participar en todas las fases del ciclo de vida de la tecnología, para todos los proyectos.
	Resultados	**Recomendaciones**
Requisitos de seguridad	No hay responsabilidades ni roles definidos para las personas encargadas de la seguridad de la información.	Para poder tener capacidad de respuesta ante incidentes de forma rápida, eficaz y organizada, todos los roles y responsabilidades deben definirse para cada miembro del equipo de seguridad encargado de los datos.
Subcategoría	**Mejores prácticas recomendadas**	
Evaluaciones de seguridad	Las evaluaciones por parte de terceros aportan una perspectiva objetiva muy valiosa para las medidas de seguridad de una empresa. Estas evaluaciones también podrían resultar beneficiosas para cumplir las estipulaciones legales y los requisitos de los clientes, socios y fabricantes. Las evaluaciones deben incluir la infraestructura, las aplicaciones, las políticas y los procedimientos de auditoría. Estas evaluaciones no deben centrarse exclusivamente en la identificación de vulnerabilidades, sino también en señalar configuraciones que no sean seguras o privilegios de acceso externo. Se deben revisar las políticas y los procedimientos de seguridad para descubrir faltas.	
Subcategoría	**Mejores prácticas recomendadas**	
Formación sobre seguridad	Un programa formal de formación sobre las medidas de seguridad ayuda a los empleados a contribuir a la seguridad global de la empresa, puesto que se les mantiene informado acerca de los riesgos existentes. La mejor garantía de alerta ante problemas potenciales es informar debidamente al personal en materia de seguridad. Un programa de formación eficaz debe incluir todos los aspectos relacionados con la seguridad (aplicaciones, redes y medios físicos), a la vez que debe proporcionar pautas sencillas para que los empleados sepan cómo actuar ante una posible señal de alerta. Ponga en práctica políticas para regular el uso de los recursos corporativos por parte de los empleados. Los programas de formación deben ser parte del curso de orientación de empleados nuevos. Se debe proporcionar información actualizada y cursos para asegurar que todos los empleados conozcan las prácticas y los riesgos más recientes. Se deben realizar comprobaciones periódicas para asegurarse de que los empleados han asimilado la información.	

Subcategoría	Mejores prácticas recomendadas
Relaciones con terceros	Con el objeto de reducir el riesgo de divulgación de datos, deben implementarse políticas y procedimientos formales enfocados a las relaciones con terceros. De esta forma, se podrá detectar cualquier problema de seguridad y la responsabilidad de cada parte a la hora de solucionarlo. Dichas políticas deben incluir: + El nivel de conectividad y acceso + La presentación y la manipulación de los datos + El cargo y las responsabilidades (incluida la autoridad) de cada parte + La administración de la relación: creación, mantenimiento y término.

COCLUSIONES

- La utilización de una guía para el control de brechas de seguridad en los servicios de internet logro optimizar el control se quien y que servicios están disponibles a ser utilizados por usuarios de Petroproducción y usuarios que no son parte de la Petroproducción.

- Con la utilización de la guía facilita la creación de políticas y normas a seguir para la implementación de sistemas de seguridad informática.

- Mediante la implantación de los sistemas informáticos dedicados a seguridad informática como. Astaro Gateway y System Management Server 2003 (SMS), para el control de brechas de seguridad en servicios de Internet, se obtiene un mejor aseguramiento del entorno informático así como también permitió optimizar el tiempo y recursos de la empresa Petroproducción, logrando de esta manera una mayor eficiencia y eficacia.

- El amplio desarrollo de las nuevas tecnologías informáticas, permiten a las empresas mejorar sus sistemas de control, minimizando el riesgo de ingreso a bases de datos e información confidencial a personal no autorizado, garantizando de esta manera la integridad corporativa de la empresa, todo esto mediante la proactividad del personal que integra el departamento de sistemas de la organización.

- Para prevenir, principalmente, el daño y/o pérdida de la información que en última instancia es el conocimiento con que se cuenta, debido a que consideran como un gasto el invertir en sistemas de seguridad y capacitación al personal, lo que es contrario a la realidad ya que se debe considerar como una inversión más no como un gasto ya que mediante sistemas actualizados y un personal capacitado se lograra eficiencia en la organización, y por ende optimización de recursos.

RECOMENDACIONES

- Se recomienda la aplicación sistematizada de los programas Astaro y System Management Server 2003 (SMS), como medida de seguridad en el entorno informático ya que permiten mejorar la seguridad informática en los servicios de Correo Electrónico, Internet, y FTP en la empresa PETROPRODUCCION.

- Debido a los constantes cambios y avances tecnológicos, se recomienda a la empresa PETROPRODUCCIÓN, innovación constante en los sistemas de seguridad informáticos, por ende impulsar a la empresa a que sea proactiva y se anticipe a los problemas.

- Realizar capacitaciones al personal de seguridad sobre las nuevas tecnologías, normas, metodologías de seguridad informática por lo menos una vez al año.

- Revisar periódicamente los listados de actualizaciones para las aplicaciones y sistemas operativos Microsoft para poder actualizar los ordenadores y servidores con la finalidad de cerrar las vulnerabilidades de los mismos.

- Realizar monitoreo constante de el trafico de navegación de internet como el trafico de navegación intranet, con el fin de conocer cuáles son los servicios más utilizados que consumen recursos de red.

RESUMEN

Se desarrolló un estudio sobre los mecanismos de seguridad sobre las plataformas de Astaro Security Gateway 6.0 y SMS SP2 para la implementación de una guía para el control de brechas de seguridad en los servicios de internet aplicada a PETROPRODUCCION la cual garantiza una mejor seguridad para todas las aplicaciones y conexiones que utilizan los servicios de Internet.

De acuerdo al estudio realizado y mediante los parámetros de comparación Seguridad, Integridad, Disponibilidad, Confidencialidad, Autenticación y Confiabilidad se determinó que el mejor mecanismo de seguridad es la utilización un aplicativo que contenga la mayor gama de elementos de seguridad por lo cual se opto el uso de Astaro Security Gateway 6.0. Para la implementación y pruebas de funcionalidad se instalo Astaro Security en una maquina virtual con una licencia de tiempo limite de y para 10 Pcs donde cada uno de estas fueron configuradas para que tengan acceso a internet para luego realizar la captura de los paquetes mediante el software de Astaro para realizar el respectivo análisis de comparación de la información obtenida.

Se recomienda utilizar Astaro Security Gateway 6.0. Ya que gracias a este tipo de aplicación se logrará reducir las diferentes amenazas que utilizan los servicios más utilizados como el Correo Electrónico, navegación por HTTP, FTP que día a día aparecen.

SUMMARY

A study on the security devices on the platforms ofAstaro Security Gateway 6.0 and SMS SP2 to ¡mplement a guide for the control of security gaps ¡n the internet services applied to PETROPRODUCCION which guarantses a better security for all the applications and connections using the internet services.

According to the study and through the comparison parameters Security, Integrity , Availability, Confidence , Authentication and Reliability it was determined that the best security device is the use of a component containing the widest range of security elements ; this is why the Astaro Security Gateway 6.0 use was selected.

For the implementation and functionality tests the Astaro Security was installed in a virtual machine with a limit time licence of and for 10 Pcs where each one of these were configured to access to the internet to , then, carry out the capture of the packages through the Astaro software os as to perform the corresponding analysis of information comparison.

It is recommended to use the Astaro Security Gateway 6.0 as thanks to this application type it will be possible to reduce the different threats using the most used services such as the Electronic Mail, Surfing by HTTP, FTP which appear everyday.

ANEXOS

ANEXO 1.

Para entender el procedimiento supongamos la siguiente situación:

IP Cliente: IP 195.1.1.1
IP Servidor: IP 195.1.1.2
IP Atacante: IP 195.1.1.3

1. El cliente establece una conexión con su servidor enviando un paquete que contendrá la dirección origen, destino, número de secuencia (para luego armar el paquete) y un número de autentificación utilizado por el servidor para "reconocer" el paquete siguiente en la secuencia. Supongamos que este paquete contiene:
   IP Origen: 195.1.1.1 Puerto 1025
   IP Destino: 195.1.1.2 Puerto 23
   SEQ = 3DF45ADA (el primero es al azar) ACK = F454FDF5
   Datos: Solicitud

2. El servidor, luego de recibir el primer paquete contesta al cliente con paquete Hecho (recibido).

   IP Origen: 195.1.1.2 Puerto 1025
   IP Destino: 195.1.1.1 Puerto 23
   SEQ = F454FDF5 (ACK enviado por el cliente) ACK = 3DF454E4
   Datos: Recepción OK (Echo)

3. El cliente envía un paquete ACK al servidor, sin datos, en donde le comunica lo "perfecto" de la comunicación.
   IP Origen: 195.1.1.1 Puerto 1025

IP Destino: 195.1.1.2 Puerto 23
SEQ = 3DF454E4 (ACK enviado por el servidor) ACK = F454FDFF
Datos: Confirmación de Recepción (ACK)

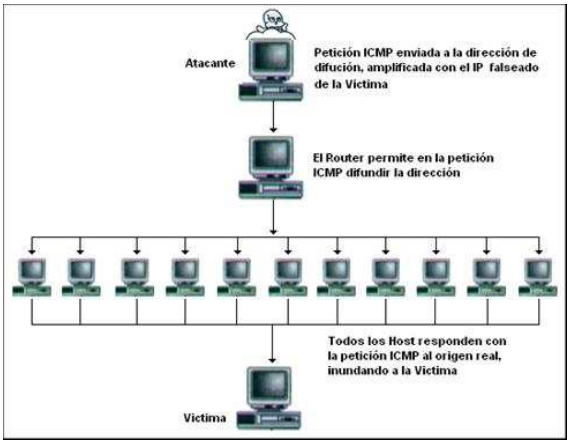
4. El atacante que ha visto, mediante un Sniffer, los paquete que circularon por la red calcula el número de secuencia siguiente: el actual + tamaño del campo de datos. Para calcular el tamaño de este campo:
   1° Paquete ACK Cliente = F454FDF5
   2° Paquete ACK Cliente = F454FDFF
   Tamaño del campo datos = F454FDFF – F454FDF5 = 0A

5. Hecho esto el atacante envía un paquete con la siguiente aspecto:
   IP Origen: IP 195.1.1.1
   IP del Cliente por el atacante
   IP Destino: IP 195.1.1.2
   IP del Servidor
   SEQ = 3DF454E4 (Ultimo ACK enviado por el Cliente) ACK = F454FE09 (F454FDFF + 0A)

El servidor al recibir estos datos no detectará el cambio de origen ya que los campos que ha recibido como secuencia y ACK son los que esperaba recibir. El cliente, a su vez, quedará esperando datos como si su conexión estuviera colgada y el atacante podrá seguir enviando datos mediante el procedimiento descripto.

ANEXO 2.

Este paquete maliciosamente manipulado, será repetido en difusión (Broadcast), y cientos ó miles de hosts mandarán una respuesta a la víctima cuya dirección IP figura en el paquete ICMP.
Gráficamente:



Suponiendo que se considere una red de tipo C la dirección de BroadCast sería .255; por lo que el “simple” envío de un paquete se convierte en un efecto multiplicador devastador. Desgraciadamente la víctima no puede hacer nada para evitarlo. La solución está en manos de los administradores de red, los cuales deben configurar adecuadamente sus Routers para filtrar los paquetes ICMP de petición indeseada (Broadcast); o bien configurar sus máquinas para que no respondan a dichos paquetes. Es decir, que lo que se parchea son las máquinas/redes que puedan actuar de intermediarias (inocentes) en el ataque y no la máquina víctima.

También se podría evitar el ataque si el Router/Firewall de salida del atacante estuviera convenientemente configurado para evitar Spoofing. Esto se haría filtrando todos los paquetes de salida que tuvieran una dirección de origen que no perteneciera a la red interna.

ANEXO3

Listado de servidores y Hardware Compatible.

El propósito de esta lista es darle cierta ayuda e información sobre el hardware para ser usado con Astaro Security Linux. Nosotros suba de precio si usted contribuye para este dominado y pueda darnos realimentación. Por favor, envie su correo electrónico para hardware@astaro.com.

Nota introductoria:

Habrá normalmente ningunos problemas con los |harddisks| detectores, CPU y los |motherboards| al instalar el cortafuego. Para ayudarle decidiendo que El Ethernet (10/100/1000 Mbit), DIRIJA ATAQUES SORPRESIVOS CONTRA y dispositivos de controlador de SCSI usted puede use, hemos compilado una lista de compatibilidad de hardware, donde algunos recomiende el hardware es listado y donde adicionalmente cierta ayuda es dió con respecto a recomendar hardware.

La lista de controladores sostenidos y sin apoyo el T = "ensayado" con Astaro Security Linux 6.1: soportamos éstos controladores la e = " esperó para trabajar ": esperamos que estos controladores trabajan, pero nosotros hicimos no examinó esos, ni haga hicimos recibimos los reportes eso esos controladores trabajan - > irando hacia adelante para su contribución la u = "sin apoyo": nosotros o un cliente ha examinado y no trabaja la h = |linkbeat| puede verificarse para arriba Availibility la v = apoyo de VLAN

* = Este servidor usa el software dirige ataques sorpresivos contra. Astaro Security Linux no puede manejar este tipo especial de emuló dirija ataques sorpresivos contra. En este caso, Astaro Security Linux detecte dos Harddrives.

```
-Compaq-------------------------------------------------------------
--------|
HP COMPAQ DL 320 (G2) P III  1,26 GHz  SCSI HDD 36GB
|
-------------------------------------------------------------------
--------|
HP COMPAQ DL 320 (G3) P III  1,26 GHz  SCSI HDD 36GB
|
```

```
--------------------------------------------------------------------
--------|
HP COMPAQ ML 330 (G2) Xeon 2,4 GHz    Smart Array 5i or 532, SCSI-HDD
36GB    |
--------------------------------------------------------------------
--------|
HP COMPAQ ML 350 (G2) Xeon 2,4 GHz    Smart Array 5i or 532, SCSI-HDD
36GB    |
--------------------------------------------------------------------
--------|
HP COMPAQ ML 370 (G2) Xeon 2,8 GHz    Smart Array 5i or 532, SCSI-HDD
36GB    |
--------------------------------------------------------------------
--------|
HP COMPAQ ML 330 (G3) Xeon 2,4 GHz    Smart Array 5i or 532, SCSI-HDD
3*72GB  |
--------------------------------------------------------------------
--------|
HP COMPAQ ML 350 (G3) Xeon 2,4 GHz    Smart Array 5i or 532, SCSI-HDD
3*72GB  |
--------------------------------------------------------------------
--------|
HP COMPAQ ML 370 (G3) Xeon 2,8 GHz    Smart Array 5i or 532, SCSI-HDD
3*72GB  |
--------------------------------------------------------------------
--------|
HP COMPAQ DL 360 (G3),2*Xeon 3,0 GHz  Smart Array 5i/6i Raid 0/1 SCSI
2*72GB  |
--------------------------------------------------------------------
--------|
HP COMPAQ DL 360 (G4),2*Xeon 3,0 GHz  Smart Array 5i/6i Raid 0/1 SCSI
2*72GB  |
--------------------------------------------------------------------
--------|
HP/COMPAQ DL 380 (G3) 2*Xeon 2,8 GHz  Smart Array 5i+, HDD 2*72GB
|
--------------------------------------------------------------------
--------|
HP/COMPAQ DL 380 (G4) 2*Xeon 3,2 GHz  Smart Array 6i+, HDD 36GB (Raid)
|
--------------------------------------------------------------------
--------|

-Dell---------------------------------------------------------------
--------|
DELL PowerEdge 420SC,  2,53 GHz Intel Celeron, SATA-HDD 160GB, C3
Software    |
                       Raid*, Onboard NIC 10/100/1000 Broadcom
|
--------------------------------------------------------------------
--------|
DELL PowerEdge 430SC,  2,8 GHz Intel Pentium 4 HT, 512 MB RAM, SATA
80GB,     |
                       Onboard NIC DELL 10/100/1000
|
--------------------------------------------------------------------
--------|
DELL PowerEdge 750, 2,8 GHz, 1GB RAM, the CERC/PERC 1.5 6 channel PCI
|
```

```
                    SATA RAID card (Bios v4.1-0, build 7403), 2x 73 GB
HDD    |
-------------------------------------------------------------------------
--------|
DELL PowerEdge 1425SC,Dual 3,2 GHz XEON, 2xSATA-HDD 40 GB RAID 1,
|
                       2x onboard NIC 10/100/1000 Intel
|
                  Raid Controller Cerc SATA 2S V.2.1-11 2026
|
-------------------------------------------------------------------------
--------|
DELL PowerEdge 1600SC,Dual 2,8 GHz XEON, IDE-HDD 80GB, Onboard NIC
10/100/1000|
-------------------------------------------------------------------------
--------|
DELL PowerEdge 1750, 2,8 GHz XEON, 2xSCSI-HDD 36GB, 2xOnboard NIC
10/100/1000 |
                       Raid Controller Perc 4/Di Rev. 4.12W
|
-------------------------------------------------------------------------
--------|
DELL PowerEdge 1850, Dual 2,8 GHz XEON, PERC 4e/Si SCSI RAID
Controller,      |
                       onboard Intel 82541GI/PI (10/100/1000)
|
-------------------------------------------------------------------------
--------|
DELL PowerEdge 2650, 2,8 GHz XEON, SCSI-Raid1 36GB, Onboard NIC 3x
10/100/1000|
                       Raid Controller Perc 3/Di (only the LSI Version)
|
                   Dell has two Models for the Perc 3/Di
|
                   LSI        Device: pci 0x0013
|
                   Adaptec    Device: pci 0x00a
|
-------------------------------------------------------------------------
--------|
DELL PowerEdge 2850, 3.6 GHz XEON, SCSI-Raid5 3x 73GB, Onboard NIC
10/100/1000|
                       Raid Controller Perc 4/DC
|
-------------------------------------------------------------------------
--------|

-Hitachi---------------------------------------------------------------
--------|
GSA110DA-CN1CN30, P4 3,0 GHz, 2xSATA-HDD 120GB, Onboard NIC 1x 10/100,
|
                    1x 10/100/1000, (SATA controller 6300ESB will only
work in  |
                    legacy mode)
|
-------------------------------------------------------------------------
--------|
```

-Nexcom---
--------|
EBS1563, VIA CPU 800 MHz, 256 MB SDRAM, 3xIntel 10/100 MBit, 20 GB HDD
|

--------|
NSA1080, Intel PIII 1,2 GHz, 512 MB SDRAM, 8xIntel 10/100 MBit, 20 GB
HDD |

--------|
NSA1080, Intel P4 2,8 GHz, 1024 MB DDR, 40 GB HDD, 8xIntel 10/100
MBit, |
         4xIntel 10/100/1000 MBit
|

--------|

-Hewlett Packard---
--------|
ML 150 G2, Intel Xeon 3 GHz, SATA-HDD, Marvel MV88SX6041 4 Port SATA-
CTRL |
           onboard NIC Broadcom 5721 10/100/1000
|

--------|

-IBM---
--------|
IBM x206, Intel P4 2,8 GHz, SATA-HDD 80 GB, IBM 6300ESB Software
Raid*, |
          onboard NIC INTEL 82547GI 10/100/1000
|

--------|
IBM x346 2*Xeon 3,2 GHz, IBM ServeRAID-7K Ver.: 7.12.02 (RAID 1),
|
          2*146 GB HDD, 2*IBM Ethernet Controller (bcm5700) onboard
|

--------|

-Sun---
--------|
Sun LX50, 2x 1,4 GHz Pentium III, 2xIntel Pro 100 10/100 MBit
|
          1x 36 GB (onboard AIC-7889 SCSI Controller)
|

--------|
Sun Fire V20z, 2x 1,8 GHz Opteron, 2 GB RAM, 2x10/100/1000 MBit, 1x 36
GB |
               Ultra 320 SCSI (onboard LSI 53C1030 SCSI Controller)
|

--------|

Unsupported tested Servers
==========================

ANEXO 4.

Reporte Ejecutivo De Astaro

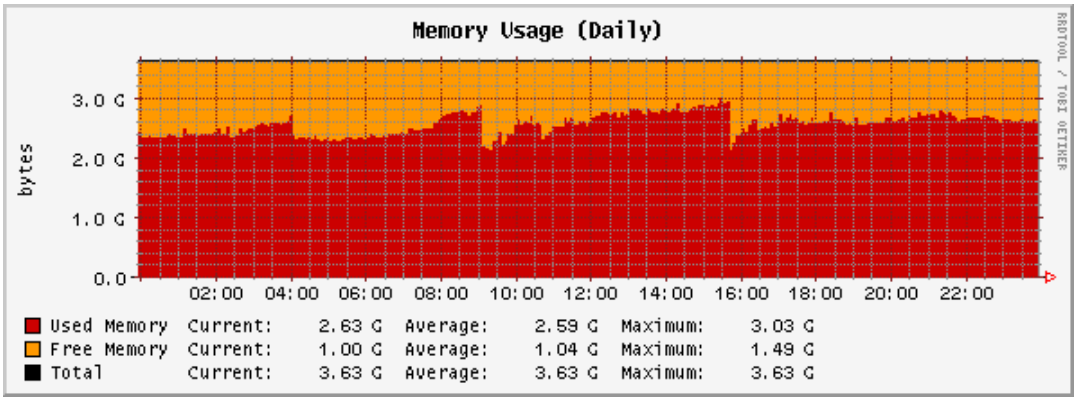
Executive Report for petroproduccion.com.ec **Wed, 14 May 2008**

Administration	Today	Yesterday	Last 7 Days	Last 30 Days
WebAdmin logins (success/failed)	16 / 0	6 / 0	35 / 4	136 / 10
Remote logins (success/failed)	0 / 0	0 / 0	0 / 0	0 / 0
Local logins (success/failed)	0 / 0	0 / 0	0 / 0	0 / 0
Up2Date: System (success/failed)	0 / 0	0 / 0	0 / 0	0 / 0
Up2Date: Virus Protection (success/failed)	3 / 0	1 / 1	42 / 10	250 / 21
Up2Date: Spam Protection (success/failed)	0 / 0	0 / 0	0 / 0	1 / 0
Up2Date: Intrusion Protection (success/failed)	0 / 0	0 / 0	0 / 0	1 / 0
Config changes (total)	24	12	122	580
ACM uploads (total)	0	0	0	0
System restarts (total)	0	0	0	1
HA takeover (total)	0	0	0	0
Uplink failover events (total)	0	0	0	0

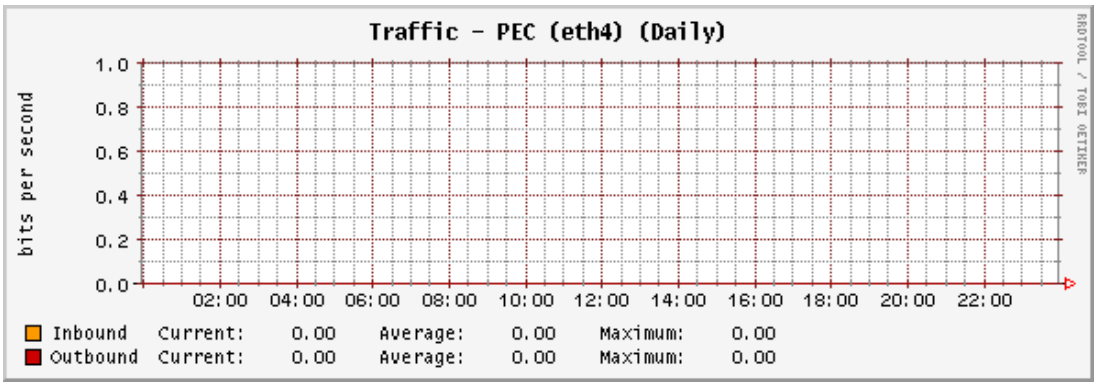
Virus Protection	Today	Yesterday	Last 7 Days	Last 30 Days
SMTP viruses	42	42	179	599
POP3 viruses	0	0	0	0
HTTP viruses	1	3	28	175

CPU Load (Daily Graph)

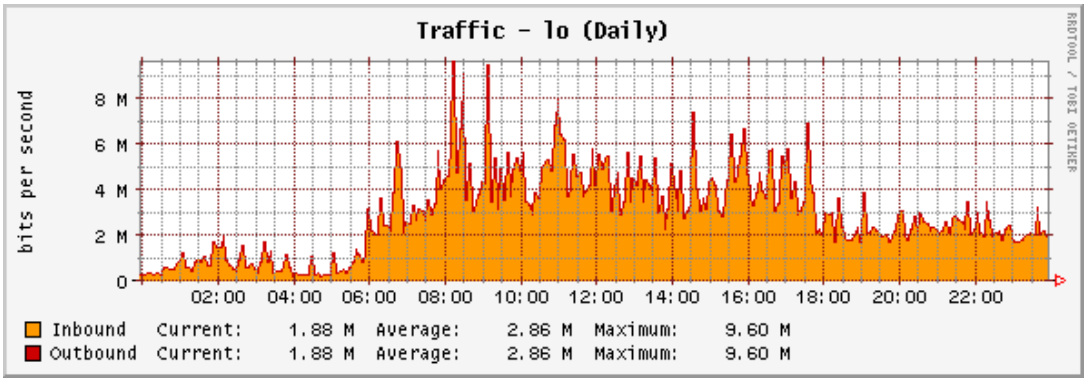
Memory Usage (Daily Graph)



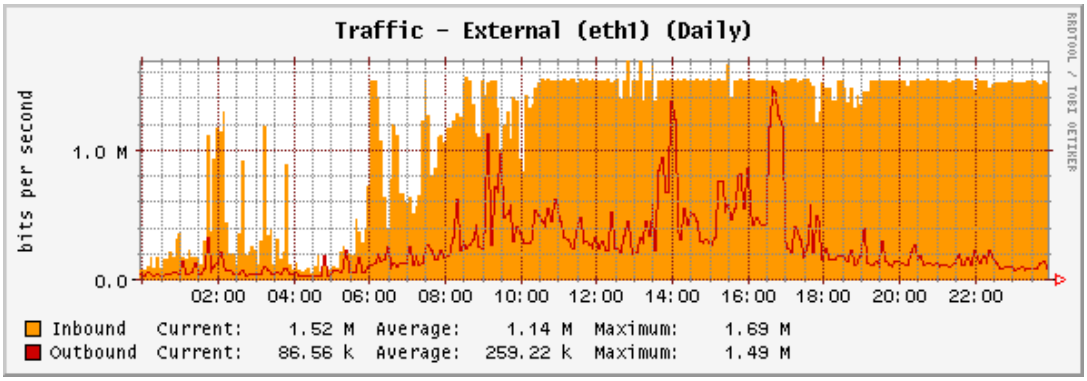
Traffic - PEC (eth4) (Daily Graph)



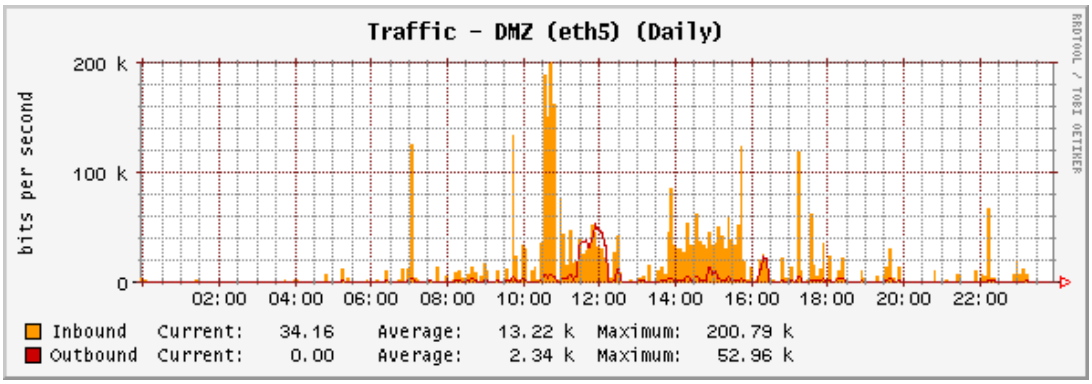
Traffic - lo (Daily Graph)



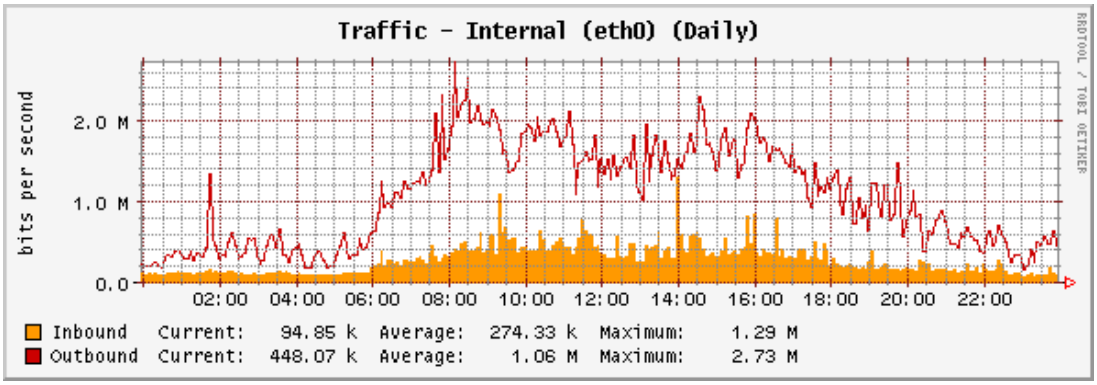
Traffic - External (eth1) (Daily Graph)



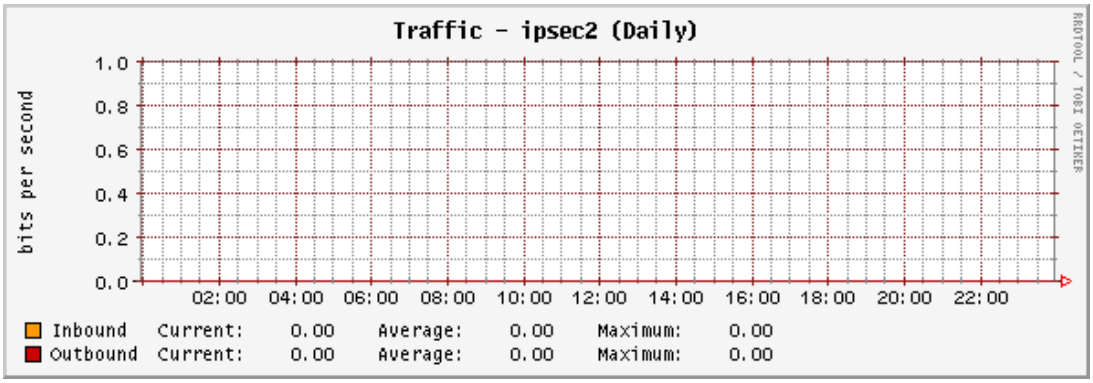
Traffic - DMZ (eth5) (Daily Graph)



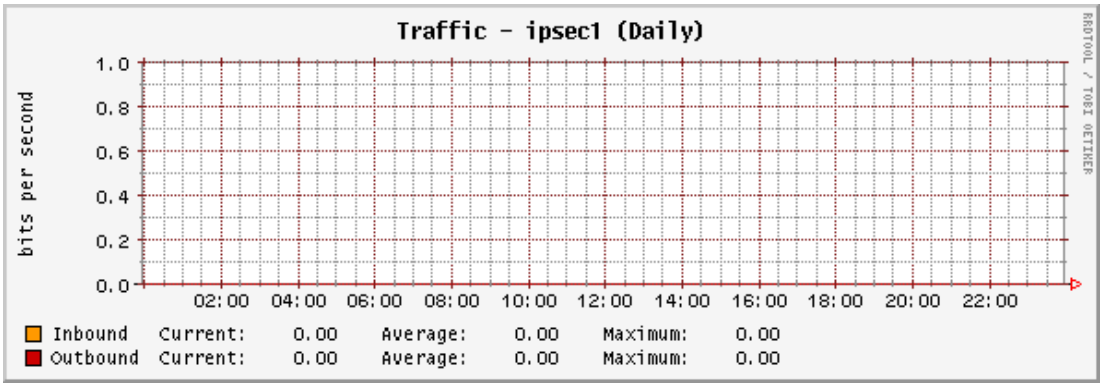
Traffic - Internal (eth0) (Daily Graph)



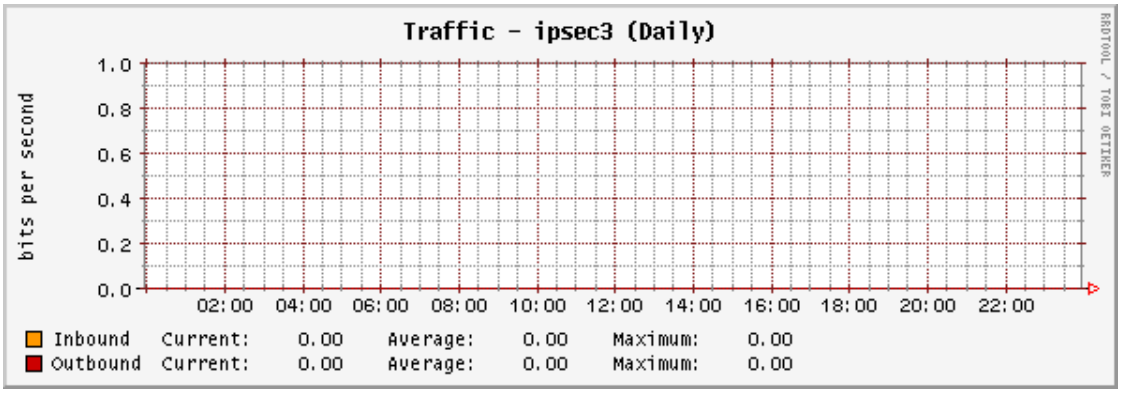
Traffic - ipsec2 (Daily Graph)



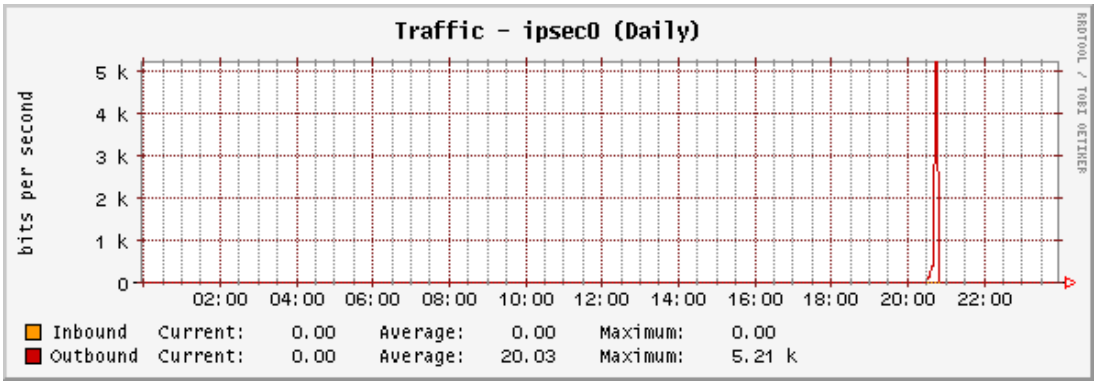
Traffic - ipsec1 (Daily Graph)



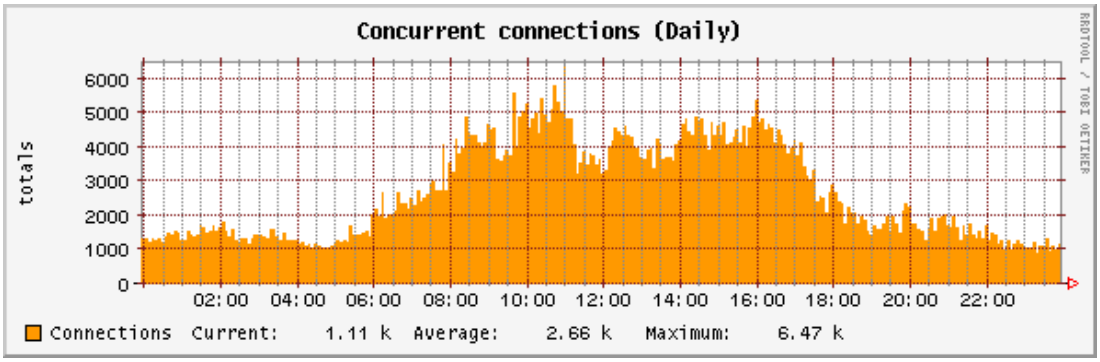
Traffic - ipsec3 (Daily Graph)



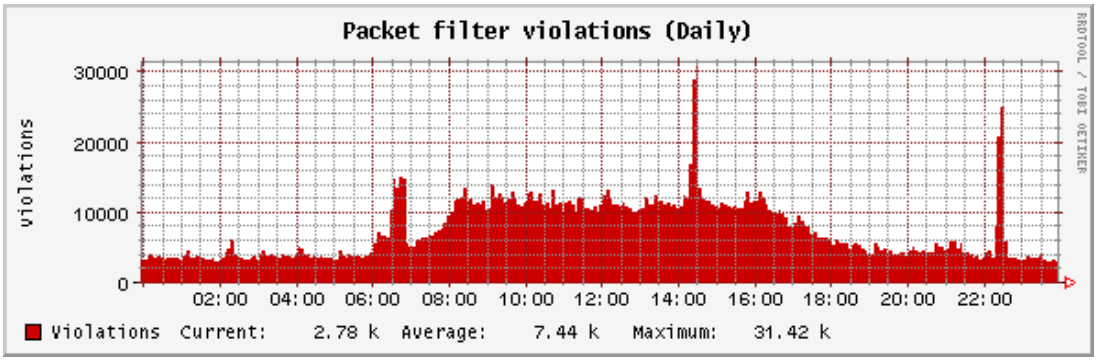
Traffic - ipsec0 (Daily Graph)



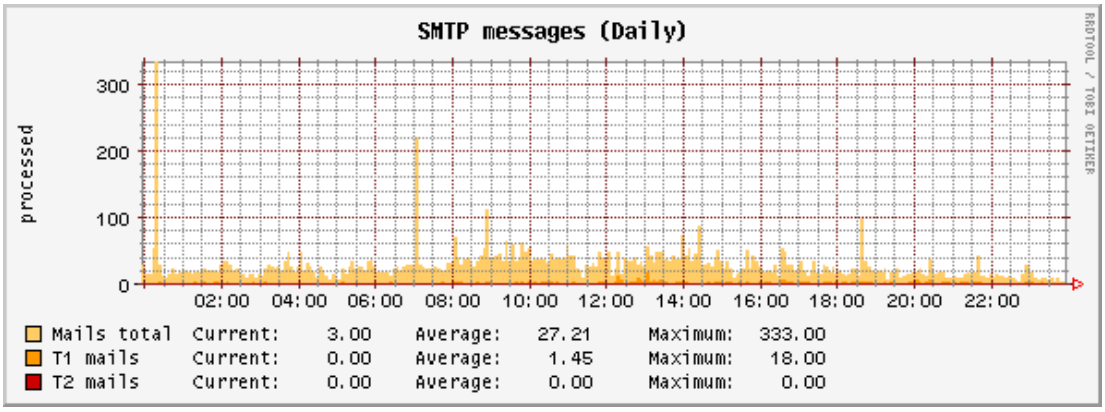
Concurrent connections (Daily Graph)



Packet filter violations (Daily Graph)

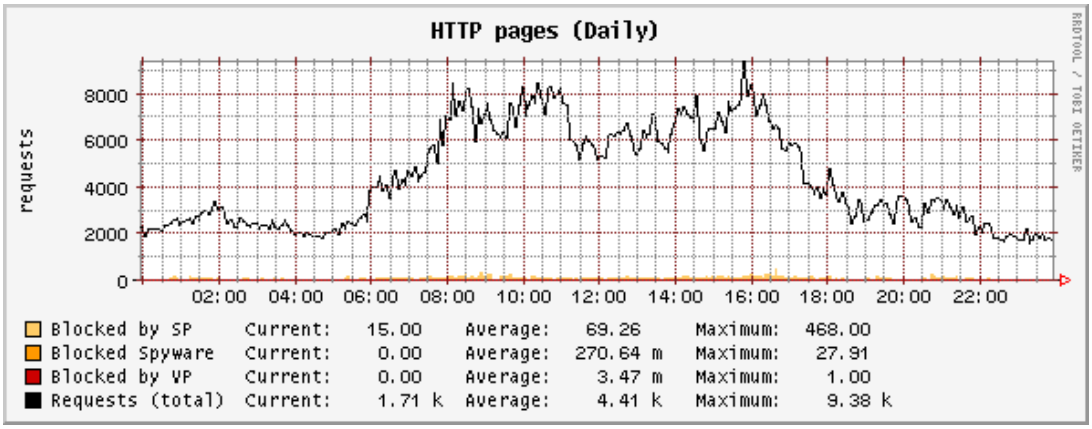


SMTP messages (Daily Graph)



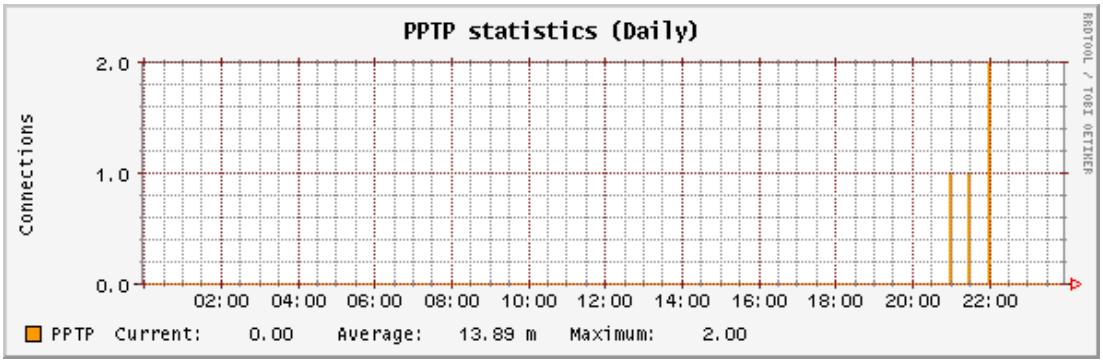
Content Filter	Today	Yesterday	Last 7 Days	Last 30 Days
SMTP mails processed (total)	7 836	8 449	52 536	209 324
SMTP processed mail size	753.7 MB	619.5 MB	3.4 GB	15.8 GB
SMTP average mail size	98.5 kb	75.1 kb	67.0 kb	79.0 kb
SMTP average spam score	0.4	0.4	0.4	0.5

HTTP pages (Daily Graph)

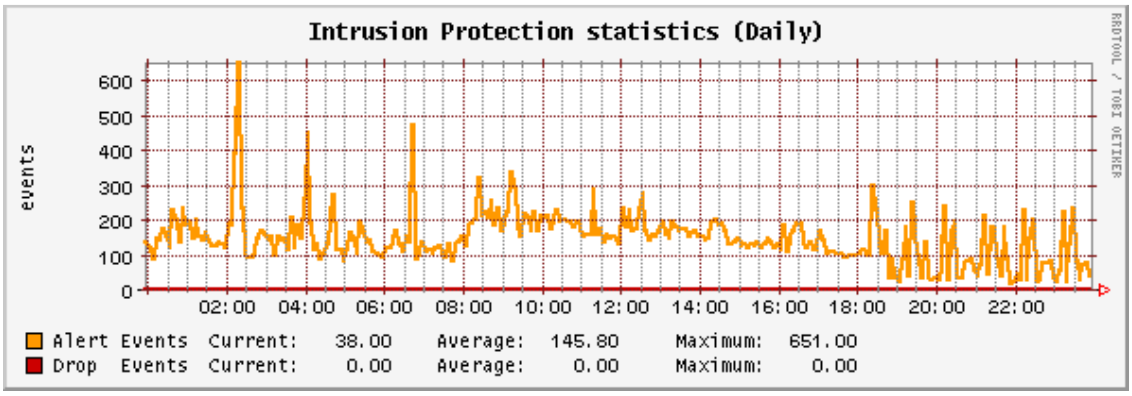


Content Filter	Today	Yesterday	Last 7 Days	Last 30 Days
HTTP pages requested (total)	1 269 187	1 338 365	5 591 087	23 828 100
- Top 1: Music	5 805	6 622	30 246	130 535
- Top 2: Dating / Relationships	4 213	5 497	23 592	88 843
- Top 3: Private Homepages	3 379	3 844	22 218	103 444
- Top 4: Cinema / Television	3 136	3 066	18 057	87 817
- Top 5: Humor / Comics	2 580	2 942	12 370	42 648
- URL Blacklist	0	0	0	0
HTTP pages blocked by VP (total)	1	3	28	175
Blocked Spyware (total)	71	29	370	2 407

PPTP statistics (Daily Graph)



Intrusion Protection statistics (Daily Graph)



SIP	Today	Yesterday	Last 7 Days	Last 30 Days
Incoming call requests (total)	0	0	0	0
Outgoing call requests (total)	0	0	0	0
Successful calls (total)	0	0	0	0

System Version: 6.310 Uptime: 23 d 7 h 44 m Load average: 0.47

BIBLIOGRAFÍA

LIBROS

PETERSON, R. Red Hat Linux: manual del administrador. 3ra. ed. Madrid: McGraw-Hill, 2004. pp. 396.

NORTHCUTT, **S**. Y NOVAK, J. Detección de Intrusos: guía avanzada. 2ª. ed. EE.UU: Prentice Hall, 2001. pp. 152

MAXWELL, **S**. Centos Server: herramientas para la administración de redes. 3ra. ed. Madrid: McGraw-Hill, 2004. pp. 497.

HERNÁNDEZ, **R**. Firewalls: seguridad en las redes e Internet. 2ª. ed. Madrid: McGraw-Hill, 2004. pp. 87. (Boletín de Política Informática N° 2)

ARÉVALO, F. Blindaje de Redes: tu red invulnerable a los hackers. 2ª. ed. Madrid: Anaya, 2005. pp. 162

STALLINGS, W. Fundamentos de Seguridad en Redes: seguridades en redes. 2ª. ed. EE.UU: Añil, 2004. pp. 150-200.

MCCLURE, S. y SCAMBRAY, J. y KURTZ, G. Hacking Exposed: network security, secrets and solutions. 5th. ed. EE.UU: Añil, 2005. pp. 110-115

URKO ZURUTUZA, O. Sistemas de Detección Intrusos: detección de intrusos. 2ª. ed. Madrid: McGraw-Hill, 2004. pp. 75

BIBLIOGRAFÍA INTERNET

- **ASTARO INTERNET SECURITY**

  http://www.astaro.es/

  20060810

- **BOLETINES DE SEGURIDAD**

  http://www.alerta-antivirus.es

  20060615

- **DELITOS INFORMÁTICOS**

  http://www.delitosinformaticos.com/seguridad

  20070121

- **EMPRESA NV NEXTVISION.** Otra Manera De Pensar La Seguridad

  http://www.nextvision.com

  20070322

- **FIREWALLS Y SEGURIDAD EN INTERNET**

  http://www.monografias.com/

  2006

- **NOTICIAS DE SEGURIDAD INFORMATICA**

  http://www.Virusprot.com

  20060512

- **SEGURIDAD EN UNIX Y REDES**

  http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec.pdf

  20020218