ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

El presente proyecto trata sobre la implementación de un servidor para optimizar y administrar el uso del Internet en la Dirección Nacional de Migración a nivel nacional utilizando herramientas bajo Linux.

El proyecto inicia con el reconocimiento de la Dirección Nacional de Migración a nivel de institución y de la importancia que tiene el Internet y el impacto que este desarrolla si es mal utilizado. Después de tener una visión de lo que se desea hacer se procede a investigar las herramientas necesarias, que se aplicaran en el desarrollo del proyecto.

Conectarse a Internet sin un servidor de seguridad incrementa la vulnerabilidad de la información y puede provocar pérdidas y daños irremediables. En Internet, los piratas informáticos utilizan código malintencionado (como virus, gusanos y troyanos) para intentar encontrar equipos desprotegidos. Un servidor de seguridad puede disminuir el riesgo y proteger la integridad de la información en la institución.

En busca de este fin es importante realizar un estudio de la situación en la que se encuentra en este momento la Dirección Nacional de Migración en lo que a seguridades se refiere, esto incluye un análisis de su red local así como también de todas las funcionalidades de Internet que utilizan (navegación por las páginas web, publicación de weblogs y webs, correo electrónico, mensajería instantánea, foros, chats, gestiones y comercio electrónico, entornos para el ocio) que pueden significar algún riesgo.

ABSTRACT

The present project is about the implementation of a server to optimize and to administer the use of the Internet in the DNM at national level using tools under Linux.

The project initiates with the recognition of the DNM at an institutional level, the importance that the Internet has and the impact that it develops if it is badly used. After having a vision of what is desired to do, you should proceed to investigate the necessary tools that would be applied in the development of the project.

Connect to the Internet without a security server is like leaving the keys of your house front door putted in the lock, while you go to the store. Although it is possible to enter and leave without anything happens, somebody could take this opportunity. In Internet, the hackers use hostile code (like virus, worms and troyans) trying to find unprotected equipment. A security server can protect the WAN network of the DNM from this security attack and from another type.

In the search of this goal it is important to make a study of which is the actual security situation of the DNM, this includes an analysis of its local network as well as all the Internet functionalities that they use (Web navigation, weblogs and Webs publications, e-mail, instant messaging, forums, chats, managements and electronic commerce, surroundings for the leisure) that can contribute some risk.

CAPÍTULO I

1 INTRODUCCIÓN

1.1 JUSTIFICACIÓN

En la Dirección Nacional de Migración se ha vuelto imperiosa la necesidad de proveer a la institución de una optima administración del Internet que le permita tener el control de la utilización de las funcionalidades Web de los usuarios; con esto podrán optimizar el ancho de banda contratado y mantener registros de una buena utilización de este servicio dentro de la institución ya que la solución incluye seguridad y control.

Las estadísticas mundiales de seguridad muestran que hoy en día estas soluciones ya se han vuelto prácticamente indispensables en toda organización y siendo la Dirección Nacional de Migración parte de una prestigiosa institución como la Policía Nacional, es ineludible el compromiso de brindarle estas soluciones con calidad eficiencia y eficacia.

1.2 OBJETIVOS

General

Optimizar y administrar el uso del Internet en la red de Policía de Migración a nivel nacional mediante la implementación de soluciones bajo sistema operativo Linux.

Específicos

Controlar el buen uso del Internet y brindar una herramienta de administración amigable al centro de cómputo de la Dirección Nacional de Migración.

Analizar el uso actual del Internet y su aplicabilidad en la Dirección Nacional de Migración.

Diseñar la estructura del funcionamiento y distribución del Internet en la Dirección Nacional de Migración.

En base a los estudios previos de seguridad implementar un Servidor con herramientas de optimización y administración del Internet.

Verificar el correcto funcionamiento del Internet con las nuevas políticas de seguridad en las Jefaturas y Sub Jefaturas de Policía de Migración a nivel Nacional.

1.3 ALCANCE

El proyecto tiene como finalidad optimizar y administrar el uso del Internet en la Dirección Nacional de Migración, brindando diferentes soluciones como: Filtro de Contenidos, Proxy, Firewall, Controlador de Ancho de Banda, Detección de Intrusos IDS y Prevención de Intrusos IPS, además de realizar las pruebas correspondientes para su correcto funcionamiento en los destacamentos de la Dirección Nacional de Migración a nivel nacional.

Dentro de lo que a las diferentes soluciones se refiere, es necesario identificar las políticas en base a la realidad de la Dirección Nacional de Migración.

Se analizará la configuración de equipos y servidores, se evaluará la operatividad y eficiencia de la configuración, se planteará una nueva solución para mejorar la situación actual en caso de que necesite mejoras y se implementarán los cambios para mejorar la productividad de la red.

Para todos estos puntos se necesita la completa colaboración del departamento de Sistemas ya que son los que manejan el área de telecomunicaciones dentro de la Dirección Nacional de Migración.

CAPÍTULO II

2 FUNDAMENTOS TEÓRICOS

2.1 INTRODUCCION

A partir del 28 de diciembre de 1971, se crea la Ley de Migración con Decreto No. 1899. La Policía Nacional del Ecuador asume la vigilancia y represión de la inmigración y radicación clandestina de extranjeros.

El principio universal de toda nación es el uso de la soberanía; impedir el ingreso de extranjeros al territorio nacional y admitirlos de acuerdo a los tratados y convenios internacionales.

Con estos antecedentes se crea el Servicio de Migración al amparo de la Ley Orgánica de la Policía Nacional constando como una de las funciones esenciales "El control del movimiento migratorio y la permanencia de extranjeros en el país", conformando para tal efecto una Dirección General en Quito, una Subdirección en Guayaquil y Jefaturas Provinciales en todas las provincias del Ecuador a excepción de la del Napo y Cañar.

2.2 DIRECCIÓN NACIONAL DE MIGRACIÓN COMO INSTITUCIÓN

La Dirección de Migración se ha planteado como objetivo primordial la modernización de los servicios migratorios y el fortalecimiento del control, mediante la implantación de nueva tecnología, la simplificación de los procesos de trabajo, la profesionalización de los recursos humanos, el establecimiento de un nuevo modelo de gestión migratoria y el mejoramiento del servicio al cliente.

Localización del servicio de Migración en las diferentes provincias del país:

- Dirección Nacional de Migración Quito
- Jefatura Provincial de Migración de Pichincha
- Policía Aeroportuaria Mariscal Sucre
- Jefatura Provincial de Migración Guayas

- Aeropuerto José Joaquín de Olmedo
- Jefatura Provincial de Migración El Oro
- Sub-Jefatura Provincial de Migración Huaquillas
- Jefatura Provincial de Migración de Manabí
- Subjefatura Portoviejo
- Jefatura Provincial de Migración de Chimborazo
- Jefatura Provincial de Migración Azuay
- Jefatura Provincial de Migración Macará
- Puente Internacional Macará
- Sub-Jefatura Provincial de Migración de Loja
- Jefatura Provincial de Migración Los Ríos
- Jefatura Provincial de Migración de Tungurahua
- Sub-Jefatura Baños
- Jefatura Provincial de Migración Carchi
- Jefatura Provincial de Migración de Bolívar
- Jefatura Provincial de Migración de Imbabura
- Sub-Jefatura Provincial de Migración Otavalo
- Jefatura Provincial de Migración de Cotopaxi
- Jefatura Provincial de Migración de Esmeraldas
- Sub-Jefatura San Lorenzo
- Jefatura Provincial de Migración Cañar
- Jefatura Provincial de Migración Pastaza
- Jefatura Provincial de Migración de Morona Santiago
- Jefatura Provincial de Migración Zamora
- Jefatura Provincial de Migración San Cristóbal
- Sub-Jefatura Provincial de Migración Santa Cruz
- Jefatura Provincial de Migración Napo
- Jefatura Provincial de Migración Sucumbíos
- Jefatura Provincial de Migración Orellana
- Jefatura Provincial de Migración Santo Domingo

Misión

"La Dirección Nacional de Migración es la Institución que en el Ecuador se encarga de el control migratorio (entradas y salidas de personas nacionales y extranjeros) y pasaportación en todo el territorio nacional; y, de control y permanencia de extranjeros en el país, de conformidad con las leyes y reglamentos pertinentes; utilizando para ello los recursos humanos, tecnológicos y logísticos acordes a las exigencias de la sociedad actual y bajo parámetros de eficiencia y eficacia en los servicios para la comunidad."

Visión

"La Dirección Nacional de Migración se constituirá en una Institución fuerte, organizada, capacitada, especializada, moderna y efectiva en el control migratorio, asumiendo con ética y profesionalismo la tarea encomendada por el estado y la sociedad en su conjunto para erradicar la migración ilegal y velar por el bienestar colectivo; no escatimará esfuerzos ni recursos para alcanzar los máximos objetivos institucionales orientándose siempre hacia un servicio cada vez más personalizado, humano y solidario."

2.3 LINUX COMO SISTEMA OPERATIVO

Linux es un sistema operativo diseñado por cientos de programadores de todo el planeta, aunque el principal responsable del proyecto es Linus Tovalds. Su objetivo inicial es propulsar el software de libre distribución junto con su código fuente para que pueda ser modificado por cualquier persona, dando rienda suelta a la creatividad. El hecho de que el sistema operativo incluya su propio código fuente expande enormemente las posibilidades de este sistema. Este método también es aplicado en numerosas ocasiones a los programas que corren en el sistema, lo que hace que podamos encontrar muchos programas útiles totalmente gratuitos y con su código fuente.

Las funciones principales de este sistema operativo son:

1. **Sistema multitarea:** En Linux es posible ejecutar varios programas a la vez sin necesidad de tener que parar la ejecución de cada aplicación.

2. **Sistema multiusuario:** Varios usuarios pueden acceder a las aplicaciones y recursos del sistema Linux al mismo tiempo. Y, por supuesto, cada uno de ellos puede ejecutar varios programas a la vez (multitarea).
3. **Shells programables:** Un shell conecta las ordenes de un usuario con el Kernel de Linux (el núcleo del sistema), y al ser programables se puede modificar para adaptarlo a tus necesidades. Por ejemplo, es muy útil para realizar procesos en segundo plano.
4. **Independencia de dispositivos:** Linux admite cualquier tipo de dispositivo (módems, impresoras) gracias a que cada una vez instalado uno nuevo, se añade al Kernel el enlace o controlador necesario con el dispositivo, haciendo que el Kernel y el enlace se fusionen. Linux posee una gran adaptabilidad y no se encuentra limitado como otros sistemas operativos.
5. **Comunicaciones:** Linux es el sistema más flexible para poder conectarse a cualquier ordenador del mundo. Internet se creó y desarrollo dentro del mundo de Unix, y por lo tanto Linux tiene las mayores capacidades para navegar, ya que Unix y Linux son sistemas prácticamente idénticos.

Linux no sacrifica en ningún momento la creatividad, tal y como lo hacen algunas compañías informáticas. Linux es una ventana abierta por la que es posible huir hacia un mundo donde la verdadera informática puede ser disfrutada sin límites ni monopolios.

Linux es distribuido mediante una serie de distribuciones como RedHat, Slackware, Debian, Ubuntu, etc, las cuales se diferencian por su método de instalación y por los paquetes (software) que viene incluido. Todo el software de Linux está regido por la licencia de GNU, con la cual cualquier persona puede modificar un programa y venderlo según el desee, con la condición que la persona que compra ese producto puede realizar la misma acción o simplemente hacer copias para todos aquellos que lo quieran sin tener que pagar más. Esta licencia es la garantía que afirma la absoluta libertad de este sistema operativo.

2.3.1 Historia de Linux

Linux, es un sistema operativo. Es una implementación de libre distribución UNIX para computadoras personales (PC), servidores y estaciones de trabajo.

Linux es la denominación de un sistema operativo tipo-Unix y el nombre de un núcleo.

Es uno de los paradigmas más prominentes del software libre y del desarrollo del código abierto, cuyo código fuente está disponible públicamente, para que cualquier persona pueda libremente usarlo, estudiarlo, redistribuirlo y, con los conocimientos informáticos adecuados, modificarlo.

Linux es usado como sistema operativo en una amplia variedad de plataformas de hardware y computadores, incluyendo los computadores de escritorio (PCs x86 y x86-64, Macintosh y PocketPC), servidores, supercomputadores, mainframes, y dispositivos empotrados así como teléfonos celulares.

En 1983 Richard Stallman fundó el proyecto GNU, con el fin de crear sistemas operativos parecidos a UNIX y compatibles con POSIX. Dos años más tarde creó la "Fundación del Software Libre" y escribió la GNU General Public License para posibilitar el software libre en el sistema de copyright.

El software GNU se extendía muy de prisa y dentro de poco una multitud de programas fueron escritos, de manera que ya a principios de 1990 había bastantes software GNU como para hacer un sistema operativo propio, pero faltaba el Kernel.

A principios de los años 1990, no había un sistema operativo libre completo a pesar de que el proyecto GNU era desarrollado constantemente, no disponía sin embargo de ningún buen Kernel basado en UNIX, por el contrario era un número de proyectos de software libres que podían ser traducidos en las variantes UNIX mediante el compilador de GNU.

Su creador Linus Benedit Torvalds nació en Helsinki, Finlandia, en el año de 1969. Su abuelo, matemático y estadista le compró un Comodore en 1980 y fue quien "enganchó" a Linus al mundo de los computadores.

En 1988 Linus Torvalds entra a la Universidad. Ese mismo año fue cuando el sistema operativo didáctico, basado en UNIX y creado por Andy Tannenbaum, empezó a cobrar importancia. Dicho sistema era el Minix.

Linus entró a formar parte de la comunidad de usuarios Minix. Andy Tannenbaum cometió un error en su sistema operativo. Era demasiado limitado, tanto técnicamente como políticamente, en ningún momento tuvo en cuenta la posibilidad de incluir Minix al proyecto GNU. La creación de Andy Tannenbaum estaba pensando para ser distribuida. Su primer error fue ceder todos sus derechos a Prentice Hall, que empezó a cobrar 150 dólares por licencia.

Así, Linus tomó la decisión de cambiar esta política debido a que el sistema Minix era ideal para los estudiantes de sistemas operativos, y su precio era considerablemente alto.

Año 1991, cuando Linus se acabó de comprar su primer 386, la intención era crear un nuevo Kernel (al que posteriormente llamaría Linux) de UNIX basado en el Kernel de Minix y modificarlo periódicamente de manera que fuera capaz de ejecutar aplicaciones GNU.

La historia de Linux está fuertemente vinculada a la del proyecto GNU. Hacia 1991, cuando la primera versión del núcleo Linux fue liberada, el proyecto GNU había producido varios de los componentes del sistema operativo, incluyendo un intérprete de comandos, una biblioteca C y un compilador, pero aún no contaba con el núcleo que permitiera complementar el sistema operativo. Entonces, el núcleo creado por Linus Torvalds, llenó el hueco final que el sistema operativo GNU exigía.

Linus nunca anunció la versión 0.01 de Linux (agosto 1991), esta versión no era ejecutable, solamente incluía los principios del núcleo del sistema, estaba

escrita en lenguaje ensamblador y asumía que uno tenía acceso a un sistema Minix para su compilación.

El 5 de octubre de 1991, Linus anuncio la primera versión "Oficial" de Linux, -versión 0.02, con esta versión Linus pudo ejecutar Bash (GNU Bourne Again Shell) y gcc (Compilador GNU de C) pero no mucho mas funcionaba. En este estado de desarrollo ni se pensaba en los términos soporte, documentación, distribución. Después de la versión 0.03, Linus salto en la numeración hasta la 0.10, más programadores a lo largo y ancho del internet empezaron a trabajar en el proyecto y después de revisiones, Linus incremento el numero de versión hasta la 0.95 (marzo 1992). En Diciembre de 1993 el núcleo del sistema estaba en la versión 0.99 y la versión 1.0, llego el 14 de marzo de 1994.

Linux se refiere estrictamente al núcleo Linux, pero es comúnmente utilizado para describir al sistema operativo tipo Unix (que implementa el estándar POSIX), que utiliza primordialmente filosofía y metodologías libres (también conocido como GNU/Linux) y que está formado mediante la combinación del núcleo Linux con las bibliotecas y herramientas del proyecto GNU y de muchos otros proyectos/grupos de software (libre o no libre).

La expresión "Linux" es utilizada para referirse a las distribuciones GNU/Linux, colecciones de software que suelen contener grandes cantidades de paquetes además del núcleo. El software que suelen incluir consta de una enorme variedad de aplicaciones, como: entornos gráficos, suites ofimáticas, servidores web, servidores de correo, servidores FTP, etcétera. Coloquialmente se aplica el término "Linux" a éstas. Algunas personas opinan que es incorrecto denominarlas distribuciones Linux, y proponen llamarlas sistema GNU/Linux. Otras personas opinan que los programas incluidos proceden de fuentes tan variadas que proponen simplificarlo denominándolo simplemente a "Linux".

2.3.2 Características de Linux

Linux implementa la mayor parte de las características que se encuentran en otras implementaciones de UNIX, más algunas otras que no son habituales:

a. multitarea: varios programas (realmente procesos) ejecutándose al mismo tiempo.
b. multiusuario: varios usuarios en la misma máquina al mismo tiempo (¡y sin licencias para todos!).
c. multiplataforma: corre en muchas CPUs distintas, no sólo Intel.
d. funciona en modo protegido 386.
e. tiene protección de la memoria entre procesos, de manera que uno de ellos no pueda colgar el sistema.
f. carga de ejecutables por demanda: Linux sólo lee de disco aquellas partes de un programa que están siendo usadas actualmente.
g. política de copia en escritura para la compartición de páginas entre ejecutables: esto significa que varios procesos pueden usar la misma zona de memoria para ejecutarse. Cuando alguno intenta escribir en esa memoria, la página (4Kb de memoria) se copia a otro lugar. Esta política de copia en escritura tiene dos beneficios: aumenta la velocidad y reduce el uso de memoria.
h. memoria virtual usando paginación (sin intercambio de procesos completos) a disco: una partición o un archivo en el sistema de archivos, o ambos, con la posibilidad de añadir más áreas de intercambio sobre la marcha (se sigue denominando intercambio, es en realidad un intercambio de páginas). Un total de 16 zonas de intercambio de 128Mb de tamaño máximo pueden ser usadas en un momento dado con un límite teórico de 2Gb para intercambio.
i. la memoria se gestiona como un recurso unificado para los programas de usuario y para el caché de disco, de tal forma que toda la memoria libre puede ser usada para caché y éste puede a su vez ser reducido cuando se ejecuten grandes programas.
j. librerías compartidas de carga dinámica (DLL's) y librerías estáticas también, por supuesto.
k. se realizan volcados de estado (core dumps) para posibilitar los análisis post-mortem, permitiendo el uso de depuradores sobre los programas no sólo en ejecución sino también tras abortar éstos por cualquier motivo.
l. casi totalmente compatible con POSIX, System V y BSD a nivel fuente.

m. mediante un módulo de emulación de iBCS2, casi completamente compatible con SCO, SVR3 y SVR4 a nivel binario.

n. todo el código fuente está disponible, incluyendo el núcleo completo y todos los drivers, las herramientas de desarrollo y todos los programas de usuario; además todo ello se puede distribuir libremente. Hay algunos programas comerciales que están siendo ofrecidos para Linux actualmente sin código fuente, pero todo lo que ha sido gratuito sigue siendo gratuito.

o. control de tareas POSIX.

p. pseudo-terminales (pty's).

q. emulación de 387 en el núcleo, de tal forma que los programas no tengan que hacer su propia emulación matemática. Cualquier máquina que ejecute Linux parecerá dotada de coprocesador matemático. Por supuesto, si tu ordenador ya tiene una FPU (unidad de coma flotante), será usada en lugar de la emulación, pudiendo incluso compilar tu propio kernel sin la emulación matemática y conseguir un pequeño ahorro de memoria.

r. soporte para muchos teclados nacionales o adaptados y es bastante fácil añadir nuevos dinámicamente.

s. consolas virtuales múltiples: varias sesiones de login a través de la consola entre las que se puede cambiar con las combinaciones adecuadas de teclas (totalmente independiente del hardware de video). Se crean dinámicamente y puedes tener hasta 64.

t. soporte para varios sistemas de archivo comunes, incluyendo minix-1, Xenix y todos los sistemas de archivo típicos de System V, y tiene un avanzado sistema de archivos propio con una capacidad de hasta 4 Tb y nombres de archivos de hasta 255 caracteres de longitud.

u. acceso transparente a particiones MS-DOS WINDOWS (o a particiones OS/2 FAT32, NTFS) mediante un sistema de archivos especial: no necesitas ningún comando especial para usar la partición MS-DOS WINDOWS, parece un sistema de archivos normal de Unix.

v. un sistema de archivos especial llamado UMSDOS que permite que Linux sea instalado en un sistema de archivos DOS.

w. soporte en sólo lectura de HPFS-2 del OS/2 2.1

x. sistema de archivos de CD-ROM que lee todos los formatos estándar de CD-ROM.

y. TCP/IP, incluyendo ftp, telnet, NFS, etc.

z. Appletalk disponible en el actual núcleo de desarrollo.

aa. software cliente y servidor Netware disponible en los núcleos de desarrollo.

2.4 METODOLOGÍA

Los métodos a utilizarse para la especificación de requerimientos serán los empíricos, ya que la información que se obtendrá para plantear el desarrollo del proyecto será en base a entrevistas, encuestas y planificación. Una vez recopilada la información se utilizará el método teórico analítico, ya que en base a la misma se obtendrá una solución específica.

2.4.1 Método empírico

El método empírico-analítico o método empírico es un modelo de investigación científica, que se basa en la lógica empírica y que junto al método fenomenológico es el más usado en el campo de las ciencias sociales y en las ciencias descriptivas. El término empírico deriva del griego antiguo (Aristóteles utilizaba la reflexión analítica y el método empírico como métodos para construir el conocimiento) de experiencia, έμπειρία, que a su vez deriva de έυ (en) y πειρ (prueba): en pruebas, es decir, llevando a cabo el experimento. Por lo tanto los datos empíricos son sacados de las pruebas acertadas y los errores, es decir, de experiencia. Su aporte al proceso de investigación es resultado fundamentalmente de la experiencia. Estos métodos posibilitan revelar las relaciones esenciales y las características fundamentales del objeto de estudio, accesibles a la detección sensoperceptual, a través de procedimientos prácticos con el objeto y diversos medios de estudio. Su utilidad destaca en la entrada en campos inexplorados o en aquellos en los que destaca el estudio descriptivo.

Corriente lógica

La lógica empírica es la base del razonamiento empírico y por lo tanto del método empírico. Esta visión de la lógica proviene de la antigua grecia. El término empírico deriva del griego antiguo de experiencia έμπειρία, que a su vez deriva

de ἔυ, en, y πεῖρα, prueba, experimento. Su origen se deduce a través de la observación de las relaciones entre los objetos la convierte en la base ideal para las leyes del conocimiento. Su aparición en la Antigua Grecia y Mundo Árabe provoca la definitiva separación entre las ciencias formales (geometría y álgebra) de las ciencias empíricas (zoología, botánica), siendo su máximo exponente el propio Aristóteles. Su paso a través de la historia provoca el descubrimiento de la lógica experimental y se mantiene hasta nuestros días.

Características

- Es un método **fáctico**: se ocupa de los hechos que realmente acontecen
- Se vale de la verificación empírica: no pone a prueba las hipótesis mediante el mero sentido común o el dogmatismo filosófico o religioso, sino mediante una cuidadosa contrastación por medio de la percepción.
- Es auto correctivo y progresivo (a diferencia del fenomenológico). La ciencia se construye a partir de la superación gradual de sus errores. No considera sus conclusiones infalibles o finales. El método está abierto a la incorporación de nuevos conocimientos y procedimientos con el fin de asegurar un mejor acercamiento a la verdad.
- Muestra: El muestreo es un parte importante del método analítico ya que si se toma mal la muestra los resultados serian erróneos o inservibles.

Clasificaciones

Entre los Métodos Empíricos se encuentran:

- experimental: Es el más complejo y eficaz de los métodos empíricos, por lo que a veces se utiliza erróneamente como sinónimo de método empírico. Algunos lo consideran una rama tan elaborada que ha cobrado fuerza como otro método científico independiente con su propia lógica, denominada lógica experimental.
- En este método el investigador interviene sobre el objeto de estudio modificando a este directa o indirectamente para crear las condiciones

necesarias que permitan revelar sus características fundamentales y sus relaciones esenciales bien sea:

- Aislando al objeto y las propiedades que estudia de la influencia de otros factores
- Reproduciendo el objeto de estudio en condiciones controladas
- Modificando las condiciones bajo las cuales tiene lugar el proceso o fenómeno que se estudia.

Así, los datos son sacados de la manipulación sistemática de variables en un experimento (ver método hipotético deductivo, el cual a su vez también se considerar como un tipo de método empírico fuera del método experimental por su relevancia y eficacia). Una diferencia clara con el método empírico en general es que éste además trata de considerar los errores de modo que una inferencia pueda ser hecha en cuanto a la causalidad del cambio observado (carácter auto correctivo).

Corriente lógica

Un salto verdaderamente espectacular en este desarrollo se produce con Galileo Galilei que da sustento a una nueva rama dentro de la lógica empírica, la lógica experimental. Ésta combina la lógica empírica de observación de los fenómenos con dos métodos desarrollados en otras ramas del conocimiento formal: la hipótesis (ver método hipotético deductivo y la medida (ver Método de la medición. Esta vertiente da lugar al Método experimental.

- **Método de la observación científica:** Fue el primer método utilizado por los científicos y en la actualidad continua siendo su instrumento universal. Permite conocer la realidad mediante la sensopercepción directa de entes y procesos, para lo cual debe poseer algunas cualidades que le dan un carácter distintivo. Es el más característico en las ciencias descriptivas.
- **Método de la medición:** Es el método empírico que se desarrolla con el objetivo de obtener información numérica acerca de una propiedad o cualidad del objeto, proceso o fenómeno, donde se comparan magnitudes medibles conocidas. Es la asignación de valores numéricos a determinadas propiedades del objeto, así como relaciones para

evaluarlas y representarlas adecuadamente. Para ello se apoya en procedimientos estadísticos.

Pasos generales del método empírico-analítico

Existen variadas maneras de formalizar los pasos de este método. De entre ellas destacamos:

- **Forma convencional:**
    a. Identificación de un problema de investigación.
    b. Formulación de hipótesis.
    c. Prueba de hipótesis.
    d. Resultados.
- **Formulación de Neil J. Salkind.:**
    a. Formulación de un problema.
    b. Identificar factores importantes.
    c. Formulación de hipótesis de investigación.
    d. Recopilación de la información.
    e. Probar la Hipótesis.
    f. Trabajar con la hipótesis.
    g. Reconsideración de la teoría.
    h. Confirmación o refutación.

2.4.2 Metodología de la especificación de requerimientos

Esta fase permite conocer las expectativas del usuario. Para ello, se identifican los grupos de usuarios reales y posibles con sus áreas de aplicación, se revisa la documentación existente, se analiza el entorno operativo y sus requerimientos de procesado y se realizan entrevistas o cuestionarios a los usuarios.

Para todo este proceso existen técnicas formalizadas de especificación de requerimientos que más o menos concuerdan con las siguientes:

Se identifican las entradas del problema, los resultados deseados o salidas y cualquier requerimiento o restricción adicional en la solución.

- **Obtener información acerca de lo que los usuarios desean**

Los requerimientos son el punto en que el cliente y el proyecto se unen, esta unión es necesaria para poder configurar un servidor que satisfaga las necesidades del cliente.

Si los requerimientos se enfocan a describir las necesidades del cliente, entonces es lógico que la obtención de esta información sea de primera mano. Esto es, mediante entrevistas con el cliente o buscando documentación que describa la manera que el cliente desea que funcione la solución.

Las necesidades y/o requerimientos del cliente evolucionan con el tiempo y cada cambio involucra un costo. Por eso es necesario tener archivada una copia de la documentación original del cliente, así como cada revisión o cambio que se haga a esta documentación

Como cada necesidad del cliente es tratada de diferente forma, es necesario clasificar estas necesidades para saber cuáles de ellas serán satisfechas por el proyecto y cuales por algún otro producto del sistema.

- **Clasificar y estructurar requerimientos**

El clasificar requerimientos es una forma de organizarlos, ya que hay requerimientos que por sus características no pueden ser tratados igual que a otros. Por ejemplo, los requerimientos de entrenamiento de personal no son tratados de la misma manera que los requerimientos de una conexión a Internet.

La siguiente es una recomendación de cómo pueden ser clasificados los requerimientos aunque cada proyecto pueda usar sus propias clasificaciones.

  - Requerimientos del "entorno"

El entorno es todo lo que rodea a la aplicación. Aunque no podemos cambiar el entorno, existen ciertos tipos de requerimientos que se clasifican en esta categoría, ya que el sistema usa el entorno y lo necesita como una fuente de servicios necesarios para su funcionamiento. Ejemplos del entorno podemos mencionar: sistemas operativos, sistema de archivos, herramientas de seguridad.

- Requerimientos funcionales

Estos son los que describen lo que el proyecto debe hacer. Es importante que se describa el ¿Qué? Y no el ¿Cómo? Estos requerimientos al tiempo que avanza el proyecto se convierten en los algoritmos, la lógica y gran parte de la configuración de los servicios.

- Requerimientos de desempeño

Estos requerimientos nos informan las características de desempeño que debe tener el servidor. ¿Qué tan eficaz?, ¿Que tan seguro?.

- Disponibilidad (en un determinado periodo de tiempo)

Este tipo de requerimientos se refiere a la durabilidad, degradación, portabilidad y flexibilidad. Este tipo de requerimiento es también muy importante en servicios de tiempo real puesto que estos servicios manejan aplicaciones críticas que no deben estar fuera del servicio por periodos prolongados de tiempo.

- Entrenamiento

Este tipo de requerimientos se enfoca a las personas que van a administrar la solución. ¿Qué tipo de usuarios son?, ¿Qué tipo de operadores?, ¿Que manuales se entregarán y en qué idioma?

Este tipo de requerimientos, aunque muchas veces no termina con especificaciones de la configuración del servicio, son muy importantes en el proceso de diseño ya que facilitan la introducción y aceptación del servicio en donde será implementado.

- Restricciones de diseño

Muchas veces las soluciones de un servicio son normadas por leyes o estándares, este tipo de normas caen como "restricciones de diseño".

- **Especificar formalmente los requerimientos de acuerdo al nivel de audiencia que se desea.**

Una vez que ya han sido recopilados, clasificados y alojados en el nivel de jerarquía que les corresponde, hay que poner por escrito los requerimientos del servicio. Sin embargo, ¿Hasta dónde llegará esta especificación?

La habilidad de comunicarse con una audiencia debe de ser balanceada con la necesidad de especificar los requerimientos precisamente y sin ambigüedad alguna.

2.4.3 Método teórico analítico

2.4.3.1 FASE I Determinación de la situación actual

Actualmente, hay una convicción de que conviene mejorar la seguridad de la información en las instituciones y corregir algunas deficiencias del modelo de las redes LAN y WAN que se han puesto de manifiesto con el paso del tiempo. Destaca especialmente el incorrecto tratamiento de las empresas e instituciones frente a la seguridad perimetral de su red dejando huecos informáticos que permiten el manipuleo de personas no autorizadas sobre su información.

Para determinar la situación actual primero se recopilará toda la documentación existente sobre la red en la DIRECCIÓN NACIONAL DE MIGRACIÓN para poder tener un criterio concreto del estado y su funcionamiento del uso del Internet, permisos y controles de seguridad en la red WAN.

Posteriormente se instalara un servidor demo el cual nos servirá para poder generar reportes del uso del Internet como el consumo por sitio Web y porcentajes de descargas a nivel de usuario, con estos reportes podremos

determinar la gravedad del problema en cuestión seguridad y sobre todo poder establecer normas regulatorias sobre el uso del Internet Dentro de la institución.

La red de Policía de Migración está integrada por varios puntos a nivel nacional, algunos de estos puntos se conectan a Internet directamente sin ninguna protección ni control de acceso arriesgando así la integridad de la red a nivel nacional.

En todos los puntos de Policía de Migración deben acceder a un sistema en línea, el cual se encuentra centralizado en Quito, las maquinas que utilizan este sistema debe tener como gateway el router de cada localidad para que se autorice el acceso al mismo, por tal motivo las maquinas que necesitan el Internet en las diferentes localidades necesitan usar una red alterna al del sistema para su funcionamiento limitando al usuario a tener los 2 servicios paralelamente.

La red al momento permite la conexión directa a través de canales dedicados de datos entre cada una de las diferentes sucursales con la central de Quito.

La asignación de las direcciones dentro de toda la red de Policía de Migración es de forma estática y al momento no existen un control centralizado de esto, así como no existe una administración centralizada de usuarios, por lo que se asume que todo usuario dentro de Policía de Migración es administrador de la maquina que utiliza.

2.4.3.2 FASE II Reingeniería de la red

Según los negocios van evolucionando y creciendo, las necesidades tecnológicas pueden cambiar, llevando a conflictos con las premisas asumidas en un inicio, cuando se implementó la red de la DIRECCIÓN NACIONAL DE MIGRACIÓN.

La introducción de cambios en la configuración de red puede resultar costosa si no se hace con la debida planificación. Esta reconfiguración implica modificaciones en los equipos conectados, tales como ordenadores, routers y

otros. Además, los diversos servicios de la red dependen de ese enrutamiento para su perfecto funcionamiento, lo que conlleva modificaciones en servidores DNS, servidores DHCP y servidores de acceso.

Primero se realizará el levantamiento del diagrama de la red, con el fin de tener un punto de inicio a la reingeniería se tiene que dividir la red en física como en lógica para saber qué es lo que posee cada parte y así mismo de sus necesidades.

En lo que a parte física se refiere, el proceso de reingeniería se enfoca a un análisis de los puntos remotos, y en base a este estudio se emitirán conclusiones y recomendaciones acerca de la situación actual de la red WAN.

Lógicamente se analizará la configuración de equipos y servidores, para evaluar la operatividad y eficiencia de la configuración actual.

2.4.3.3 FASE III Análisis

En lo que se refiere al análisis, se va a utilizar los estudios realizados anteriormente como punto de partida, con el fin de entender el entorno de la necesidad del Internet en la DNT.

2.4.3.4 FASE IV Implementación

Con los resultados de la Fase de Análisis se consideraran aspectos como el fundamento de la utilización del Internet en la institución los cuales estarán de acorde a las necesidades del proyecto. Se configurara el servidor con las soluciones de: Spam, Filtro de Contenidos, Proxy, Firewall, Controlador de Ancho de Banda, Detección de Intrusos IDS y Prevención de Intrusos IPS, haremos pruebas con cada servicio configurado lo cual garantizara el correcto funcionamiento del proyecto.

2.5 HERRAMIENTAS DE ANÁLISIS E IMPLEMENTACIÓN

2.5.1 Linux ClarkConnect

2.5.1.1 Descripción

ClarkConnect es un software para servidor de puerta de enlace gateway basado en sistema operativo linux, con acceso simultáneo a internet para múltiples usuarios con una sola conexión sobre líneas dedicadas, incluye un completo módulo de administración con todas las optimizaciones necesarias aprovechando los recursos de hardware disponibles.

Figura 2.1 Pantalla de ClarkConnect 5.0

Es una solución poderosa como servidor de internet. Se instala bajo su misma plataforma Linux la cual ya la trae incluida dentro de la solución.

- Provee aplicaciones del core de servidor: Mail, web, VPN, backup, servicios de impresión y de archivos.
- Protege la red y data: Antivirus, antispam, firewall, prevention de intrusión
- Refuerza las políticas de uso de internet: Filtrado de contenido, peer-to-peer filter, administración del ancho de banda.
- Simplifica la administración y monitoreo: Monitoreo de los sistemas del servidor, software de actualización, backup del mail.

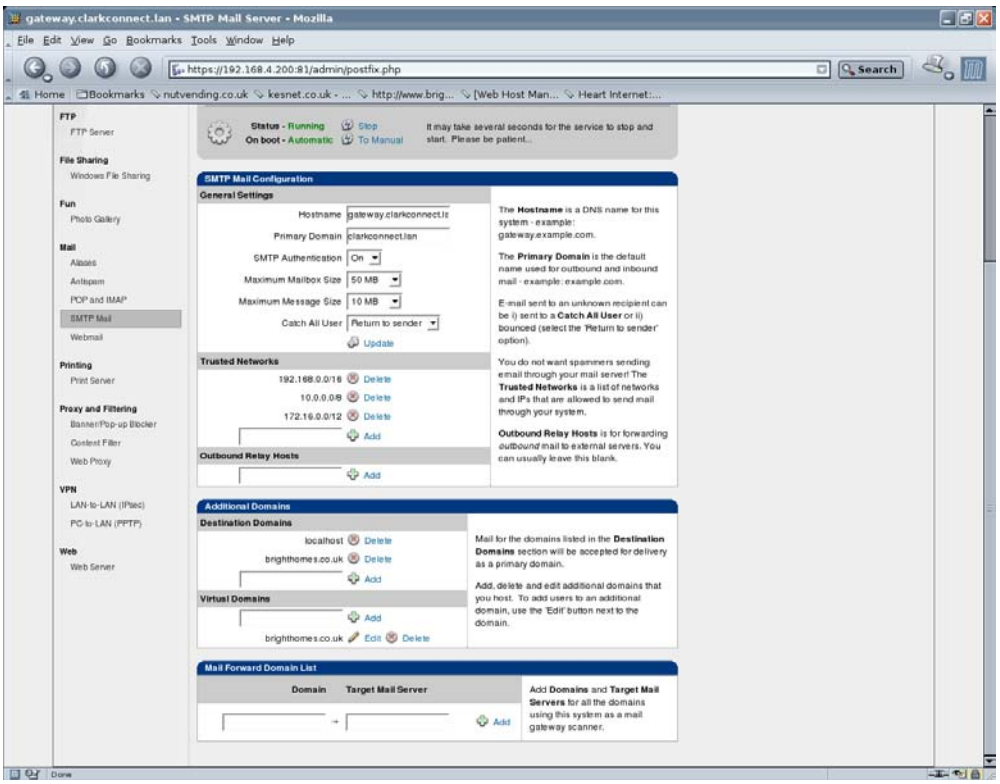


Figura 2.2 Servicios que incluyen en ClarkConnect 5.0

2.5.1.2 Características

Un estudio realizado por la firma websense, la cual se dedica a brindar seguridad empresarial, dio a conocer que el 95% de los empleados de empresas en América Latina utiliza la computadora para navegar por páginas que no están relacionadas con su actividad laboral en horas de trabajo.

Los empleados del sector público, son los que más tiempo navegan en internet por razones personales, en promedio 70 minutos aproximadamente, tiempo en el que visitan alrededor de cinco páginas diferentes al día.

Según el estudio, a las autoridades del sector público no les preocupa tanto el tiempo que sus empleados invierten en el internet, sino el mal manejo que éstos tengan con la tecnología, ya que puede repercutir en su seguridad y finanzas.

Entre las amenazas más frecuentes para una empresa se encuentra la fuga de datos por medio de correos enviados de manera equivocada por parte de sus subordinados.

Balanceo de carga y Failover: Cada vez más, las conexiones a Internet o Intranet en la institución, son más críticas y los tiempos de resolución por parte de los operadores de Internet, no son lo rápidos que deberían.

Para ello implantamos balanceo de carga que permite tolerancia a fallos en las conexiones de Internet, de modo que siempre se cuenten con al menos dos operadores, disponiendo por tanto a la institución de una garantía mucho mayor.

Al balancear la carga entre varias líneas podemos decidir qué parámetro tener en cuenta para realizar ese balanceo: podemos realizarlo en base a las direcciones IP origen, la dirección IP destino, el puerto origen o destino u otros factores.

Brinda información del servidor: Estado actual del hardware como memoria, disco duro, interfaces de red, estadísticas del sistema, procesos, conexiones y monitoreo del tráfico.

Aceleración Web Proxy: Un servidor Proxy es un equipo intermediario situado entre el sistema del usuario e Internet. Se utilizara para registrar el flujo de información de cada usuario, teniendo así el control total del uso del Internet dentro de la Institución.

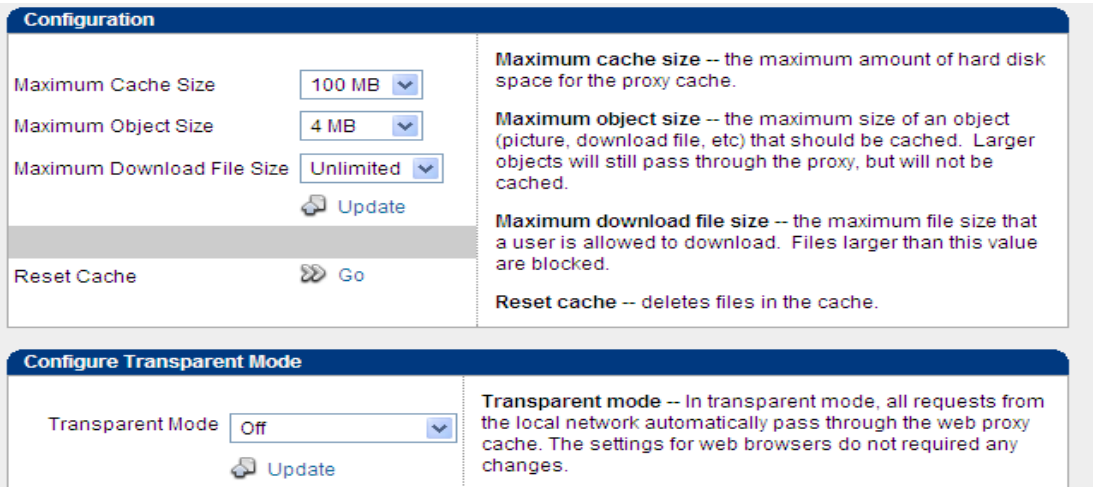


Figura 2.3 Servicio web proxy en ClarkConnect 5.0

Mejora el rendimiento.

El Proxy guarda en la memoria caché las páginas Web a las que acceden los sistemas de la red durante un cierto tiempo. Cuando un sistema solicita la misma página Web, el servidor Proxy utiliza la información guardada en la memoria caché en lugar de recuperarla del proveedor de contenidos. De esta forma, se accede con más rapidez a las páginas Web.

Administración centralizada del ancho de banda: Con asignación de cuotas límites para subidas y descargas de archivos. El rendimiento de las aplicaciones a través de Internet o de la Red de Área Extendida (WAN) resulta crítico para la institución. El correo electrónico, las descargas peer-to-peer y el uso de Internet compiten por los recursos y pueden afectar al rendimiento de aplicaciones críticas. Las Soluciones de Bandwidth Management son dispositivos de gestión del tráfico de aplicaciones que proporcionan visibilidad hacia estos problemas y la capacidad de resolverlos. Basado en la inteligencia a nivel de aplicación de estos equipos, que supervisan, controlan y aceleran el tráfico en la red, proporcionando así una elevada calidad de servicio a las aplicaciones críticas y permitiendo alinear los recursos de red de una organización con las necesidades del negocio.

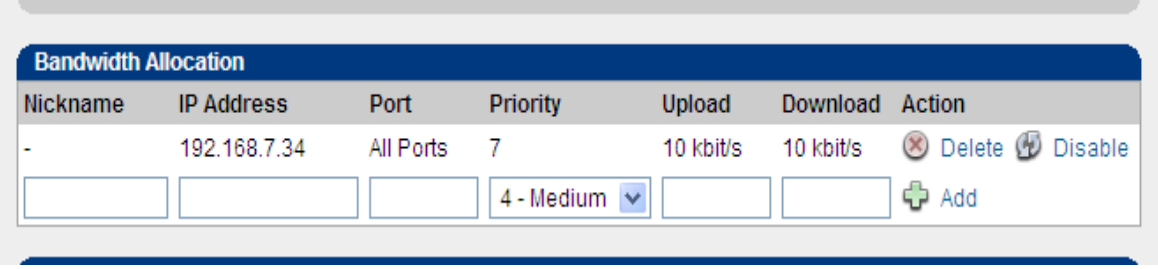


Figura 2.4 Servicio control ancho de banda en ClarkConnect 5.0

Filtrado de contenido Web: Filtro de Contenido WEB. Bloquea sitios que no son permitidos por las políticas de la empresa, aumentando la productividad del personal y reduciendo la posibilidad de infección, ya que algunas paginas contienen virus que dañan los equipos de computo.

Sus funciones básicas son:

Controlar y restringir la navegación en una computadora específica.

Definir filtros y los aplicarlos a cada miembro de la institución.

Bloquear páginas Web con temas específicos tales como: sexo, violencia, drogas, compras, música, juegos, azar.

Delimitar el tiempo máximo de navegación en Internet.

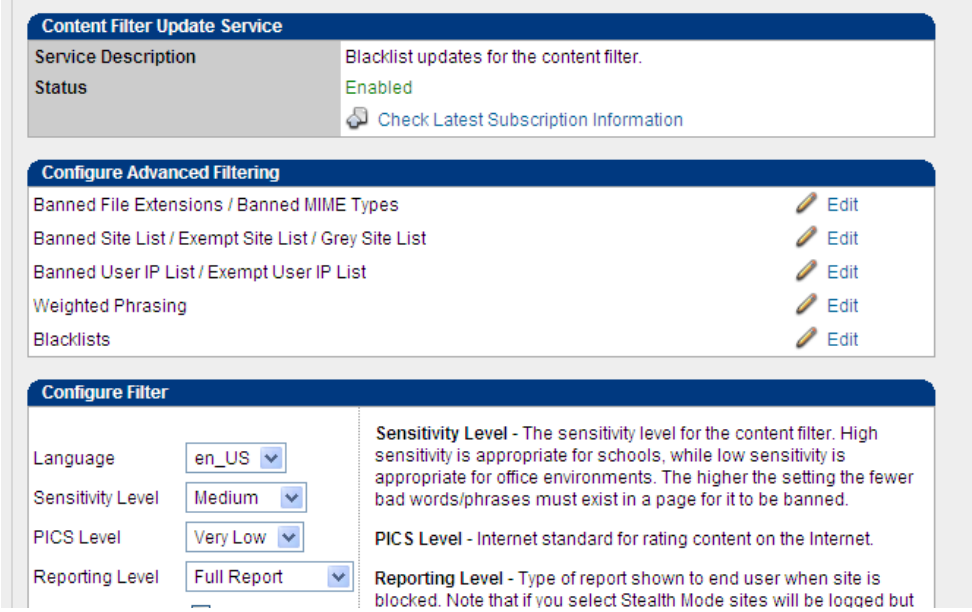


Figura 2.5 Servicio filtro de contenidos en ClarkConnect 5.0

El servicio Filtro de Contenidos permite a las empresas asegurar un uso consecuente de la red de banda ancha que tienen instalada en su oficina. De esta manera, se reduce el tiempo de uso personal que realizan los empleados de las aplicaciones de comunicaciones de Internet, acceso a contenidos Web o descarga de ficheros.

Servidor para páginas Web: Se ejecuta continuamente en el servidor, manteniéndose a la espera de peticiones de ejecución que le hará un cliente o un usuario de Internet. El servidor web se encarga de contestar a estas peticiones de forma adecuada, entregando como resultado una página web o información de todo tipo de acuerdo a los comandos solicitados. Además. contiene reportes de acceso al servidor.

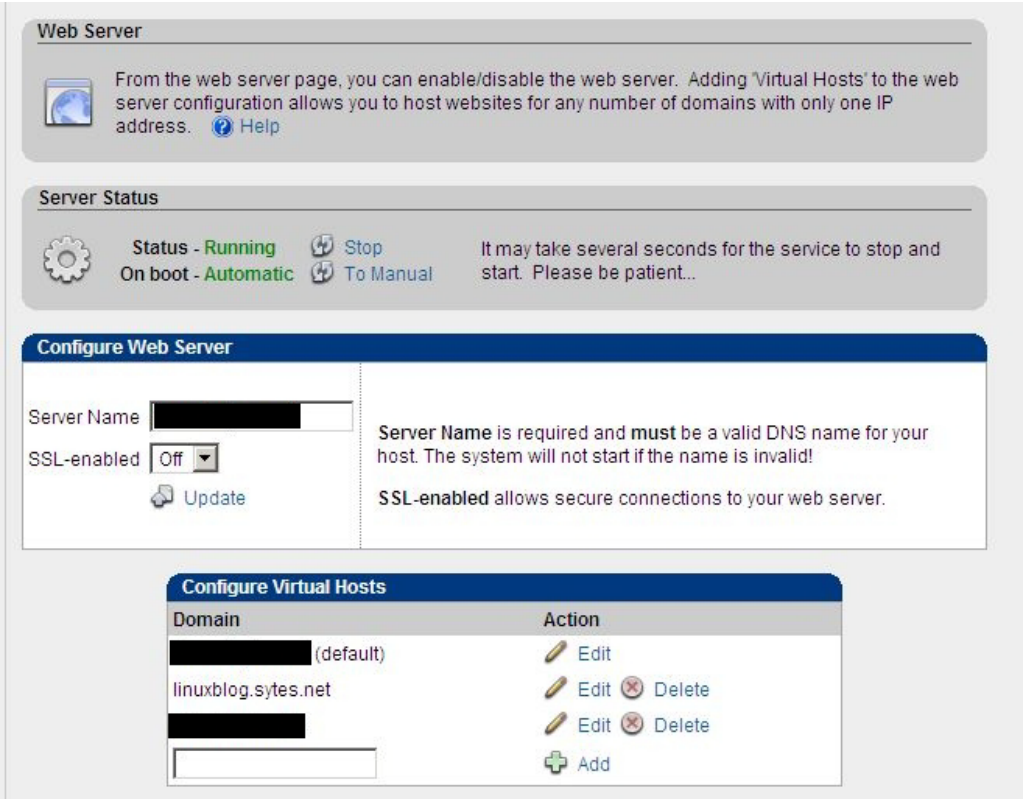


Figura 2.6 Servicio servidor web en ClarkConnect 5.0

Servidor de correo: Utiliza una interfaz Web o los clientes de correo Outlook, incluye además una administración de alias y listas de correo. Para lograr la conexión se definen una serie de protocolos, cada uno con una finalidad concreta:

SMTP, Simple Mail Transfer Protocol: Es el protocolo que se utiliza para el envio de correo ya sea desde un servidor de correo a otro, o bien, desde un Cliente de correo electrónico al servidor.

POP, Post Office Protocol: Se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario.

IMAP, Internet Message Access Protocol: Su finalidad es la misma que la de POP, pero el funcionamiento y las funcionalidades que ofrecen son diferentes.

Así pues, un servidor de correo consta en realidad de dos servidores: un servidor SMTP que será el encargado de enviar y recibir mensajes, y un servidor POP/IMAP que será el que permita a los usuarios obtener sus mensajes.

Para obtener los mensajes del servidor, los usuarios se sirven de clientes, es decir, programas que implementan un protocolo POP/IMAP. En algunas ocasiones el cliente se ejecuta en la máquina del usuario (como el caso de Mozilla

Thunderbird, Evolution, Microsoft Outlook). Sin embargo existe otra posibilidad: que el cliente de correo no se ejecute en la máquina del usuario; es el caso de los clientes vía web, como GMail, Hotmail, OpenWebmail, SquirrelMail.

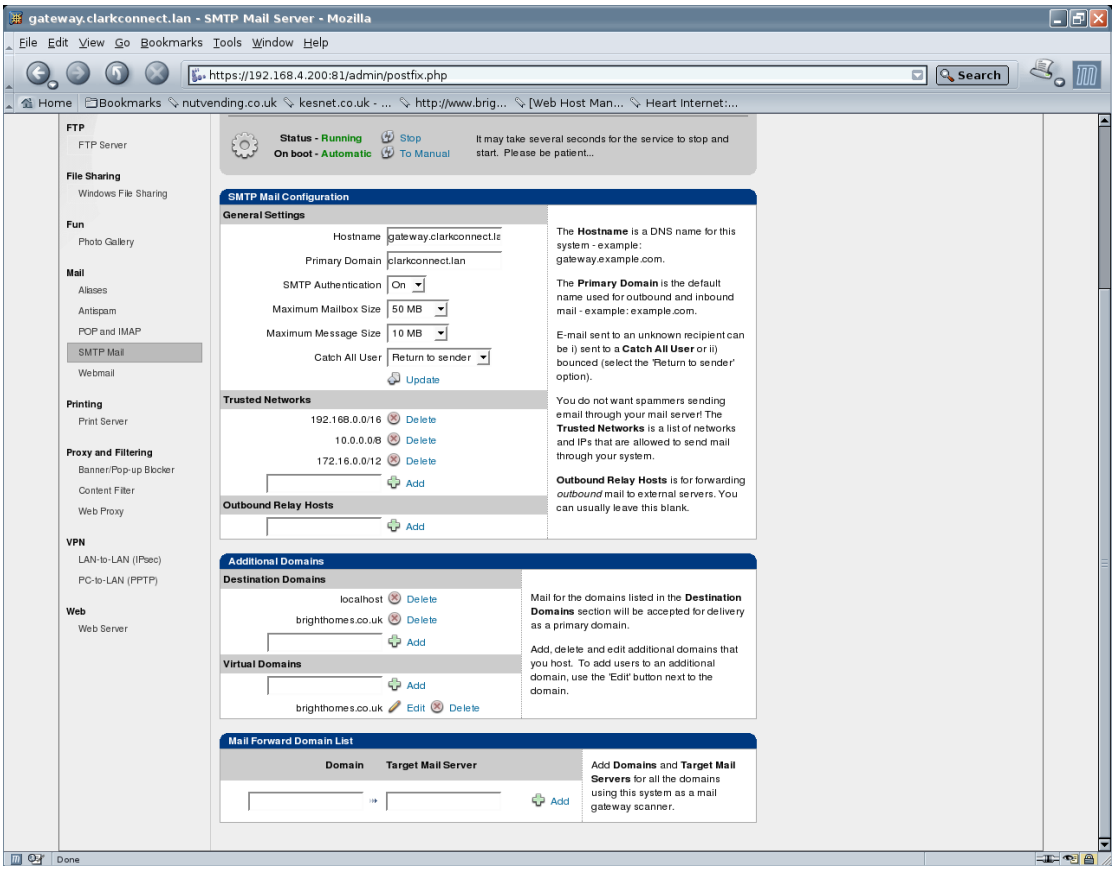


Figura 2.7 Servicio servidor mail en ClarkConnect 5.0

Software centralizado AntiSpam y Antivirus: Para proteger la red interna chequea correos entrantes y salientes, lo que permite no solo evitar contaminaciones sino también detectar los equipos dentro de la red local que estén infectados. Se deberá realizar una revisión de todas las maquinas de Policía de Migración a nivel nacional hasta estar completamente seguros que toda la red está libre de Virus, ya que es totalmente absurdo querer controlar Virus externo si existe Virus en la red Interna.

La revisión de Spam y Virus por maquina incluye las siguientes tareas como:
Realizar un chequeo exhaustivo de toda la maquina hasta que se considere que la maquina está libre de problemas

Instalación o Revisión de la configuración de un software Antivirus en cada máquina, este software deberá conectarse automáticamente a Internet y actualizar su definición de virus por lo menos una vez a la semana. Además de realizar un chequeo programado automáticamente de toda la maquina por completo al menos 1 vez a la semana.

Instalación de un software anti-spyware y chequeo completo, de ser posible configuración de este programa para realizar chequeos programados semanalmente.

Desinstalación de todo programa no autorizado por el departamento de sistemas de Policía de Migración.

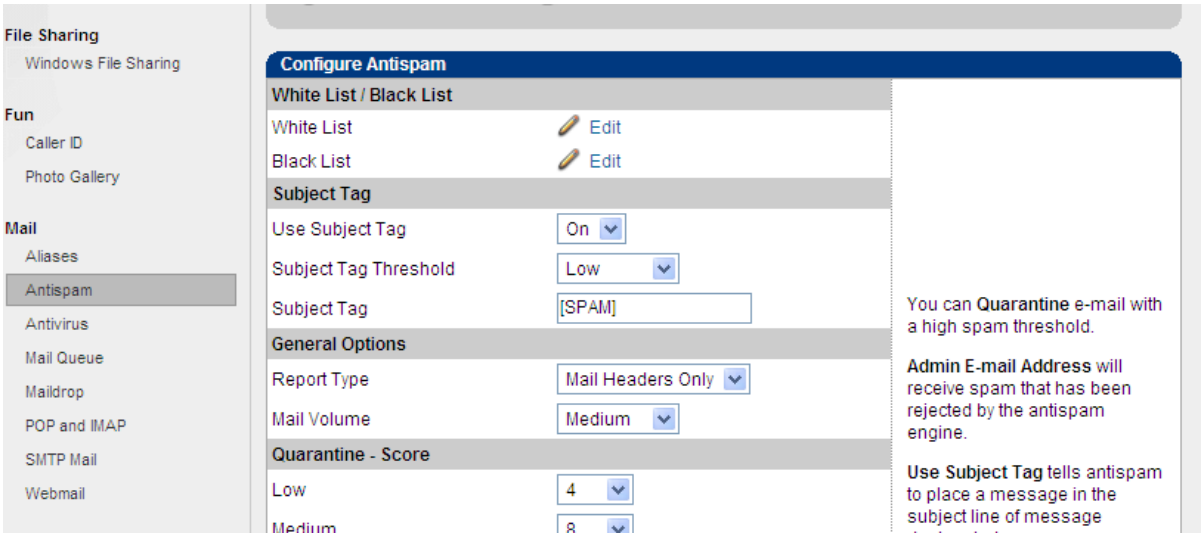


Figura 2.8 Servicio antispam y antivirus en ClarkConnect 5.0

Además de estas tareas esta tesis ayudara al departamento de sistemas de Policía de Migración a la implementación de políticas de seguridad a nivel de toda la empresa pues los usuarios en general no deben tener privilegios Administrativos en las maquinas de trabajo, para evitar instalación de programas no permitidos, cambios de configuración que pueden provocar que la maquina no funcione correctamente.

Además de esto se hará una revisión de los filtros de correo del Servicio Antispam y Antivirus a nivel de servidor.

Módulo de seguridad contra ataques indeseados y controles de acceso (Intrusion Detection System IDS): Incluye un Firewall basado en estándares Iptables, configurable de acuerdo a las necesidades de la red local de la empresa.

Tener un firewall y no un IDS genera con frecuencia un sentido falso de seguridad a la institución. Aunque los firewalls y otros controles pueden bloquear el acceso no autorizado a los recursos de la red, tienen limitaciones en su capacidad para protegerse de un ataque de Negación de Servicio (DoS), Caballos de Troya, gusanos y demás ataques maliciosos que son más frecuentes. El uso del IDS en la red de Policía de Migración ayudara básicamente a que el atacante de un nivel de determinación o destreza no pueda lanzar una amenaza que pueda penetrar eficazmente las redes protegidas por esta capa adicional de seguridad.

Un cambio o aumento repentino en la actividad de los puertos puede indicar un posible ataque, aunque pasaría desapercibido si únicamente se cuenta con un firewall para la protección en el perímetro. El IDS monitorea y analiza constantemente los incidentes que ocurren en un sistema o red informáticos en busca de actividades sospechosas (señales preliminares como rastreos de equipos host o análisis de puertos) o ataques directos que lo alertan en tiempo real para que tome decisiones inmediatas.

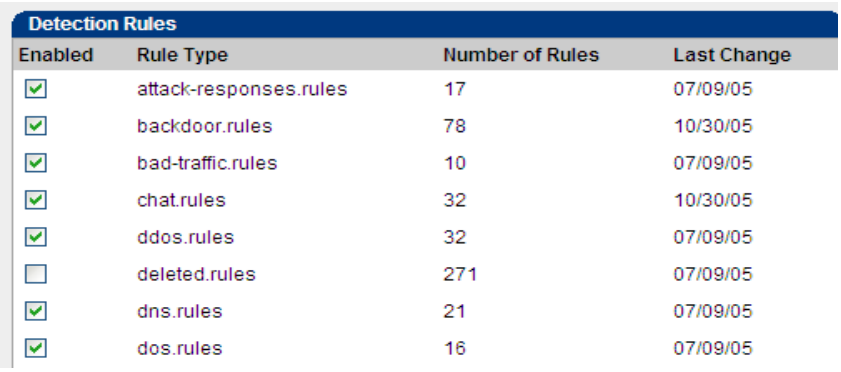


Figura 2.9 Servicio detención de intrusos en ClarkConnect 5.0

El entorno actual exige IDS

La mayor frecuencia de las rápidas amenazas combinadas sigue siendo el problema más urgente de las pequeñas empresas que no tienen sistemas IDS. Las amenazas combinadas utilizan combinaciones de códigos maliciosos como virus, gusanos y caballos de Troya para aprovechar vulnerabilidades conocidas

en los códigos de las aplicaciones o de los sistemas. Otros problemas son el rápido aumento de amenazas Windows 32 y la creciente cantidad de amenazas dirigidas a los servicios entre pares (P2P) y estaciones de trabajo de mensajería instantánea.

Módulo de seguridad para prevención de ataques indeseados y controles de acceso (Prevención de Intrusos IPS): Un Sistema de Prevención de Intrusos (IPS) es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de Prevención de Intrusos es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.
Los IPS fueron inventados de forma para resolver ambigüedades en el monitoreo pasivo de redes de computadoras, al situar sistemas de detecciones en la vía del tráfico. Los IPS presentan una mejora importante sobre las tecnologías de firewall´s tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos.

Figura 2.10 Servicio prevención de intrusos en ClarkConnect 5.0

También es importante destacar que los IPS pueden actuar a nivel de equipo, para combatir actividades potencialmente maliciosas.

Solución servidor firewall perimetral: Un firewall es un dispositivo que filtra el tráfico entre redes. En general se debe verlo como una caja con dos o más interfaces de red en la que se establecen reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no.

Sus funciones básicas son:

Habilitar el acceso a puertos de administración a determinadas IPS privilegiadas.

Enmascarar el tráfico de la red local hacia el exterior.

Denegar el acceso desde el exterior a puertos de administración y a todos los que no estén dentro de las reglas marcadas por la institución.

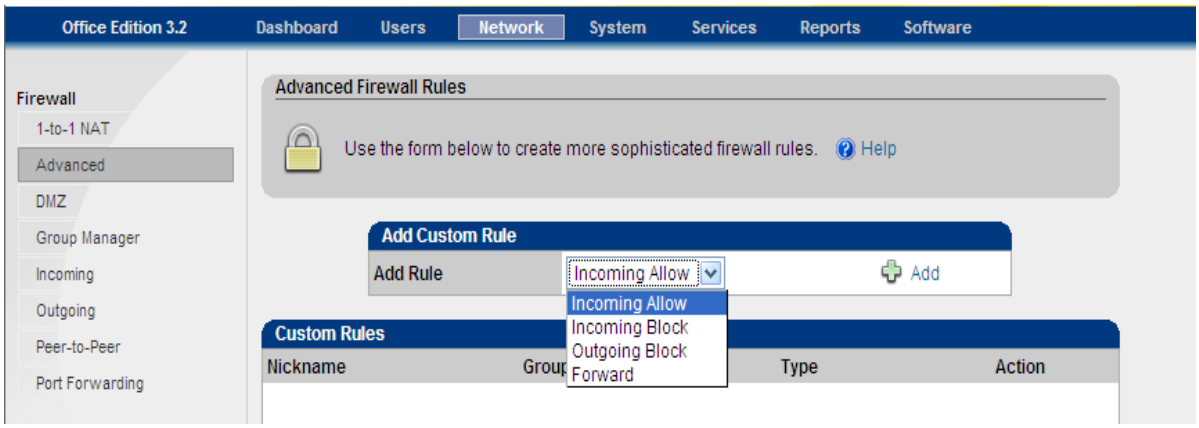


Figura 2.11 Servicio firewall perimetral en ClarkConnect 5.0

Servicio de acceso Virtual Private Network (VPN): Permite la conexión en red de varias oficinas, creando un túnel entre cliente y servidor en una comunicación segura PPTP a través de Internet, sin necesidad de montar canales de comunicación entre ellas.

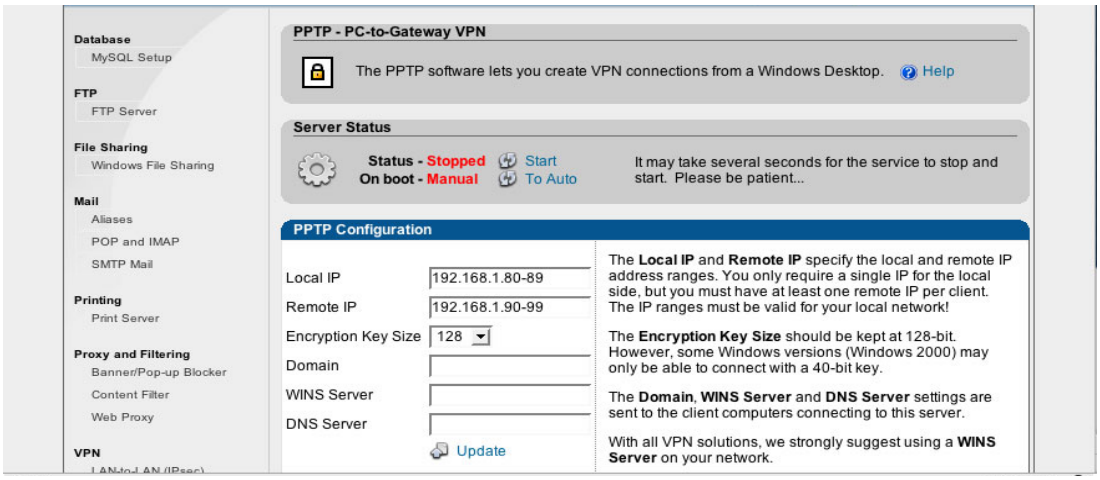


Figura 2.12 Servicio VPN en ClarkConnect 5.0

2.6 DEFINICIÓN DE ESTÁNDARES

2.6.1 Linux standard base

Linux Standard Base ha sido estudiada, verificada, y nombrada por la ISO/IEC como estándar ISO. La Base Standard para Linux es una recopilación de pruebas y casos de éxito manejados por el Free Standards Group para lograr la compatibilidad de las distribuciones en la instalación y ejecución de servicios y aplicaciones. Por lo tanto el sistema operativo Linux y sus aplicaciones está siendo reconocido por los organismos internacionales de estandarización.

Este estándar lo realizan las empresas creadoras de distribuciones Linux para que éstas sean totalmente compatibles a nivel de instalación y ejecución. De esta forma, si tenemos una aplicación preparada para ejecutarse sobre una distribución que cumpla con la recomendación LSB, será indiferente el sistema operativo linux sobre la cual corra siempre y cuando esta cumpla con LSB. Existen diferentes versiones de la especificación LSB, por lo que un determinado producto puede cumplir con las condiciones establecidas en LSB 1.3 , 2.0 o 3.0 por ejemplo.

El éxito de un sistema operativo está directamente vinculado con el número de aplicaciones que se ejecutan y la calidad con la que corren sobre él Linux y sus diferentes distribuciones, de cualquier modo, presenta a desarrolladores individuales con un conjunto único de retos: diferentes distribuciones de Linux hacen uso de diferentes versiones de bibliotecas, archivos importantes almacenados en diferentes sitios, y así muchas otras variantes.

La LSB fue creada para resolver estos problemas y reducir los costos globales de apoyo a la plataforma libre Linux. Al minimizar las diferencias entre las distintas distribuciones individuales de Linux, LSB reduce los costos relacionados con las aplicaciones de portar diferentes modos de distribuciones.

La LSB está basada en la Especificación POSIX, la Especificación Única de UNIX (Single UNIX Specification) y en varios otros estándares abiertos, aunque extiende éstos en ciertas áreas.

El objetivo de la LSB es desarrollar y promover un conjunto de estándares que aumentarán la compatibilidad entre las distribuciones de Linux y permitirán que las aplicaciones puedan ser ejecutadas en cualquier sistema Linux. Además, la LSB ayudará a coordinar esfuerzos para poder reclutar productores y proveedores de programas que creen productos nuevos para Linux o adaptaciones de aplicaciones existentes.

Mediante un proceso de certificación es posible obtener la conformidad a la LSB en una aplicación. Esta certificación la dirige el Open Group en conjunto con el Free Standards Group (Grupo de Estándares Libres).

Por ejemplo, la LSB especifica librerías estándar, un conjunto de utilerías que mejoran el estándar POSIX, la estructura del sistema de archivos, los niveles de ejecución, y varias extensiones al modo gráfico X Window.

Hasta ahora, LSB consistía en una especificación única, pero el FSG anuncio la posible creación de dos tipos de estándares LSB, uno para los servidores y otro para los desktop.

Dividiendo el estándar en dos, el FSG consigue que este pueda abarcar una amplia gama de tecnologías, pues no se le da el mismo uso a un servidor que a un computador de escritorio. Un ejemplo bastante simple, pero didáctico es que puede no ser tan importante el reconocimiento de hardware USB en un servidor al que seguramente nunca le añadiremos un disco duro externo o similar, como en un computador de escritorio, en el cual estaremos continuamente conectando, pen drives USB, cámaras de fotos y de video. De esta forma, dividir los estándares puede ser útil a cada grupo de desarrollo para centrarse solamente en lo que necesitan para cada definición de estándar.

También hay interés en incluir en el estándar LSB el entorno de ejecución de aplicaciones Java (JRE, Java Runtime Environment), aunque esto puede representar una tarea más dificultosa ya que se requiere de licencia de Sun Microsystems.

2.6.2 Estándares de protocolos de Internet RFC

2.6.2.1 RFC de TCP/IP

La familia de protocolos de Internet está todavía evolucionando mediante el mecanismo de Petición de Comentario (RFC). Los nuevos protocolos (la mayoría de los protocolos de aplicación) los han diseñado e implementado investigadores y científicos y han sido expuestos a la comunidad de Internet en forma de petición de comentario RFC. El Internet Architecture Board (IAB) supervisa el mecanismo RFC. La mayor fuente de RFC es la Internet Engineering Task Force (IETF. Sin embargo, cualquiera puede proponer una petición de comentario RFC al editor de RFC. Existe una serie de reglas que los autores de RFC deben seguir para que se acepten. Estas reglas se describen en un RFC (RFC 1543) que indica cómo considerar una propuesta para un RFC.

Una vez que se ha publicado un RFC, todas las revisiones y suplementos se publicarán como nuevos RFCs. Un nuevo RFC que revise o reemplace uno existente se dice "actualizado" u "obsoleto". El RFC existente se dice "actualizado por" u "obsoleto por" el nuevo. Por ejemplo el RFC 1521 que describe el protocolo MIME es una "segunda edición", siendo una revisión del RFC 1341 y RFC 1590 es una corrección al RFC 1521. RFC 1521 es por tanto etiquetada como "Obsoleto RFC 1341; Actualizado por RFC 1590". Por consiguiente, no existe confusión alguna de si dos personas se están refiriendo a versiones diferentes de un RFC, dado que no hay nunca versiones diferentes.

Algunos RFCs se describen como documentos de información que otros describen como protocolos de Internet. El Internet Architecture Board (IAB) mantiene una lista de los RFCs que describen la familia de protocolos. Cada uno de estos tiene asignado un estado y un status.

Un protocolo de Internet puede tener uno de los siguientes estados:

Estándar

El IAB ha establecido esto como un protocolo oficial para Internet. Se separan en dos grupos:

- Protocolo IP y citados, protocolos aplicados enteramente a Internet.

- Protocolos específicos de red, generalmente especificaciones de cómo hacer IP sobre tipos particulares de redes.

Estándar Borrador

El IAB está considerando activamente como un posible protocolo estándar. El IAB somete los comentarios y resultados de pruebas. Existe una posibilidad que si cambia será hecho un protocolo preliminar antes de que esto se haga un estándar.

Estándar Propuesto

Estos son protocolos propuestos que debe considerar IAB para su estandarización en el futuro. Son deseables implementaciones y comprobaciones de varios grupos. La revisión del protocolo es probable.

Experimental

Un sistema no debería implementar un protocolo experimental a no ser que esté participando en el experimento y ha coordinado su uso del protocolo con el desarrollador del protocolo.

Informativo

Los protocolos desarrollados por otras organizaciones, o vendedores, o que están por otras razones fuera del alcance de IAB deben publicarse como RFCs por conveniencia de la comunidad de Internet como protocolos informativos. Tales protocolos pueden en algunos casos también estar recomendados para uso en Internet por IAB.

Histórico

Estos son protocolos que con poca probabilidad llegan a ser estándares en Internet porque los han reemplazado los desarrolladores más tarde o por falta de interés.

Definiciones de estado del protocolo:

Requerido

Un sistema debe implementar los protocolos requeridos.

Recomendado

Un sistema debe implementar los protocolos recomendados.

Electivo

Un sistema puede o no implementar un protocolo electivo. La noción general es que si se va a hacer algo como esto, se debe hacer exactamente esto.

Uso limitado

Estos protocolos están para usar en circunstancias limitadas. Esto puede ser debido a su estado experimental, naturaleza específica, funcionalidad limitada o estado histórico.

No recomendado

Estos protocolos no se recomiendan para uso general. Esto se puede deber a su funcionalidad limitada, naturaleza específica o estado experimental o histórico.

2.6.2.2 RFC de Internet

El estándar propuesto, el borrador y los protocolos estándar se describen como constituyentes del Internet Standards Track. El track estándar lo controla el Grupo de Dirección de Ingenieros de Internet (IESG) del IETF. Cuando un protocolo alcanza el estado de estándar se le asigna un número estándar (STD). El propósito de los números STD es indicar claramente qué RFCs describen los estándares de Internet. Los números STD referencian múltiples RFCs cuando la especificación de un estándar se divide en múltiples documentos. No como con los RFCs, donde el número se refiere a un documento específico, los números STD no cambian cuando un estándar se actualiza. Los números STD, sin embargo, no tienen número de versión dado que todas las actualizaciones se realizan vía RFCs y los números de RFC son únicos. De este modo, para especificar sin ambigüedad qué versión de un estándar único se está refiriendo, se pondría de manifiesto el número estándar y todos los RFCs que incluye. Por ejemplo, el Sistema de Nombres de Dominio (DNS) es STD 13 y se describe en los RFCs 1034 y 1035. Para referenciar el estándar se podría utilizar algo como "STD-13/RFC-1034/RFC-1035". Para una descripción de los Procesos Estándares, ver RFC 1602 -- Los Procesos Estándares de Internet - Revisión 2.

Para algunos estándares RFCs la categoría de status no siempre contiene suficiente información útil. Por lo tanto, se complementa, notablemente por protocolos de enrutamiento por un applicability statement que se da en STD 1 o en un RFC separado.

Cuatro estándares de Internet tienen una importancia particular:

STD 1 - Estándares de Protocolos Oficiales de Internet

Este estándar da el estado y status de cada protocolo o estándar de Internet y define los significados atribuidos para cada estado o status diferente. Emitió aproximadamente una cuarta parte el IAB. Cuando se escribió este estándar fue el RFC 1780 (Marzo de 1995).

STD 2 - Números Asignados en Internet

Este estándar lista actualmente números asignados y otros parámetros de protocolos en la familia de protocolos de Internet. Lo emitió la Autoridad de Números Asignados de Internet (IANA). La edición cuando se escribió fue el RFC 1700 (Octubre de 1994).

STD 3 - Requerimientos del Host

Este estándar define los requerimientos para el software de host de Internet (a menudo con referencia a los RFCs relevantes). El estándar viene en dos partes: RFC 1122 - Requerimientos para hosts de Internet - capas de comunicaciones y RFC 1123 - Requerimientos para hosts de Internet- aplicación y ayuda.

STD 4 - Requerimientos de Pasarela

Este estándar define los requerimientos para el sofware de pasarela de Internet (router). Es el RFC 1009.

Para Tu Información (FYI)

Un determinado número de RFCs que tienen la intención de ser interesantes a los usuarios de Internet se clasifican como documentos Para Tu Información (FYI). Contienen frecuentemente información introductoria u otro tipo de información útil. Como los números de STD, un número de FYI no cambia cuando se emite la revisión de un RFC. Distintos STDs, FYIs corresponden a un único documento RFC. Por ejemplo, FYI 4 -- FYI sobre Preguntas y Respuestas -

respuestas a preguntas comunes "Nuevo Usuario de Internet" está actualmente en su cuarta edición. Los números de RFC son 1177, 1206, 1325 y 1594.

Principales Protocolos de Internet

Para dar una idea sobre la importancia de los principales protocolos, se listan algunos de ellos junto con su estado actual y número de STD donde es aplicable en la tabla que se muestra abajo. La lista completa puede encontrarse en el RFC 1780 - Estándares de Protocolos Oficiales de Internet.

Protocolo	Nombre	Estado	Estado	STD
IP	Protocolo de Internet	Estándar	Requerido	5
ICMP	Protocolo de Control de Mensajes de Internet	Estándar	Requerido	5
UDP	Protocolo de Datagrama de Usuario	Estándar	Recomendado	6
TCP	Protocolo de Control de Transmisión	Estándar	Recomendado	7
Telnet	Protocolo Telnet	Estándar	Recomendado	8
FTP	Protocolo de Transferencia de Ficheros	Estándar	Recomendado	9
SMTP	Protocolo Sencillo de Transferencia de Correo	Estándar	Recomendado	10
MAIL	Formato de Mensajes de Correo Electrónico	Estándar	Recomendado	11
DOMAIN	Sistema de Nombres de Dominio	Estándar	Recomendado	13
DNS-MX	Enrutamiento de Correo y el Sistema de Dominio	Estándar	Recomendado	14
MIME	Extensiones Multipropósito de Correo de Internet	Borrador	Electivo	
SNMP	Protocolo Sencillo de Administración de Redes	Estándar	Recomendado	15
SMI	Estructura de Información de Administración	Estándar	Recomendado	16

MIB-I	Base de Información de Administración	Histórico	No Recomendado	
MIB-II	Base de Información de Administración-II	Estándar	Recomendado	17
NetBIOS	Protocolo de Servicios NetBIOS	Estándar	Electivo	19
TFTP	Protocolo de Transferencia de Ficheros Trivial	Estándar	Electivo	33
RIP	Protocolo de Información de Enrutamiento	Estándar	Electivo	34
ARP	Protocolo de Resolución de Direcciones	Estándar	Electivo	37
RARP	Protocolo de Resolución de Direcciones Inversa	Estándar	Electivo	38
GGP	Protocolo Pasarela a Pasarela	Histórico	No Recomendado	
BGP3	Protocolo de Pasarela Exterior 3	Borrador	Electivo	
OSPF2	Abrir Primero la Trayectoria Más Corta	Borrador	Electivo	
IS-IS	IS-IS OSI para Entornos Duales TCP/IP	Propuesto	Requerido	
BOOTP	Protocolo Bootstrap	Borrador	Recomendado	
GOPHER	Protocolo Gopher de Internet	Informativo		
SUN-NFS	Protocolo de Sistema de Ficheros de Red	Informativo		
SUN-RPC	Protocolo de Llamada a Procedimiento Remoto Versión 2	Informativo		

Tabla 2.1 Estándares de Protocolos Oficiales de Internet

A la hora de escribir no hay RFC asociados con HTTP usado en implementaciones WWW.

Los siguientes RFCs describen el URL y conceptos asociados:

- RFC 1630 - Identificador de Recursos Universal en WWW.

- RFC 1737 - Requerimientos Funcionales para Nombres de Recursos Uniformes.
- RFC 1738 - Localizador de Recursos Uniformes (URL).

2.6.3 Estándares de Internet IETF

Internet Engineering Task Force (IETF) es una institución formada básicamente por técnicos en Internet e informática cuya misión es velar porque la arquitectura de la red y los protocolos técnicos que unen a millones de usuarios de todo el mundo funcionen correctamente. Es la organización que se considera con más autoridad para establecer modificaciones de los parámetros técnicos bajo los que funciona la red de redes Internet.

Convierte y promueve estándares de Internet, trabaja de cerca con W3C y ISO/IEC grupos que se ocupan particularmente de estándares TCP/IP y protocolos generales de Internet. Todos los participantes y líderes son voluntarios, aunque su trabajo es financiado generalmente por patrocinadores; por ejemplo, al momento es financiado por la entidad de verificación digital VeriSign y la agencia de seguridad nacional del gobierno de los Estados Unidos.

Se organiza grupos de trabajo y grupos de discusión (BOF) s, los cuales deben ocuparse de un asunto específico, dar solución y cerrar el caso. Cada grupo de trabajo tiene una tarea designada (o a veces varias co-tareas), junto con una carta que describa su enfoque, y qué y cuándo se espera que salga a producción.

Los grupos de trabajo se organizan en áreas por tema. Las áreas actuales incluyen: Casos de uso, casos generales, casos de Internet, operaciones y gerencia, usos e infraestructura en tiempo real, enrutamiento, seguridad, y transporte. Cada área es supervisada por su director del área, teniendo con la mayoría de las áreas dos co-directores. Los directores son responsables de designar tareas al grupo de funcionamiento. Los directores de área, junto con la tarea del IETF, forman Internet Engineering Steering Group (IESG), que es responsable de la operación total del IETF.

El IETF tiene una actividad conjunta con el Internet Society formalente. El IETF es supervisado por Internet Architecture Board (IAB), que supervisa sus relaciones externas, y relaciones con el Redactor del RFC. El IAB es también responsable del Comité administrativo de descuidos del IETF (IAOC), que supervisa la actividad de la ayuda administrativa del IETF (IASA), que proporciona ayuda y seguimiento logístico para el IETF. El IAB también maneja Internet Research Task Force (IRTF), con que el IETF tiene relaciones de grupo de trabajo y control.

Área de seguridad

El área del IETF para seguridad empieza el 10 de diciembre del 2007, fue dirigido por Tim Polk en el National Institute of Standards and Technology (NIST) de los Estados Unidos y SAM Hartman que en ese entonces era del Instituto de Tecnología de Massachusetts (MIT) también en los Eestado Unidos. Fueron apoyados por una cantidad de participantes (activos o no) que tenían direcciones de correo con dominios de bbn.com, de bear.com, de cisco.com, de cmu.edu, de columbia.edu, de comcast.net, de coopercain.com, de gmx.net, de hactrn.net, de hotmail.com, de hyperthought.com, de ibm.com, de ieca.com, de ihtfp.com, de imc.org, de isode.com, de it.su.se, de iu-bremen.de, de juniper.net, de laposte.net, de ltsnet.net, de microsoft.com, de mit.edu, de motorola.com, de navy.mil, de nec.de, de networkresonance.com, de nokia.com, de nortel.com, de nortelnetworks.com, de opentext.com, de orionsec.com, de qualcomm.com, de rsa.com, de safenet-inc.com, de sendmail.com, de sun.com, de tcd.ie, de tislabs.com, de verisign.com, de vigilsec.com, y de xmission.com. La participación pública ocurre cuando se envía la lista nombrada por SAAG, que es recibido por el MIT y administrado por Polk, Hartman, y Jeffrey I. Schiller, que es el encargado de la seguridad de la red Internet y anterior director del área de seguridad general.

Jonatán Zittrain ha sugerido que los usuarios del Internet acepten la responsabilidad de supervisar el código fuente para evitar el vandalismo por Internet. Él escribió, “la responsabilidad del IETF de un estándar u otro debe ser provechoso y crucial para aumentar la seguridad en el Internet y así la tecnología de red generativa se pueda justificar”.

CAPÍTULO III

3 DETERMINACION DE LA SITUACION ACTUAL

Para determinar la situación actual primero se recopilará toda la documentación existente sobre la red para poder tener un criterio concreto del estado de situación y su funcionamiento.

Posteriormente se instalara un servidor demo el cual nos servirá para poder generar reportes del uso del Internet como el consumo por sitio Web y porcentajes de descargas a nivel de usuario.

3.1 RECOPILACION DE INFORMACION ACERCA DE LA RED

Actualmente la red de la Policía de Migración está integrada por varios puntos a nivel nacional, algunos de estos puntos se conectan a internet directamente sin ninguna protección ni control de acceso, arriesgando así la integridad de la red a nivel nacional. Ver Figura 3.1

En todos los puntos de la Policía de Migración se accede a un sistema en línea, el cual se encuentra centralizado en Quito, las máquinas que utilizan este sistema debe tener como gateway el router de cada localidad para que se autorice el acceso al mismo, por tal motivo las máquinas que necesitan el Internet en las diferentes localidades necesitan usar una red alterna a la del sistema para su funcionamiento, limitando al usuario a tener los 2 servicios paralelamente.

La red, al momento, permite la conexión directa con la central de Quito a través de canales dedicados de datos entre cada una de las diferentes sucursales.

La asignación de las direcciones dentro de toda la red de la Policía de Migración es de forma estática y al momento no existen un control centralizado de esto, así como no existe una administración centralizada de usuarios. Por lo que

se asume que todo usuario dentro de la Policía de Migración es administrador de la máquina que utiliza.

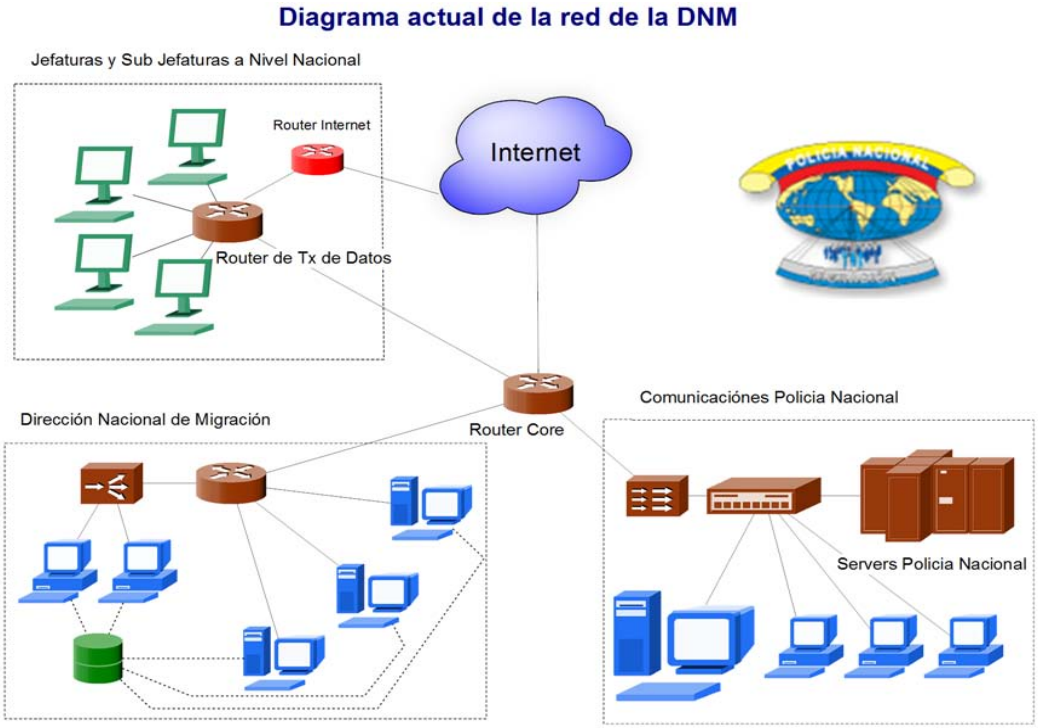


Figura 3.1 Diagrama situación actual

El sistema actual de seguridad tiene algunas falencias y se resume en que al tener salidas a internet independientes sin ningún tipo de protección pone en riesgo a la red WAN de la Policía Nacional ya que todos los puertos están abiertos y vulnerables debido al mal uso del internet.

Hay miles de sitios en internet que brindan información, métodos y herramientas para vulnerar sistemas informáticos. Todos los meses se publican nuevos libros con información sobre seguridad. Existen muchas personas dedicadas a la seguridad informática: algunos lo hacen porque es la profesión y aplica estrictas normas éticas al trabajo. Pero otras lo hacen con intenciones menos amigables y son las que provocan y crean caos en la seguridad de la información.

Hace poco tiempo la mayoría de las debilidades sobre seguridad informática en la DIRECCIÓN NACIONAL DE MIGRACIÓN tenían que ver con los virus. Hoy ya casi no se acuerdan de ellos, ahora han aparecido nuevas palabras que preocupan como: phishing, spamming, pharming, hacker, cracker, adware,

spyware, etc. El mundo de la seguridad informática y los medios de comunicación han creado todo una extensa lista de términos para denominar los peligros de los que la DIRECCIÓN NACIONAL DE MIGRACIÓN ha sido víctima y no sabe como contrarrestarlos.

Para un atacante con conocimientos medios le resulta relativamente sencillo introducirse en el sistema informático de la DIRECCIÓN NACIONAL DE MIGRACIÓN. En las aproximaciones previas a la formulación del proyecto se asombraron de lo fácil que es entrar en su router de conexión a Internet en las Jefaturas y Sub Jefaturas o en la base de datos de su sitio Web.

Los temas sobre seguridad informática son muy amplios y se encuentran en todo lado y hace mucho tiempo que este tema se convirtió, por derecho propio, en una rama específica de la informática. Para estar al día de todos los posibles riesgos es necesario especializarse y dedicar mucho tiempo a estudiarlos. Por obvias razones, todo este esfuerzo no puede exigirse al usuario común pero si al departamento de sistemas de la institución.

3.2 ESQUEMATIZACION DEL USO ACTUAL DEL INTERNET

Se instaló un servidor Linux ClarckConnect 5.0 con licencia Enterprise como demo el cual será el encargado de dar salida al Internet y monitoreo de puertos. (Ver anexo A).

La navegación se lo hizo a través del puerto 3128 para no afectar al sistema en línea, teniendo así operativos al Internet y al sistema de forma paralela.

El servidor comenzó a registrar información de cada usuario, como páginas en las que ha navegado, las descargas que ha realizado. Estos reportes los presentamos a continuación:

3.2.1 Detección de intrusos

El reporte de la detección de intrusos muestra todos los intentos de acceso al servidor tratando de violar a la seguridad del sistema.

En las graficas tomadas a partir del 22 de enero se puede observar intentos de ataque por protocolo (ver Figura 3.2 y Figura 3.3), además nos muestra las clasificación de los ataques recibidos con fecha y tipo de evento (ver Figura 3.4 y Figura 3.5), para ver los tipos de eventos que existen por ataque ver Anexo G.

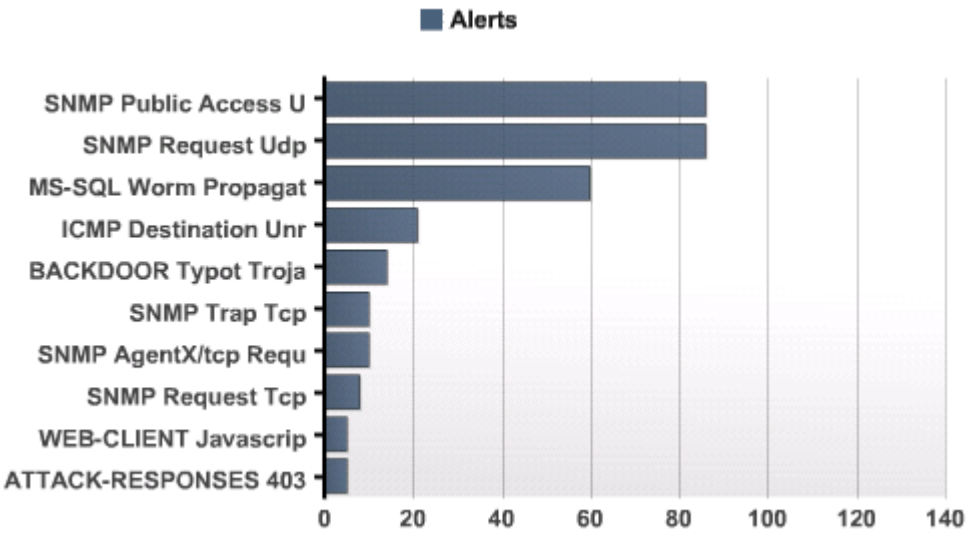


Figura 3.2 Alertas recibidas durante el mes

Alerts

ID	Alerts	Hits	Date
1411	SNMP public access udp	86	22 23
1417	SNMP request udp	86	22 23
2003	MS-SQL Worm propagation attempt	60	23 24 25 26 27 28
486	ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	21	28
2182	BACKDOOR typot trojan traffic	14	26 27 28
1421	SNMP AgentX/tcp request	10	26
1420	SNMP trap tcp	10	26
1418	SNMP request tcp	8	26
1201	ATTACK-RESPONSES 403 Forbidden	5	25 26 28
1841	WEB-CLIENT Javascript URL host spoofing attempt	5	26 27 28

Figura 3.3 Detalle de las alertas recibidas con fecha y tipo de evento.

Classifications

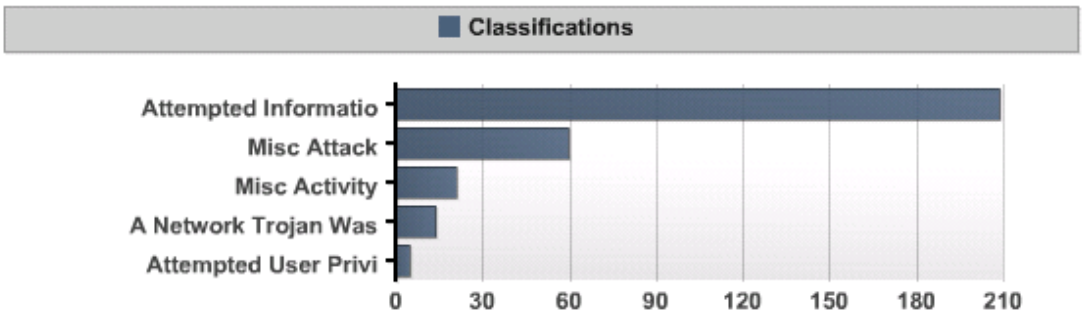


Figura 3.4 Clasificación de tipo de ataques recibidos durante el mes

Misc Attack			
ID	Alerts	Hits	Date
2003	MS-SQL Worm propagation attempt	60	23 24 25 26 27 28
Misc Activity			
ID	Alerts	Hits	Date
486	ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	21	28
A Network Trojan Was Detected			
ID	Alerts	Hits	Date
2182	BACKDOOR typot trojan traffic	14	26 27 28
Attempted User Privilege Gain			
ID	Alerts	Hits	Date
1841	WEB-CLIENT Javascript URL host spoofing attempt	5	26 27 28
Access To A Potentially Vulnerable Web Application			
ID	Alerts	Hits	Date
1070	WEB-MISC WebDAV search access	1	23
1042	WEB-IIS view source via translate header	1	23

Figura 3.5 Detalle de la clasificación de los ataques recibidos con fecha y tipo de evento.

La Figura 3.6 nos muestra el detalle de los días en los que mayor cantidad de ataques y número de intentos se recibieron. Como se puede observar lo días que se intentó atacar más fuertemente fueron el 22, con 169 intentos; el día 26, con 49 intentos y el día 28, con 45 intentos de ataques al sistema de información de la DIRECCIÓN NACIONAL DE MIGRACIÓN.

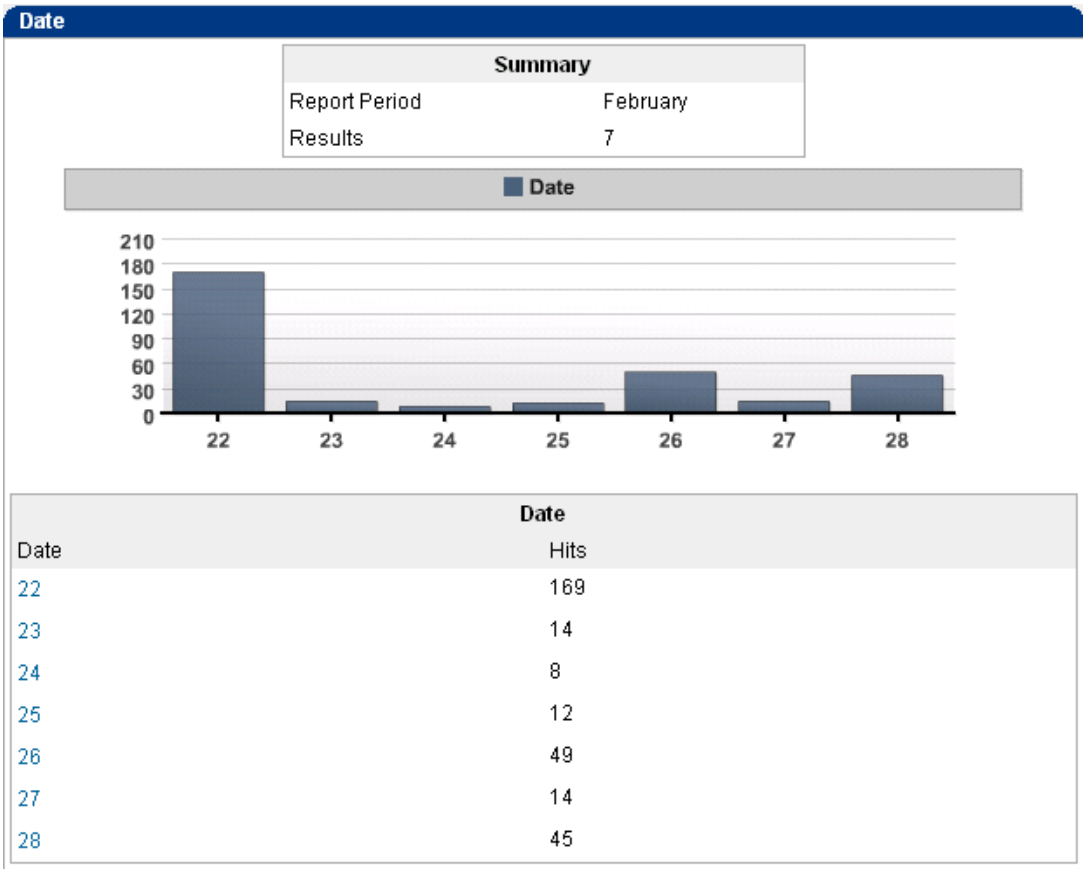


Figura 3.6 Detalle de los días en los que se recibieron mayor cantidad de ataques y número de intentos recibidos

En la Figura 3.7 se observa las direcciones IP de los intrusos que intentaron atacar al sistema. Puede observarse que la más insistente es una red hecha nat por el mismo proveedor de internet de la DIRECCIÓN NACIONAL DE MIGRACIÓN. Muchas veces los ataques pueden llegar por medio del iternet de alguna Jefatura o Sub Jefatura provincial, dado que actualmente no hay una figura de internet centralizada.

Además en la Figura 3.7 se observa el detalle de los días en los que se realizaron los ataques: los días 22 y 23 la IP 192.168.198.104 ha tratado 165 veces de violar la seguridad del servidor.

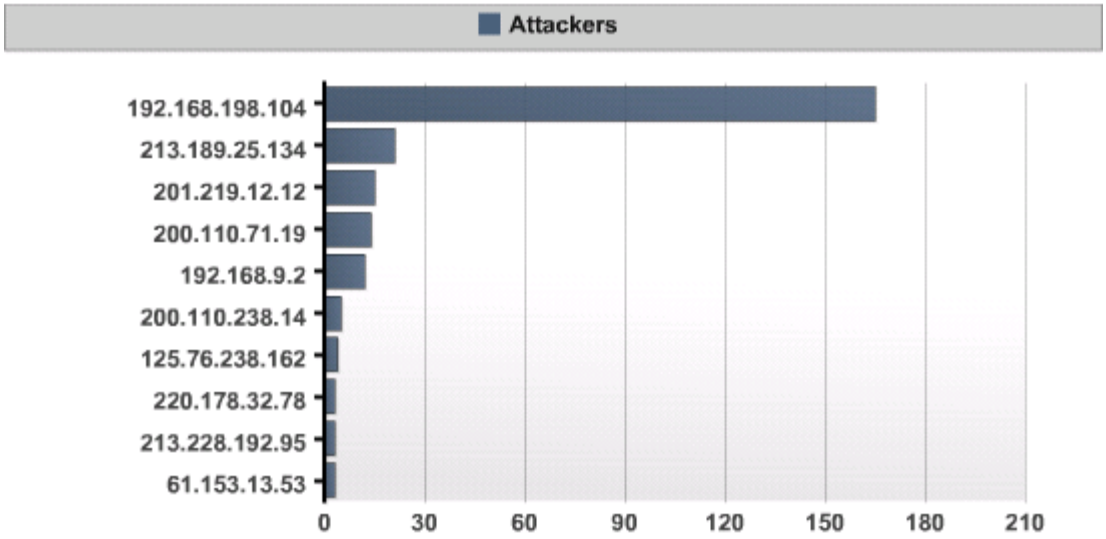


Figura 3.7 Direcciones IP de los intrusos que intentaron atacar al sistema

Attackers		
Attackers	Hits	Date
192.168.198.104	165	22 23
213.189.25.134	21	28
201.219.12.12	15	26
200.110.71.19	14	26
192.168.9.2	12	22
200.110.238.14	5	25 26 28
125.76.238.162	4	23 25 27 28
213.228.192.95	3	27
61.153.13.53	3	25 26 28
220.178.32.78	3	25 26 28

Figura 3.8 Detalle de los días en los que se realizaron los ataques

En la Figura 3.9 se observa las direcciones IP que fueron víctimas de ataques por usuarios internos de la DIRECCIÓN NACIONAL DE MIGRACIÓN Esto se da cuando el servidor registra intentos de conexión a servidores o aplicaciones externas a la institución, generalmente se da por usar aplicaciones no autorizadas o los famosos P2P (Aplicaciones punto a punto) como kazZa, Ares, que entre otros sirven para descargar todo tipo de ficheros como aplicaciones, música, videos, fotos, etc. En la Figura 3.10 se observa el detalle de los días con número

de intentos de conexión en los que se recibieron los ataques por usuarios de la DIRECCIÓN NACIONAL DE MIGRACIÓN.

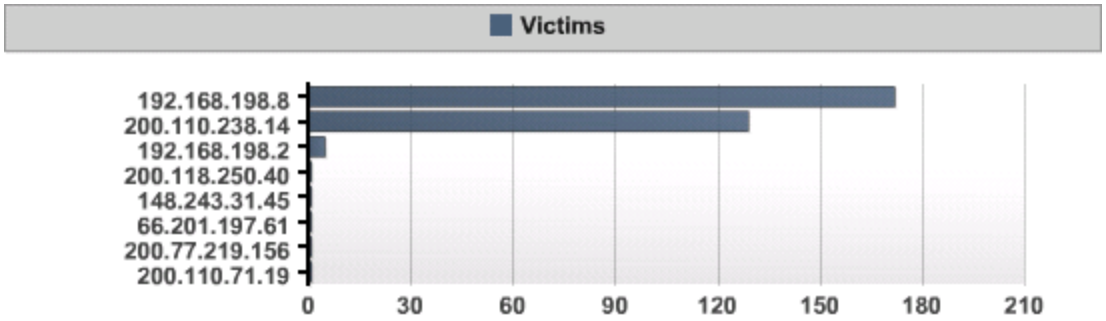


Figura 3.9 Direcciones IP que fueron víctimas de ataques por usuarios de la DIRECCIÓN NACIONAL DE MIGRACIÓN

Victims

Victims	Hits	Date
192.168.198.8	172	22 23
200.110.238.14	129	23 24 25 26 27 28
192.168.198.2	5	22 23
66.201.197.61	1	26
200.77.219.156	1	26
200.110.71.19	1	26
148.243.31.45	1	25
200.118.250.40	1	28

Figura 3.10 Detalle de los días, con número de intentos en los que se recibieron los ataques.

En la Figura 3.11 se observa el detalle de los protocolos utilizados para realizar los ataques a la DIRECCIÓN NACIONAL DE MIGRACIÓN, en este caso, se observa que el más usado es UDP. En la Figura 3.13 se detalla el número de intentos de ataques realizados. Dependiendo del protocolo usado, se ve que hay un total de 232 intentos con el protocolo UDP, 55 intentos con TCP y 24 intentos con ICMP.

En la Figura 3.12 se observa el detalle de los puertos usados para los ataques (ver Anexo F). El más usado como se puede ver en la Figura 3.14 es el UDP 161, con 180 intentos de ataques, en los días 22, 23 y 26.

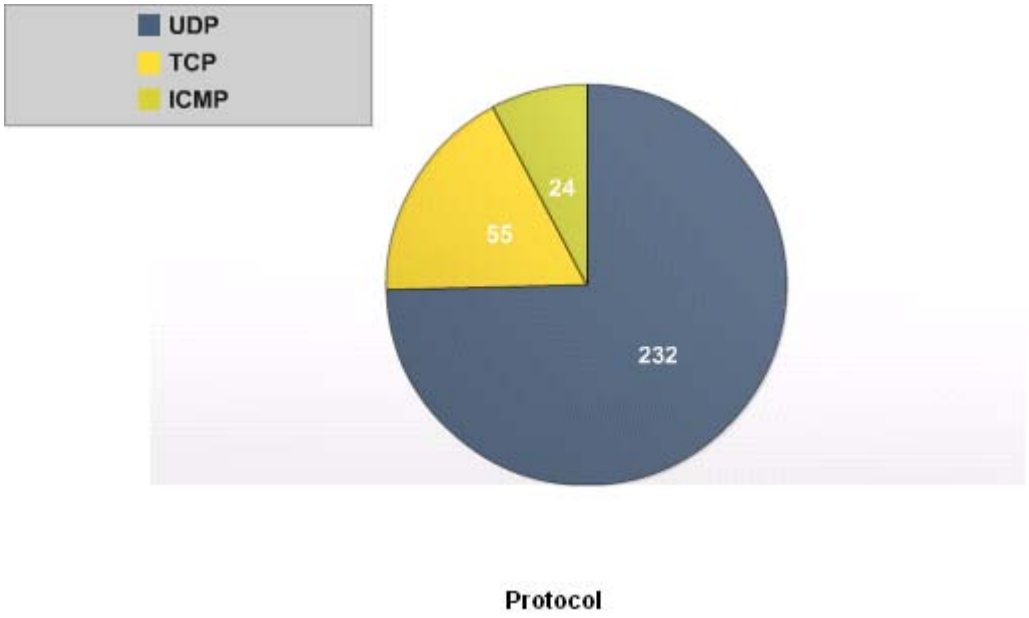


Figura 3.11 Detalle de los protocolos usados para realizar los ataques.

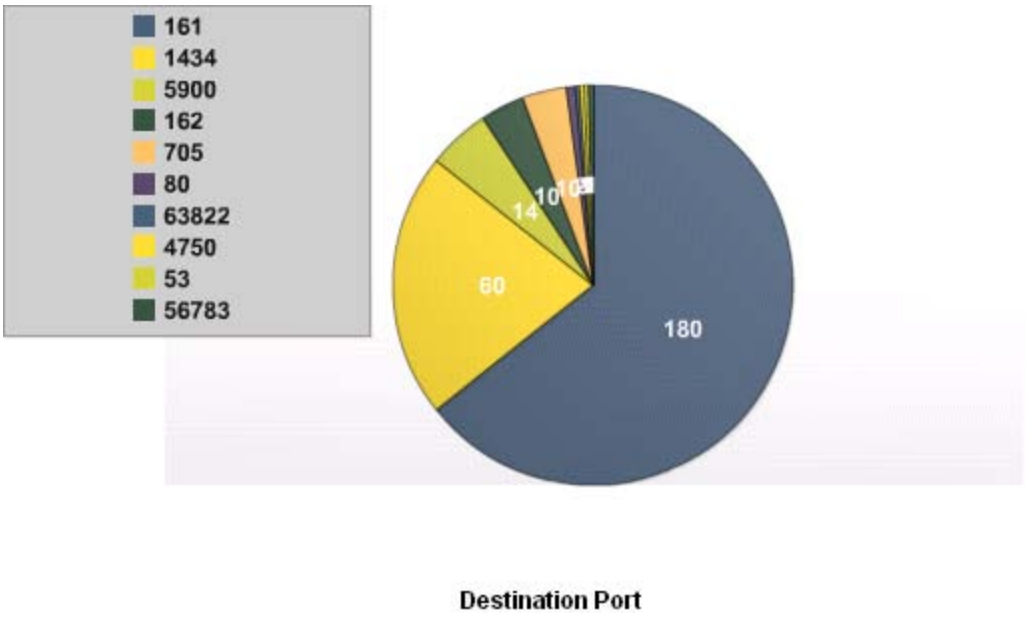


Figura 3.12 Detalle de los puertos por los que se intento realizar los ataques, dependiendo del protocolo usado.

Protocol	
Protocol	Hits
UDP	232
ICMP	24
TCP	55

Figura 3.13 Detalle del número de intentos de ataques realizados dependiendo del protocolo usado.

Destination Port		
Destination Port	Hits	Date
161	180	22 23 26
1434	60	23 24 25 26 27 28
5900	14	26 27 28
705	10	26
162	10	26
80	2	23
53	1	26
56783	1	25
4750	1	28
63822	1	26

Figura 3.14 Detalle de los puertos por los que se intento realizar los ataques, con fecha y número de intentos realizados.

Conclusión de las muestras de las gráficas de detección de intrusos:

Según los gráficos obtenidos se procedió a clasificar los distintos sistemas de detección de intrusos.

La primera forma de clasificar se realiza a partir de sistemas en tiempo real y entre aquellos que no lo son.

Los sistemas en tiempo real permanecen siempre chequeando el sistema, buscando alguna señal de un incidente de seguridad, que si ocurre, es detectado provocando inmediatamente una alarma. Los sistemas de detección de intrusos que no son de tiempo real, se usan generalmente cuando se sabe o presume que se está ante un incidente de seguridad, entonces se usa para recopilar información del tipo y alcance de esta incidencia, generalmente sobre registros o información del sistema y del posible atacante.

La segunda forma de clasificar es más rigurosa y se realiza según los medios para monitorizar los ataques que utilizan los sistemas de detección de intrusos.

Según esta clasificación existen cuatro tipos de sistemas:

- **Basados en el host:** estos sistemas recopilan información del sistema para realizar un análisis a profundidad de las posibles incidencias pero siempre desde el punto de vista del propio sistema y con sus recursos.

- **Basados en la red:** sistemas que observan el tráfico de red monitoreando y escaneando indicios de algún ataque conocido. Generalmente un interfaz en modo promiscuo buscando datos sobre una red. (Suelen pertenecer también al tipo de tiempo real).

- **Basados en la aplicación: e**stos recopilan información de una aplicación activa en el sistema (por ejemplo los logs de la web) y buscan posibles evidencias en los datos. La diferencia con los basados en host es que estos usan los propios recursos como detectores de intrusos y en el caso de aplicación los datos han de ser filtrados para ser tratados como alarmas.

- **Basados en el objetivo: e**stos monitores se basan en salvaguardar la integridad del objetivo que podría ser cualquier recurso del sistema (por ejemplo el sistema ERP).

Y por último se puede diferenciar los tipos de sistemas de detección de intrusos según el tipo de análisis que realiza:

- **Detección de uso inadecuado:** en estos casos el sistema busca una guía de un ataque muy bien definido.

- **Detección de alguna anomalía:** se examina sobre el sistema algún tipo de anomalía que pueda hacer creer que hay un incidente de seguridad, pero que no necesariamente puede ser provocada por esa acción o anomalía.

3.2.2 Web Proxy Squid

El Reporte del Web Proxy muestra las estadísticas de uso de Internet. Entre otras estadísticas, se puede observar el uso de ancho de banda del canal mediante: Dirección IP, Sitio Web, fecha.

En las gráficas tomadas a partir el 22 de enero se observa el mal uso que los usuarios le dan al internet, navegando en páginas de distracción de adultos, páginas de juegos, páginas de compras en línea, páginas de ocio y mail gratuito (ver Figura 3.16 – 3.22); además se observa el ancho de banda que cada IP usa con el número de conexiones (ver Figura 3.15).

NUM	USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILISEC	%TIME
1	192.168.7.26	21K	282M	22.31%	12.26%	87.74%	14:26:25	52M	18.45%
2	192.168.7.111	23K	200M	15.82%	2.72%	97.28%	13:05:27	48M	16.72%
3	192.168.7.57	13K	140M	11.03%	4.61%	95.39%	07:26:52	27M	9.51%
4	192.168.7.1	13K	98M	7.77%	2.94%	97.06%	06:17:04	23M	8.03%
5	192.168.16.59	14K	81M	6.34%	7.87%	92.13%	05:07:36	19M	6.55%
6	192.168.7.27	10K	58M	4.53%	2.69%	97.31%	03:55:35	15M	5.02%
7	192.168.7.33	16K	48M	3.80%	1.44%	98.56%	04:07:55	15M	5.28%
8	192.168.7.52	8K	42M	3.27%	1.66%	98.34%	02:15:10	9M	2.88%
9	192.168.7.56	4K	32M	2.47%	2.28%	97.72%	01:47:55	7M	2.30%
10	192.168.7.42	7K	31M	2.46%	3.72%	96.28%	01:50:32	7M	2.35%
11	192.168.7.23	2K	27M	2.13%	3.93%	96.07%	01:02:02	4M	1.32%
12	192.168.7.40	6K	27M	2.12%	7.86%	92.14%	01:37:12	6M	2.07%
13	192.168.7.34	6K	24M	1.87%	10.27%	89.73%	02:05:58	8M	2.68%
14	192.168.7.3	774	23M	1.82%	0.97%	99.03%	00:44:32	3M	0.95%
15	192.168.7.53	4K	23M	1.77%	5.72%	94.28%	01:02:41	4M	1.33%
16	192.168.7.50	3K	22M	1.68%	2.29%	97.71%	00:43:23	3M	0.92%
17	192.168.7.37	111	20M	1.58%	0.30%	99.70%	00:21:54	2M	0.47%
18	192.168.7.29	2K	13M	0.99%	23.00%	77.00%	02:37:36	10M	3.36%
19	192.168.7.25	2K	13M	0.96%	5.42%	94.58%	01:27:19	6M	1.86%
20	192.168.7.44	2K	12M	0.93%	3.06%	96.94%	01:09:57	5M	1.49%
21	192.168.7.51	766	11M	0.81%	0.49%	99.51%	00:24:34	2M	0.52%
22	192.168.7.49	4K	10M	0.78%	1.43%	98.57%	00:59:19	4M	1.26%
23	192.168.7.30	902	7M	0.51%	5.79%	94.21%	00:39:35	3M	0.84%
24	192.168.7.36	2K	7M	0.50%	5.25%	94.75%	01:05:40	4M	1.40%

25	192.168.7.43	106	6M	0.41%	0.03%	99.97%	00:09:56	596K	0.21%
26	192.168.7.28	1K	5M	0.38%	11.80%	88.20%	00:19:24	2M	0.41%
27	192.168.7.35	2K	4M	0.28%	11.94%	88.06%	00:29:37	2M	0.63%
28	192.168.7.32	356	4M	0.25%	1.75%	98.25%	00:09:23	563K	0.20%
29	192.168.7.55	593	3M	0.17%	9.67%	90.33%	00:08:43	523K	0.19%
30	192.168.7.39	786	2M	0.10%	2.68%	97.32%	00:08:38	518K	0.18%
31	192.168.7.31	316	990K	0.08%	34.69%	65.31%	00:24:46	2M	0.53%
32	192.168.7.47	212	956K	0.08%	1.74%	98.26%	00:03:01	181K	0.06%
33	192.168.7.41	49	128K	0.01%	2.27%	97.73%	00:00:19	20K	0.01%
34	192.168.7.38	30	124K	0.01%	13.48%	86.52%	00:00:18	19K	0.01%
35	200.110.71.19	1	1K	0.00%	100.00%	0.00%	00:00:00	104	0.00%
	TOTAL	**169K**	**2G**		**5.89%**	**94.11%**	**78:16:34**	**282M**	
	AVERAGE	**5K**	**37M**				**02:14:11**	**9M**	

Figura 3.15 Detalle de los hosts que navegaron en Internet con número de conexiones y cantidad de ancho de banda usado.

.

NUM	ACCESSED SITE	CONNECT	BYTES	TIME
1	207.46.107.14	6K	3M	5M
2	207.46.107.35	5K	2M	4M
3	207.46.107.34	4K	2M	4M
4	207.46.107.55	4K	2M	3M
5	207.46.107.13	3K	2M	3M
6	207.46.107.76	3K	2M	3M
7	pagead2.googlesyndication.com	3K	15M	4M
8	207.46.107.56	3K	2M	3M
9	www.gaydargirls.com	3K	9M	2M
10	207.46.107.77	3K	2M	3M
11	207.46.107.22	3K	2M	2M
12	bay130.oe.hotmail.com	3K	26M	4M
13	www.dgp-polinal.gov.ec	2K	7M	12M
14	rad.msn.com	2K	3M	2M
15	www.eluniverso.com	2K	4M	781K
16	www.programas-gratis.net	2K	20M	4M
17	msgr.dlservice.microsoft.com	2K	37M	3M
18	wwwp2.pichincha.com	2K	4M	325K
19	www.google.com.ec	2K	9M	2M
20	www.hi5.com	2K	18M	4M
21	images.hi5.com	1K	9M	2M
22	www02.pichincha.com:443	1K	3M	766K
23	ak.imgfarm.com	1K	6M	900K
24	www.powerpoints.org	1K	3M	563K
25	tbn0.google.com	1K	5M	901K
26	us.i1.yimg.com	1K	3M	520K
27	207.46.107.43	1K	660K	791K
28	www.soloadultos.net	1K	4M	672K

29	www01.pichincha.com:443	1K	3M	645K
30	www03.pichincha.com:443	1K	2M	593K
31	wwwp1.pichincha.com	1K	3M	240K
32	www.pnud.org.ec	928	2M	248K
33	www.bce.fin.ec	909	7M	805K
34	www.accivalores.com	893	4M	469K
35	mail.opi.yahoo.com	853	406K	476K
36	urs.microsoft.com:443	850	6M	2M
37	157.100.207.49:443	815	6M	6M
38	www.google-analytics.com	812	799K	303K
39	online.mmjbdata.com	761	273K	173K
40	www.migracion.gov.ec	756	2M	198K
41	www.multitrabajos.com	744	6M	848K
42	www.aduana.gov.ec	714	3M	419K
43	www.porfinempleo.com	678	3M	847K
44	services.msn.com	660	492K	5M
45	www.terra.com	653	3M	360K
46	photos.hi5.com	638	2M	680K

Figura 3.16 Páginas más visitadas por los usuarios (Parte 1)

47	www.orange.es	626	498K	71K
48	gfx1.hotmail.com	620	409K	109K
49	graphics.amigos.com	617	728K	267K
50	galerias.muyzorras.com	603	633K	144K
51	200.93.225.45	596	3M	2M
52	row.bc.yahoo.com	590	248K	544K
53	images.picsearch.com	580	2M	432K
54	www.google.com	575	948K	335K
55	gateway.messenger.hotmail.com	530	218K	336K
56	media.mediaplazza.com	529	557K	132K
57	hp.msn.com	498	546K	131K
58	www.voguenovias.com	497	855K	361K
59	www.noviasynovios.cl	479	7M	2M
60	images.google.com.ec	472	3M	365K
61	www.monografias.com	470	3M	276K
62	67.15.236.231	448	2M	217K
63	latam.msn.com	424	4M	504K
64	ad.doubleclick.net	418	252K	248K
65	www.daler.ru	408	7M	2M
66	es.wikipedia.org	393	4M	577K
67	h.msn.com	390	175K	409K
68	www.microsoft.com	378	2M	492K
69	music2.hi5.com	369	150M	25M
70	login.live.com:443	369	2M	536K
71	img.rincondelvago.com	368	364K	53K
72	207.46.108.76	362	148K	238K
73	l.yimg.com	356	2M	192K
74	www.dlh.lahora.com.ec	352	560K	90K
75	gfx2.hotmail.com	351	246K	117K

76	ads1.msn.com	349	3M	254K
77	www.evanovias.com	345	2M	313K
78	securityresponse.symantec.com	341	572K	194K
79	us.js2.yimg.com	340	7M	711K
80	stb.msn.com	340	2M	277K
81	www.sri.gov.ec	332	2M	198K
82	ad.es.doubleclick.net	328	380K	244K
83	207.46.111.43	327	138K	192K
84	previews.peliculasxsms.com	325	2M	316K
85	www.porta.net	310	4M	588K
86	ad.yieldmanager.com	304	983K	297K
87	www.arq.com.mx	304	232K	141K
88	www1.addfreestats.com	292	355K	260K
89	www.espe.edu.ec	288	2M	183K
90	chat.amigos.com	287	2M	336K
91	pms.mercadolibre.com	286	7M	746K

Figura 3.17 Páginas más visitadas por los usuarios (Parte 2)

92	eur.i1.yimg.com	286	747K	157K
93	online.musicmatch.com	282	5M	793K
94	www.8notes.com	277	702K	165K
95	ec1.images-amazon.com	271	635K	180K
96	gallys.nastydollars.com	268	3M	321K
97	cp.intl.match.com	264	2M	170K
98	compro.viewpoint.com	264	191K	87K
99	br.i1.yimg.com	263	3M	285K
100	192.168.7.24:81	259	3M	358K
101	www.symantec.com	258	2M	259K
102	books.google.com.ec	253	2M	313K
103	c.msn.com	253	117K	159K
104	ads3.qsoft.co.uk	251	244K	211K
105	by109fd.bay109.hotmail.msn.com	250	4M	401K
106	info.music.metaservices.microsoft.com	248	705K	174K
107	login.live.com	245	2M	302K
108	www.nestle.com.ec	244	2M	240K
109	g.ceipmsn.com	244	163K	84K
110	eur.a1.yimg.com	241	5M	421K
111	www.free-scores.com	241	2M	349K
112	207.46.108.56	238	187K	153K
113	www.kennedyviolins.com	237	3M	446K
114	www.quenovias.com	236	722K	263K
115	217.116.19.245	231	2M	732K
116	upload.wikimedia.org	230	2M	412K
117	www.tuparada.com	223	2M	274K
118	ax.phobos.apple.com.edgesuite.net	221	349K	51K
119	a.rad.msn.com	220	193K	136K
120	pamela.celebden.com	219	690K	138K
121	www.windowsmedia.com	217	754K	109K

122	windowsmedia.com	214	183K	102K
123	b.rad.msn.com	212	379K	157K
124	www.fotografia-digital.info	210	707K	198K
125	latam.real.com	209	224K	69K
126	search.viewpoint.com	208	2M	345K
127	p.videosz.com	208	578K	135K
128	u.univision.com	208	450K	100K
129	by19fd.bay19.hotmail.msn.com	204	4M	595K
130	www.epson.com	203	2M	221K
131	estb.msn.com	203	2M	196K
132	www.musicaparatodos.com	198	902K	279K
133	www.loteria.com.ec	197	604K	165K
134	www.iberporno.com	195	2M	159K
135	content.yieldmanager.edgesuite.net	192	4M	394K
136	www.mercadolibre.com.ec	191	542K	118K

Figura 3.18 Páginas más visitadas por los usuarios (Parte 3)

137	www.ecuadorinmediato.com	190	210K	179K
138	by104fd.bay104.hotmail.msn.com	187	4M	310K
139	www.zappingclub.com	185	767K	300K
140	media.fastclick.net	182	110K	86K
141	pics.homere.imsp.net	181	855K	264K
142	overture.geoads.net	180	137K	104K
143	g.latam.msn.com	180	77K	84K
144	www.meusdownloads.com.br	177	436K	73K
145	es.yahoo.com	175	2M	295K
146	declaraciones.sri.gov.ec:443	174	420K	404K
147	www.di-arezzo.es	172	546K	127K
148	stc.msn.com	172	508K	114K
149	descargas.muyzorras.com	170	412K	68K
150	ad.terra.com	170	92K	104K
151	www.playboy.com	168	4M	845K
152	images.taketeens.com	167	2M	382K
153	www.be2.es	167	580K	122K
154	www.utpl.edu.ec	166	814K	214K
155	www.amateurporn.ws	166	628K	107K
156	newsrss.bbc.co.uk	165	3M	163K
157	php.terra.com	161	339K	340K
158	cdn.cdmetrix.com	161	144K	80K
159	by23fd.bay23.hotmail.msn.com	160	4M	484K
160	foroviolin.hollosite.com	160	2M	337K
161	www.zonapediatrica.com	160	466K	100K
162	www.potaje.com	158	2M	240K
163	traffic.waypointcash.com	158	740K	245K
164	notlim.webcindario.com	157	329K	124K
165	www.impresionesweb.com	153	250K	99K
166	www.youtube.com	152	2M	369K

167	64.76.220.18	150	2M	640K
168	sexyfamosas.com	148	456K	112K
169	mx.yahoo.com	146	4M	535K
170	es.update.toolbar.yahoo.com	145	4M	632K
171	www.peliculasxsms.com	145	2M	199K
172	www.revistasebo.com	144	3M	359K
173	include.ebaystatic.com	144	2M	429K
174	hm.msn.com	144	225K	92K
175	www.cooperando.ws	143	950K	81K
176	previews.pornopeliculas.com	140	2M	142K
177	migracion.gov.ec	140	537K	113K
178	www.grandesestrellas.com	139	2M	189K
179	userphotos.hi5.com	139	740K	197K
180	adv.bcnclick.com	139	107K	715K
181	207.46.108.55	137	58K	137K
182	www.terra.es	136	378K	76K
183	207.46.108.34	136	65K	94K

Figura 3.19 Páginas más visitadas por los usuarios (Parte 4)

184	ad.directanetworks.com	135	77K	90K
185	www.mundogar.com	134	609K	131K
186	pics.mediaplazza.com	133	813K	213K
187	www.celebwelove.com	133	355K	113K
188	www.sonnerie.net	132	325K	95K
189	runonce.msn.com	132	262K	58K
190	www.abcdatos.com	132	192K	51K
191	go.microsoft.com	132	77K	79K
192	smileys.smileycentral.com	131	2M	244K
193	www.mutualistapichincha.com	130	780K	109K
194	ad.strict.tbn.ru	129	848K	587K
195	ad.600.tbn.ru	129	790K	681K
196	www.uprh.edu	129	453K	135K
197	consumerdownloads.ca.com	127	702K	77K
198	www.internetdelecuador.com	126	263K	27K
199	www.argentinianexplorer.com	125	801K	211K
200	www.hotmail.msn.com	124	244K	174K
201	207.46.108.14	124	46K	117K
202	www.bancodeputas.com	123	2M	359K
203	www.ecuabinn.com	122	5M	522K
204	www.todocorazon.net	122	959K	307K
205	www.5000fotos.com	121	467K	96K
206	www.hoy.com.ec	121	345K	82K
207	msnportal.112.2o7.net	121	67K	75K
208	www.contracorruptos.org	120	3M	346K
209	view.atdmt.com	120	253K	101K
210	as.starware.com	119	113K	59K
211	tooltips.hotbar.com	118	595K	149K
212	www.superwarehouse.com	118	481K	80K
213	imgserv.ya.com	118	320K	165K
214	www.toolbardearquitectura.com	118	286K	81K
215	pics.ebaystatic.com	118	244K	59K
216	by115fd.bay115.hotmail.msn.com	117	3M	337K
217	www.celebritiescentral.net	117	435K	109K
218	www.wordreference.com	116	923K	272K
219	www.dibujotecnico.com	116	649K	106K
220	ad.bus100.tbn.ru	115	406K	396K
221	157.100.207.45:443	114	951K	3M
222	search.live.com	113	2M	181K
223	www.snort.org	113	222K	36K
224	www.diablateen.com	112	467K	138K
225	secure.footprint.net:443	112	382K	119K
226	www.nlm.nih.gov	112	325K	27K
227	www.superguarras.com	111	880K	89K
228	www.videosgratistgp.com	111	369K	71K
229	207.46.108.22	111	71K	80K
230	get.live.com	110	700K	109K

Figura 3.20 Páginas más visitadas por los usuarios (Parte 5)

231	www.bp.fin.ec	110	313K	103K
232	www.muyzorras.com	109	994K	122K
233	a.tribalfusion.com	109	116K	71K
234	thumbs.tgpgalerias.com	108	2M	587K
235	72.18.205.210	108	2M	226K
236	www.pornopeliculas.com	108	978K	71K
237	www.herbspro.com	108	616K	147K
238	www.tonterias.com	108	185K	306K
239	198.104.137.238	107	906K	113K
240	www.deprati.com.ec	107	331K	39K
241	mx.update.companion.yahoo.com	106	50K	59K
242	www.solodrivers.com	104	286K	141K
243	global.msads.net	104	164K	72K
244	www.server4business.com	103	2M	300K
245	elcomercio.terra.com.ec	103	529K	131K
246	secure-uk.imrworldwide.com	103	74K	73K
247	links.traffyc.com	102	179K	49K
248	activex.microsoft.com	102	19K	47K
249	www.tetas-enormes.com.ar	101	402K	183K
250	wwwme.org	101	309K	127K
251	www.raulybarra.com	100	2M	285K
252	207.46.108.43	100	46K	75K
253	counter.yadro.ru	100	33K	88K
254	www.mylingeriestore.com	99	7M	2M
255	web.educastur.princast.es	99	319K	77K
256	www.lagaleriadehoy.com	99	258K	89K
257	www.marathon-sports.com	99	145K	32K
258	www.blubster.com	98	12M	947K
259	galleries.latinaexposed.com	98	365K	95K
260	gfx.sheetmusicplus.com	98	360K	119K
261	www.elpais.com	97	710K	135K
262	publico.bce.fin.ec:443	97	574K	984K
263	www.eset.com	97	319K	283K
264	stj.msn.com	96	852K	75K
265	www.100x100negras.com	96	422K	73K
266	al.pricegrabber.com	96	104K	40K
267	imagenes.condenet.es	95	2M	118K
268	cbtads.overture.com	95	277K	85K
269	c.latam.msn.com	95	38K	73K
270	www.ebay.com	94	4M	914K
271	www.tripod.lycos.es	94	347K	60K
272	www.onlinetv3.de	94	201K	73K
273	logs.eresmas.com	94	45K	76K
274	foro.nuvisystem.com	93	909K	97K
275	gaydarradio.com	92	581K	80K

Figura 3.21 Páginas más visitadas por los usuarios (Parte 6)

276	www.univision.com	92	432K	72K
277	galleries.maturegonewild.com	91	463K	73K
278	www.todocancer.com	91	301K	41K
279	www.lenntech.com	90	608K	80K
280	galleries.madurasguarras.com	89	470K	86K
281	www.inzacard.com	88	2M	261K
282	video.google.com	88	673K	202K
283	public-contentv4.rapid-pass.net	88	556K	132K
284	www.blogsmithmedia.com	88	235K	38K
285	www.asifunciona.com	88	180K	53K
286	www.publiboda.com	88	137K	31K
287	ads.us.e-planning.net	88	90K	45K
288	us.ebayobjects.com	88	21K	35K
289	pamelaanderson.publispain.com	87	535K	70K
290	i.imdb.com	87	311K	91K
291	www.laprensa.com.ni	87	258K	41K
292	m1.webstats4u.com	87	38K	59K
293	www.liveinternet.ru	87	26K	49K
294	www.videosgratisxxx.com	86	661K	125K
295	www.consumaseguridad.com	86	371K	63K
296	www.unileon.es	86	210K	71K
297	www1.porta.net	86	133K	19K
298	images.mixmail.ya.com	86	124K	89K
299	logc31.xiti.com	86	40K	63K
300	liveupdate.symantecliveupdate.com	85	26M	2M

Figura 3.22 Páginas más visitadas por los usuarios (Parte 7)

En el reporte de usuarios que accedieron a páginas no permitidas por la institución (ver Figura 3.23), se observa que aproximadamente un 90% son paginas de adultos, por ende esta será una de las políticas más duras que se implementará en el nuevo servidor proxy, ya que del 100% del tiempo efectivo en las horas de trabajo, un 65% lo utilizan para ver este tipo de páginas, teniendo un 35% de efectividad en las tareas diarias de trabajo por usuario. Como se mencionó anteriormente, son valores aproximados no son reales.

NUM	ACCESSED SITE	USERS
1	007musicvideos.com	192.168.7.111
2	03.sharedsource.org	192.168.7.111
3	140.99.105.62	192.168.7.111
4	157.100.207.45:443	192.168.7.25 192.168.7.29
5	157.100.207.49:443	192.168.7.29 192.168.7.31
6	192.168.7.1:8080	192.168.7.1
7	192.168.7.24:81	192.168.16.59 192.168.7.1
8	192.168.7.55:8090	192.168.7.1
9	195.235.81.13	192.168.7.56
10	198.104.137.238	192.168.7.42
11	200.110.238.14	192.168.7.1 200.110.71.19
12	200.93.225.45	192.168.7.56
13	201.219.1.25	192.168.7.1
14	206.161.121.115	192.168.7.57
15	207.234.208.71:11128	192.168.7.57
16	207.46.107.13	192.168.16.59 192.168.7.1 192.168.7.23 192.168.7.26 192.168.7.27 192.168.7.33 192.168.7.34 192.168.7.35 192.168.7.39 192.168.7.49 192.168.7.52
547	descargas.muyzorras.com	192.168.7.111 192.168.7.34
788	galerias.muyzorras.com	192.168.7.111 192.168.7.34
1653	sexo.webspacemania.com	192.168.7.111
1654	sexshop.scdata.com	192.168.7.111
1655	sexyfamosas.com	192.168.7.111
2079	www.bancodeputas.com	192.168.7.111 192.168.7.34
2426	www.iberporno.com	192.168.7.1 192.168.7.111 192.168.7.53
2704	www.pornopeliculas.com	192.168.7.1 192.168.7.111
2790	www.sexo%20con%20animales.com	192.168.7.1
2791	www.sexoactual.com	192.168.7.111
2792	www.sexoalextremo.com	192.168.7.33
2793	www.sexoanonimo.net	192.168.7.111
2794	www.sexoenlared.com	192.168.7.33
2795	www.sexoentumail.com	192.168.7.111
2796	www.sexoportada.com	192.168.7.111
2797	www.sexozu.com	192.168.7.111
2798	www.sexyfamosas.com	192.168.7.111
2825	www.soloadultos.net	192.168.7.111
2876	www.tetas19.com	192.168.7.111
2877	www.tetas-enormes.com	192.168.7.111
2878	www.tetas-enormes.com.ar	192.168.7.111
2879	www.tetas-tetas.com	192.168.7.111
2969	www.videochaterotico.com	192.168.7.111
2970	www.videochaterotico.com:443	192.168.7.111
2971	www.videochatxamateur.com	192.168.7.111
2972	www.video_de_negras_pornos_gratis.webcams-1-sms.info	192.168.7.111
2973	www.videosdecachondeo.com	192.168.7.42 192.168.7.56
2974	www.videosgratistgp.com	192.168.7.111
2975	www.videosgratisxxx.com	192.168.7.111
2976	www.videospornosms.com	192.168.7.34
2977	www.videosxrobados.com	192.168.7.111

Figura 3.23 Detalle de las páginas visitadas por los hosts con número de IP.

En el reporte de las descargas realizadas por los usuarios (ver Figura 3.24) se observa que muchas de las descargas son de páginas de Microsoft, por lo que se asume que son actualizaciones automáticas de cada sistema operativo, sin embargo existen también descargas de páginas como www.hi5.com que son de

ocio, por lo que en la implementación, el Departamento de Sistema de la DIRECCIÓN NACIONAL DE MIGRACIÓN deberá establecer políticas de descargas autorizadas sólo para las paginas que crea convenientes.

Downloads Report

USERID	IP/NAME	DATE/TIME	ACCESSED SITE
192.168.16.59	192.168.16.59	02/27/2007-14:40:33	http://fpdownload.macromedia.com/pub/shockwave/cabs/flash/swflash.cab
		02/27/2007-14:40:42	http://fpdownload.macromedia.com/pub/shockwave/cabs/flash/swflash.cab
		02/27/2007-14:41:01	http://fpdownload.macromedia.com/get/shockwave/cabs/flash/swflash.cab
		02/27/2007-14:41:30	http://fpdownload.macromedia.com/get/shockwave/cabs/flash/swflash.cab
		02/27/2007-15:05:53	http://fpdownload.macromedia.com/pub/shockwave/cabs/flash/swflash.cab
		02/27/2007-15:23:46	http://fpdownload.macromedia.com/get/shockwave/cabs/flash/swflash.cab
		02/27/2007-21:30:29	http://activex.microsoft.com/objects/ocget.dll
		02/27/2007-21:33:19	http://activex.microsoft.com/objects/ocget.dll
		02/27/2007-21:34:02	http://activex.microsoft.com/objects/ocget.dll
		02/27/2007-21:34:50	http://activex.microsoft.com/objects/ocget.dll
192.168.7.111	192.168.7.111	02/26/2007-15:40:14	http://activex.microsoft.com/objects/ocget.dll
		02/26/2007-15:40:14	http://codecs.microsoft.com/isapi/ocget.dll
		02/26/2007-17:02:07	http://upload.wikimedia.org/wikipedia/commons/thumb/f/ff/Cysticercosis.jpeg/250px-Cysticercosis
		02/26/2007-18:02:49	http://activex.microsoft.com/objects/ocget.dll
		02/26/2007-18:02:49	http://activex.microsoft.com/objects/ocget.dll
		02/26/2007-18:02:49	http://activex.microsoft.com/objects/ocget.dll
		02/26/2007-18:02:49	http://activex.microsoft.com/objects/ocget.dll
		02/26/2007-18:02:50	http://activex.microsoft.com/objects/ocget.dll
		02/26/2007-18:02:50	http://activex.microsoft.com/objects/ocget.dll
		02/26/2007-18:02:50	http://activex.microsoft.com/objects/ocget.dll
192.168.7.23	192.168.7.23	02/26/2007-12:30:11	http://d.yimg.com/us.yimg.com/p/net/20070223/thumb.8f7e0b360bfd8dfcca417b5218a6c7d4.jpeg
		02/27/2007-09:59:01	http://liveupdate.symanteclive update.com/automatic$20liveupdate_2.6.18_spanish_livetri.zip
		02/27/2007-09:59:01	http://liveupdate.symanteclive update.com/liveupdate_2.6.18_spanish_livetri.zip
		02/27/2007-09:59:02	http://liveupdate.symanteclive update.com/avenge$20microdefs25 $20savcorp10_microdefsb.curdefs_symalllanguages_livetri.zip
		02/27/2007-09:59:02	http://liveupdate.symanteclive update.com/avenge$20microdefs25 $20savcorp10_microdefsb.feb_symalllanguages_livetri.zip
		02/27/2007-09:59:02	http://liveupdate.symanteclive update.com/symantec$20antivirus$20corporate$20client_10.0_spa
		02/27/2007-10:00:01	http://sqm.msn.com/sqm/messenger/sqmserver.dll
		02/27/2007-10:03:39	http://liveupdate.symanteclive update.com/automatic$20liveupdate_2.6.18_spanish_livetri.zip

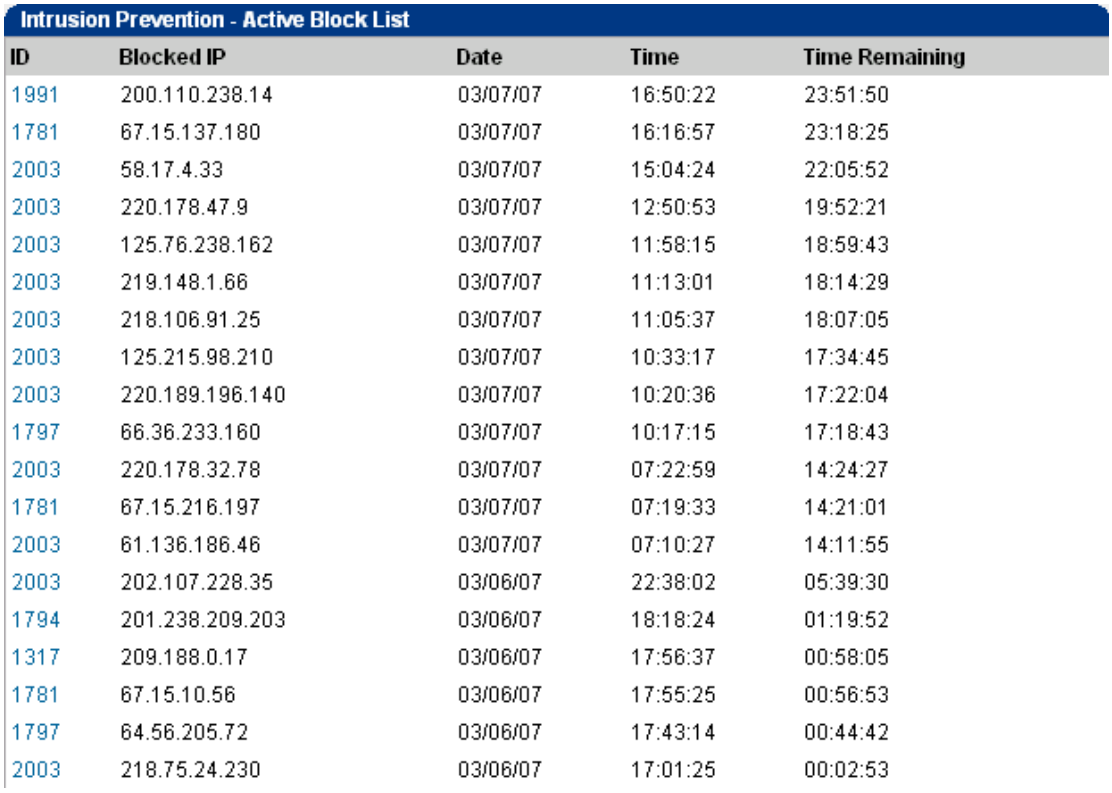
192.168.7.25	192.168.7.25	02/26/2007-13:25:33	http://sqm.msn.com/sqm/messenger/sqmserver.dll
192.168.7.26	192.168.7.26	02/26/2007-16:20:36	http://sqm.msn.com/sqm/messenger/sqmserver.dll
		02/26/2007-16:34:34	http://activex.microsoft.com/objects/ocget.dll
		02/26/2007-16:34:35	http://codecs.microsoft.com/isapi/ocget.dll
		02/26/2007-17:28:11	http://www.blubster.com/BlubsterSetup.exe
		02/26/2007-18:02:36	http://ring.homere.jmsp.net/drt/ress_hifi/mus-per-magic-shimmer-cte01-92-2.mp3
		02/26/2007-18:02:46	http://ring.homere.jmsp.net/drt/ress_hifi/mus-per-magic-shimmer-cte01-92-2.mp3
		02/26/2007-18:26:56	http://www.micasa.com.ec/avadell/ava-piso-2.zip
		02/27/2007-15:00:45	http://music2.hi5.com/0000/900/123/LETTLO900123-01.mp3
		02/27/2007-15:02:38	http://music2.hi5.com/0001/553/802/X8GS5T553802-01.mp3
		02/27/2007-15:04:02	http://music2.hi5.com/0001/183/858/P7NU6A183858-01.mp3
192.168.7.27	192.168.7.27	02/27/2007-08:31:40	http://sqm.msn.com/sqm/messenger/sqmserver.dll
		03/02/2007-11:39:57	http://sqm.msn.com/sqm/messenger/sqmserver.dll
192.168.7.28	192.168.7.28	02/27/2007-15:52:04	http://download.microsoft.com/download/D/4/6/D46381D9-6403-4821-B71C-B365D4511002/Install_Messenger.exe
192.168.7.29	192.168.7.29	02/27/2007-07:32:06	http://sqm.msn.com/sqm/messenger/sqmserver.dll
		02/28/2007-08:04:34	http://sqm.msn.com/sqm/messenger/sqmserver.dll

Figura 3.24 Detalle de las descargas realizadas por los hosts, con número de IP, fecha, hora de la descarga y sitio de acceso web.

3.2.3 Prevención de intrusos

Este reporte de prevención de intrusos muestra los hosts que han sido bloqueados por el sistema para prevenir posibles ataques.

En las gráficas tomadas desde el 22 de enero se puede observar el detalle de las direcciones IP de los host bloqueados por ClarkConnect por defecto con fecha, hora y tipo de evento (ver Figura 3.25).



Intrusion Prevention - Active Block List

ID	Blocked IP	Date	Time	Time Remaining
1991	200.110.238.14	03/07/07	16:50:22	23:51:50
1781	67.15.137.180	03/07/07	16:16:57	23:18:25
2003	58.17.4.33	03/07/07	15:04:24	22:05:52
2003	220.178.47.9	03/07/07	12:50:53	19:52:21
2003	125.76.238.162	03/07/07	11:58:15	18:59:43
2003	219.148.1.66	03/07/07	11:13:01	18:14:29
2003	218.106.91.25	03/07/07	11:05:37	18:07:05
2003	125.215.98.210	03/07/07	10:33:17	17:34:45
2003	220.189.196.140	03/07/07	10:20:36	17:22:04
1797	66.36.233.160	03/07/07	10:17:15	17:18:43
2003	220.178.32.78	03/07/07	07:22:59	14:24:27
1781	67.15.216.197	03/07/07	07:19:33	14:21:01
2003	61.136.186.46	03/07/07	07:10:27	14:11:55
2003	202.107.228.35	03/06/07	22:38:02	05:39:30
1794	201.238.209.203	03/06/07	18:18:24	01:19:52
1317	209.188.0.17	03/06/07	17:56:37	00:58:05
1781	67.15.10.56	03/06/07	17:55:25	00:56:53
1797	64.56.205.72	03/06/07	17:43:14	00:44:42
2003	218.75.24.230	03/06/07	17:01:25	00:02:53

Figura 3.25 Detalle de las direcciones IP de los host bloqueados con fecha, hora y tipo de evento.

Por último se ha hecho un mapeo del usuario 192.168.7.34 para analizar los sitios de navegación de cada uno y así tener una estadística más real del uso indebido del internet en horas de oficina.

Así, se pudo observar que el usuario navega en páginas de adultos, en páginas de ocio, páginas de música y videos, entre otras (Figura 3.26 -3.28), reiterando la medición hecha en forma general del uso del internet, lo que permite tener pruebas suficientes para poder establecer y aplicar las reglas de navegación dentro de la institución, reglas que deberán ser iguales para todos los usuarios sin excepción.

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILISEC
date/time gallys.nastydollars.com	816	11M	5.50%	1.43%	98.57%	00:25:41	2M
date/time www.sms-xvideos.com	3	11M	5.32%	0.00%	100.00%	00:31:53	2M
date/time www2.9000videos.com	3	7M	3.17%	0.00%	100.00%	00:08:47	527K
date/time www.archivodefamosas.com	1K	5M	2.47%	3.72%	96.28%	00:13:14	794K
date/time galleries9.exploitedteens.com	4	4M	1.75%	0.00%	100.00%	00:03:34	215K
date/time www.potras59.com.ar	332	3M	1.41%	1.31%	98.69%	00:10:22	623K
date/time www.assmasterpiecee.com	16	3M	1.39%	0.04%	99.96%	00:02:54	175K
date/time pics.mediaplazza.com	404	3M	1.29%	49.69%	50.31%	00:05:06	307K
date/time www.pimptrailers.com	4	3M	1.18%	0.00%	100.00%	00:02:04	125K
date/time latam.msn.com	111	3M	1.16%	0.18%	99.82%	00:05:43	343K
date/time www.lamermelculo.com	175	3M	1.14%	0.00%	100.00%	00:03:24	204K
date/time galleries2.exploitedteens.com	3	3M	1.08%	0.00%	100.00%	00:03:56	237K
date/time www.argenchicas.com.ar	394	2M	0.95%	2.03%	97.97%	00:04:52	293K
date/time pagead2.googlesyndication.com	385	2M	0.94%	0.05%	99.95%	00:08:46	527K
date/time www.descargadvds.com	166	2M	0.89%	1.39%	98.61%	00:11:25	685K
date/time thumbs.photo.net	256	2M	0.88%	2.57%	97.43%	00:05:31	331K
date/time media2.pajilleros.com	7	2M	0.87%	0.00%	100.00%	00:03:31	212K
date/time www.javiersalmones.com	134	2M	0.86%	5.80%	94.20%	00:11:05	666K
date/time www.famosas.biz	272	2M	0.86%	0.16%	99.84%	00:04:55	295K
date/time www.zumbaos.com	258	2M	0.85%	4.83%	95.17%	00:05:29	330K
date/time i.frazpc.pl	123	2M	0.82%	10.72%	89.28%	00:06:03	364K
date/time previews.peliculasxsms.com	381	2M	0.76%	0.87%	99.13%	00:05:14	314K
date/time www.ocioplayer.com	70	2M	0.76%	1.36%	98.64%	00:02:52	173K
date/time www.ocioplayer.com	70	2M	0.76%	1.36%	98.64%	00:02:52	173K
date/time www.pajilleros.com	220	2M	0.72%	1.37%	98.63%	00:08:11	491K
date/time www.150camaras.com	131	2M	0.68%	0.71%	99.29%	00:04:43	284K
date/time www.gabrielblanco.cc	316	2M	0.68%	1.47%	98.53%	00:05:40	341K
date/time www.virgenesardientes.com	170	2M	0.67%	0.93%	99.07%	00:03:29	209K
date/time graphics.adultfriendfinder.com	129	2M	0.65%	0.02%	99.98%	00:04:30	271K
date/time www.negrazas.es	2	2M	0.61%	0.00%	100.00%	00:22:42	2M
date/time images.pimproll.com	111	2M	0.61%	0.00%	100.00%	00:02:29	149K
date/time www.housewife1on1page.com	70	2M	0.58%	1.52%	98.48%	00:03:45	226K
date/time www.sexoporcam.com	297	2M	0.55%	2.77%	97.23%	00:03:31	212K
date/time www.promoxiona.com	9	2M	0.55%	0.00%	100.00%	00:04:22	262K
date/time www.cibernenas.com	156	2M	0.54%	2.23%	97.77%	00:02:21	142K
date/time www.mulhergostosa.net	124	2M	0.54%	0.10%	99.90%	00:10:27	627K
date/time crroco.hundiesgalleries.com	39	2M	0.52%	0.40%	99.60%	00:04:16	257K
date/time www.sitiosargentina.com.ar	99	991K	0.51%	0.54%	99.46%	00:01:59	119K
date/time vivamovil.ringtone-logo-game.com	18	977K	0.50%	0.00%	100.00%	00:03:09	190K
date/time www.megacorridas.com	140	948K	0.49%	1.59%	98.41%	00:02:51	171K
date/time www.peliculasxsms.com	107	941K	0.48%	0.00%	100.00%	00:06:22	383K
date/time famosas.quepasada.com	351	936K	0.48%	6.78%	93.22%	00:03:22	202K
date/time www.dealante.com	53	934K	0.48%	0.00%	100.00%	00:02:27	147K
date/time descargas3.tuvideogratis.com	24	929K	0.48%	3.85%	96.15%	00:01:56	116K
date/time www.amateurallurephotos.com	123	929K	0.48%	0.00%	100.00%	00:03:00	180K
date/time www.descuidosdefamosas.com	122	928K	0.47%	0.00%	100.00%	00:03:06	186K
date/time www.vipsex.org	142	923K	0.47%	0.00%	100.00%	00:03:45	226K
date/time www.lamusicahoy.com	7	923K	0.47%	0.00%	100.00%	00:01:31	91K
date/time www.top21.com.br	147	909K	0.47%	0.00%	100.00%	00:05:34	334K
date/time www.liandola.com	75	903K	0.46%	0.64%	99.36%	00:02:59	180K
date/time www.network54.com	41	891K	0.46%	0.15%	99.85%	00:04:30	270K
date/time www.fotosdefamosas.tk	135	887K	0.45%	1.62%	98.38%	00:03:21	201K

Figura 3.26 Detalle de los sitios que ha navegado el usuario 192.168.7.34 (Parte 1)

date/time www.zonacaliente.es	75	496K	0.25%	1.29%	98.71%	00:01:07	67K
date/time www.misnegritas.com	166	493K	0.25%	3.32%	96.68%	00:01:49	109K
date/time www.putaweb.net	57	489K	0.25%	0.00%	100.00%	00:01:17	77K
date/time banners.adultfriendfinder.com	67	483K	0.25%	0.00%	100.00%	00:01:51	112K
date/time www.9000videos.com	37	473K	0.24%	0.00%	100.00%	00:01:32	92K
date/time www.photo.net	32	471K	0.24%	0.52%	99.48%	00:00:48	48K
date/time www.sandrinha.com.br	17	470K	0.24%	0.05%	99.95%	00:00:53	53K
date/time www.papovirtual.com.br	72	470K	0.24%	0.00%	100.00%	00:01:37	97K
date/time www.iberporno.com	110	463K	0.24%	0.73%	99.27%	00:01:26	86K
date/time www.quenovias.com	114	455K	0.23%	0.10%	99.90%	00:01:34	94K
date/time www.5estrellax.com	31	450K	0.23%	0.89%	99.11%	00:01:01	62K
date/time topesexo.com	51	448K	0.23%	0.39%	99.61%	00:00:50	51K
date/time www.youtube.com	68	446K	0.23%	0.00%	100.00%	00:01:20	81K
date/time ads.adultfriendfinder.com	39	445K	0.23%	0.15%	99.85%	00:01:26	86K
date/time www.videochatxamateur.com	104	439K	0.22%	0.00%	100.00%	00:02:07	128K
date/time ktu.sv2.biz	102	437K	0.22%	0.00%	100.00%	00:01:27	88K
date/time www.geocities.com	77	436K	0.22%	0.35%	99.65%	00:01:48	109K
date/time dorado520.negrazas.es	79	435K	0.22%	1.94%	98.06%	00:01:49	109K
date/time www.bananacorp.cl	32	431K	0.22%	0.00%	100.00%	00:01:40	100K
date/time www2.blogger.com	143	428K	0.22%	1.35%	98.65%	00:02:46	167K
date/time www.peterpaulxxx.com	74	427K	0.22%	0.00%	100.00%	00:04:27	268K
date/time content3.babesmachine.com	24	423K	0.22%	0.00%	100.00%	00:01:16	77K
date/time www.quesalidas.com	2	44K	0.02%	0.00%	100.00%	00:00:12	12K
date/time ssl.google-analytics.com:443	2	44K	0.02%	0.00%	100.00%	00:00:04	5K
date/time www.ubbi.es	15	44K	0.02%	0.00%	100.00%	00:00:11	12K
date/time 67.18.226.50	10	44K	0.02%	0.00%	100.00%	00:00:06	6K
date/time 67.18.159.226	10	44K	0.02%	0.00%	100.00%	00:00:07	7K
date/time videodescargas.com	19	44K	0.02%	3.01%	96.99%	00:00:08	9K
date/time www.bicicletasguillermo.com	13	44K	0.02%	0.00%	100.00%	00:01:22	82K
date/time medias.sexywebcam.com	1	44K	0.02%	0.00%	100.00%	00:00:04	5K
date/time forums.neverside.com	3	44K	0.02%	0.00%	100.00%	00:00:07	8K
date/time www.amnistia.org.pe	1	43K	0.02%	0.00%	100.00%	00:00:04	5K
date/time www.sponsorpagos.com	9	43K	0.02%	0.00%	100.00%	00:00:08	9K
date/time www.descargarmessenger.com	25	43K	0.02%	7.74%	92.26%	00:00:15	16K
date/time spa.snap.com	8	43K	0.02%	2.00%	98.00%	00:00:09	9K
date/time v3.publipagos.com	3	42K	0.02%	0.00%	100.00%	00:00:13	14K
date/time www.putas.ca	2	42K	0.02%	0.00%	100.00%	00:00:06	7K
date/time img.blogalaxia.com	51	42K	0.02%	3.50%	96.50%	00:00:35	36K
date/time www.tuarroba.com	9	42K	0.02%	0.00%	100.00%	00:00:04	5K
date/time www.criticalgamers.com	1	41K	0.02%	0.00%	100.00%	00:00:07	7K
date/time sexofree.org	1	41K	0.02%	0.00%	100.00%	00:00:06	6K
date/time www.muyzorras.com	13	41K	0.02%	0.00%	100.00%	00:04:45	286K
date/time colasdefamosas.blogspot.com	1	41K	0.02%	0.00%	100.00%	00:00:03	4K
date/time clubedaputariabr.com	4	40K	0.02%	0.00%	100.00%	00:00:20	21K
date/time www3.cbox.ws	13	40K	0.02%	17.01%	82.99%	00:00:09	10K
date/time farm1.static.flickr.com	3	40K	0.02%	0.00%	100.00%	00:00:07	7K

Figura 3.27 Detalle de los sitios que ha navegado el usuario 192.168.7.34 (Parte 2)

date/time www.picapong.com	1	23K	0.01%	0.00%	100.00%	00:00:03	3K
date/time www.feedburner.com	5	23K	0.01%	0.00%	100.00%	00:00:06	7K
date/time www.labatidora.net	2	23K	0.01%	0.00%	100.00%	00:06:04	364K
date/time colegialas.jccafe.org	3	23K	0.01%	43.81%	56.19%	00:00:11	11K
date/time go.microsoft.com	32	23K	0.01%	0.00%	100.00%	00:00:19	20K
date/time www.maesen.com	15	23K	0.01%	7.72%	92.28%	00:00:05	5K
date/time www.farolatino.com	15	23K	0.01%	0.00%	100.00%	00:00:08	8K
date/time m1.2mdn.net	3	23K	0.01%	0.00%	100.00%	00:00:02	2K
date/time jsp.systemdoctor.com	3	23K	0.01%	0.00%	100.00%	00:00:06	6K
date/time www.google.es	2	23K	0.01%	0.00%	100.00%	00:02:02	122K
date/time www.hispamp3.com	1	23K	0.01%	0.00%	100.00%	00:00:02	3K
date/time www.tramps.com.ar	1	23K	0.01%	0.00%	100.00%	00:00:05	5K
date/time depilflash.tv	6	22K	0.01%	0.00%	100.00%	00:00:06	6K
date/time www.galeriaz.com	5	22K	0.01%	0.00%	100.00%	00:02:53	174K
date/time www.voyeura9euros.com	9	22K	0.01%	0.00%	100.00%	00:00:06	6K
date/time www.canalstar-live.net	2	22K	0.01%	1.00%	99.00%	00:00:02	2K
date/time img142.imagevenue.com	3	22K	0.01%	0.00%	100.00%	00:00:04	5K
date/time www.femjoy.com	1	22K	0.01%	0.00%	100.00%	00:00:02	2K
date/time images.google.es	8	22K	0.01%	0.00%	100.00%	00:00:04	5K
date/time banners.chicashumedas.com	2	22K	0.01%	0.00%	100.00%	00:00:05	6K
date/time zoo-a.parkingspa.com	1	22K	0.01%	0.00%	100.00%	00:00:05	6K
date/time imgs.codigobarras.net	9	22K	0.01%	0.00%	100.00%	00:00:06	7K
date/time www.da.ru	12	22K	0.01%	5.12%	94.88%	00:00:09	9K
date/time www.caserashot.com.ar	2	21K	0.01%	0.00%	100.00%	00:00:19	20K
date/time i.1100i.com	5	21K	0.01%	0.00%	100.00%	00:00:07	8K
date/time www.latinacamnetwork.com	1	21K	0.01%	0.00%	100.00%	00:00:07	8K
date/time img248.imageshack.us	2	21K	0.01%	1.08%	98.92%	00:00:04	4K
date/time www.requested-url.com	4	20K	0.01%	0.00%	100.00%	00:00:04	5K
date/time www.ademails.com	22	13K	0.01%	0.00%	100.00%	00:00:26	27K
date/time img40.imagevenue.com	2	13K	0.01%	0.00%	100.00%	00:00:02	2K
date/time www.lalupa.com	1	13K	0.01%	0.00%	100.00%	00:00:03	3K
date/time www.obanner.net	4	13K	0.01%	0.00%	100.00%	00:00:05	6K
date/time content.directanetworks.com	2	13K	0.01%	0.00%	100.00%	00:00:01	2K
date/time livesexbar.com	4	13K	0.01%	0.00%	100.00%	00:00:04	5K
date/time traces.estadisticasgratis.com	8	13K	0.01%	0.00%	100.00%	00:00:07	8K
date/time media2.carpediem.fr	2	13K	0.01%	0.00%	100.00%	00:00:03	3K
date/time secure-uk.imrworldwide.com	19	13K	0.01%	2.20%	97.80%	00:00:12	12K
date/time www.pillados.com	1	13K	0.01%	0.00%	100.00%	00:00:01	2K
date/time www.indiwiz.com	4	13K	0.01%	1.75%	98.25%	00:00:04	4K
date/time www.peru21.com	1	13K	0.01%	0.00%	100.00%	00:00:02	3K
date/time personal.auna.com	1	13K	0.01%	0.00%	100.00%	00:00:02	3K
date/time cloud.blogalaxia.com	2	12K	0.01%	0.00%	100.00%	00:00:02	2K
date/time img384.imageshack.us	1	12K	0.01%	0.00%	100.00%	00:00:03	4K
date/time www.rapid-pass.net	7	12K	0.01%	0.00%	100.00%	00:00:10	10K
date/time www.clinicamental.com	5	12K	0.01%	0.00%	100.00%	00:00:06	6K
date/time banners.strip-player.com	1	12K	0.01%	0.00%	100.00%	00:00:01	2K
date/time img253.imageshack.us	1	12K	0.01%	0.00%	100.00%	00:00:02	3K
date/time ads.us.e-planning.net	14	12K	0.01%	0.00%	100.00%	00:00:06	7K
date/time geo.yahoo.com	27	12K	0.01%	0.00%	100.00%	00:00:20	20K
date/time www.alrincon.com	1	12K	0.01%	0.00%	100.00%	00:00:02	2K
date/time img187.imageshack.us	1	12K	0.01%	0.00%	100.00%	00:00:02	2K
date/time static.technorati.com	10	12K	0.01%	0.00%	100.00%	00:00:06	7K
date/time www.comm.blogger.com.br	1	12K	0.01%	0.00%	100.00%	00:00:02	2K
date/time 3.adbrite.com	8	12K	0.01%	0.00%	100.00%	00:00:03	4K
date/time skins.neverside.com	5	12K	0.01%	0.00%	100.00%	00:00:03	3K
date/time www.servicont.com	29	12K	0.01%	1.85%	98.15%	00:00:28	28K
date/time img149.imagevenue.com	1	3K	0.00%	0.00%	100.00%	00:00:00	880
date/time sjl-static15.sjl.youtube.com	1	3K	0.00%	0.00%	100.00%	00:00:01	1K
date/time img.shinobi.jp	13	3K	0.00%	0.00%	100.00%	00:00:09	9K
date/time www.blogarama.com	6	3K	0.00%	0.00%	100.00%	00:00:03	3K
date/time www.blogs.com.br	1	3K	0.00%	0.00%	100.00%	00:00:01	2K
date/time img135.imagevenue.com	1	3K	0.00%	0.00%	100.00%	00:00:00	815
date/time t0.extreme-dm.com	18	3K	0.00%	0.00%	100.00%	00:00:08	9K
date/time c18.statcounter.com	5	3K	0.00%	0.00%	100.00%	00:00:02	2K
date/time www.tbhostedgalleries.com	8	3K	0.00%	0.00%	100.00%	00:00:04	5K
date/time media.eresmas.com	3	3K	0.00%	14.04%	85.96%	00:00:00	735

Figura 3.28 Detalle de los sitios que ha navegado el usuario 192.168.7.34 (Parte 3)

CAPÍTULO IV

4 REINGENIERÍA DE LA RED

Después de conocer los requerimientos se empieza la reingeniería de la red de la DIRECCIÓN NACIONAL DE MIGRACIÓN.

Primero se realizará el levantamiento del diagrama de la red, con el fin de tener un punto de inicio de la reingeniería. Para saber qué es lo que posee cada parte y poder entender sus necesidades se tiene que dividir la red en física y en lógica.

En lo que a la parte física se refiere, el proceso de reingeniería se enfocará a un análisis de los puntos remotos, y en base a este estudio se emitirán conclusiones y recomendaciones acerca de la situación actual de la red WAN.

Lógicamente se analizará la configuración de conexiones, esquematización de los existentes servidores, que permita evaluar la operatividad y eficiencia de la configuración actual.

4.1 LEVANTAMIENTO DEL DIAGRAMA DE LA RED WAN DE LA DIRECCIÓN NACIONAL DE MIGRACIÓN

La red Wan de Policia de Migración es una red IP MPLS cuyo proveedor es CNT, los routers son Cisco 1841 con encryptacion MD5 en la TX y RX de información.

En el diagrama se muestran los puntos remotos en los que se dará internet, el resto de puntos están tomados como fase 2 para el próximo año, ya que los enlaces de datos son de capacidades medianas a bajas (ver. Figura 4.1).

El ancho de banda en cada punto remoto del diagrama es de 1024/1024kbps, el cual esta dentro del rango adecuado para multiplexar el canal y dar Internet dedicado.

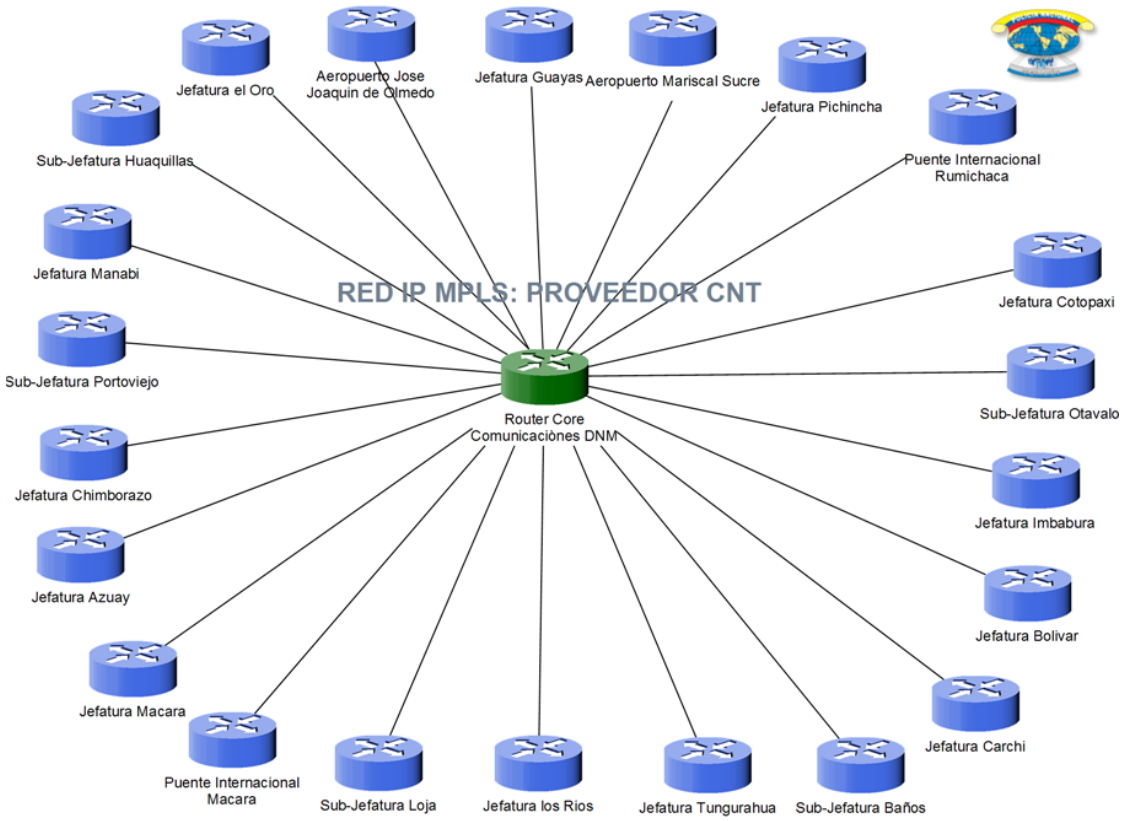


Figura 4.1 Diagrama red Wan DIRECCIÓN NACIONAL DE MIGRACIÓN

4.2 REINGENIERÍA LÓGICA DE LA RED

4.2.1 Diagrama de conexiones

Este diagrama define la forma de conexion en la cual se garantiza la integridad de la información que pasa a travez de la red de datos, además de mostrar el peligro a que está expuesta por las conexiones aisladas a internet.

4.2.1.1 Procesos de conexión actual intranet e internet

La protección de datos que la CNT le da a la Policia Nacional son altas ya que cumplen con estándares de seguridad bastante importantes, sin embargo esta protección, no sirve de nada, ya que al momento existen conexiones a internet aisladas en diferentes puntos a nivel nacional, con lo cual toda la red de la Policia de Migracion se encuentra en peligro (ver Figura 4.2).

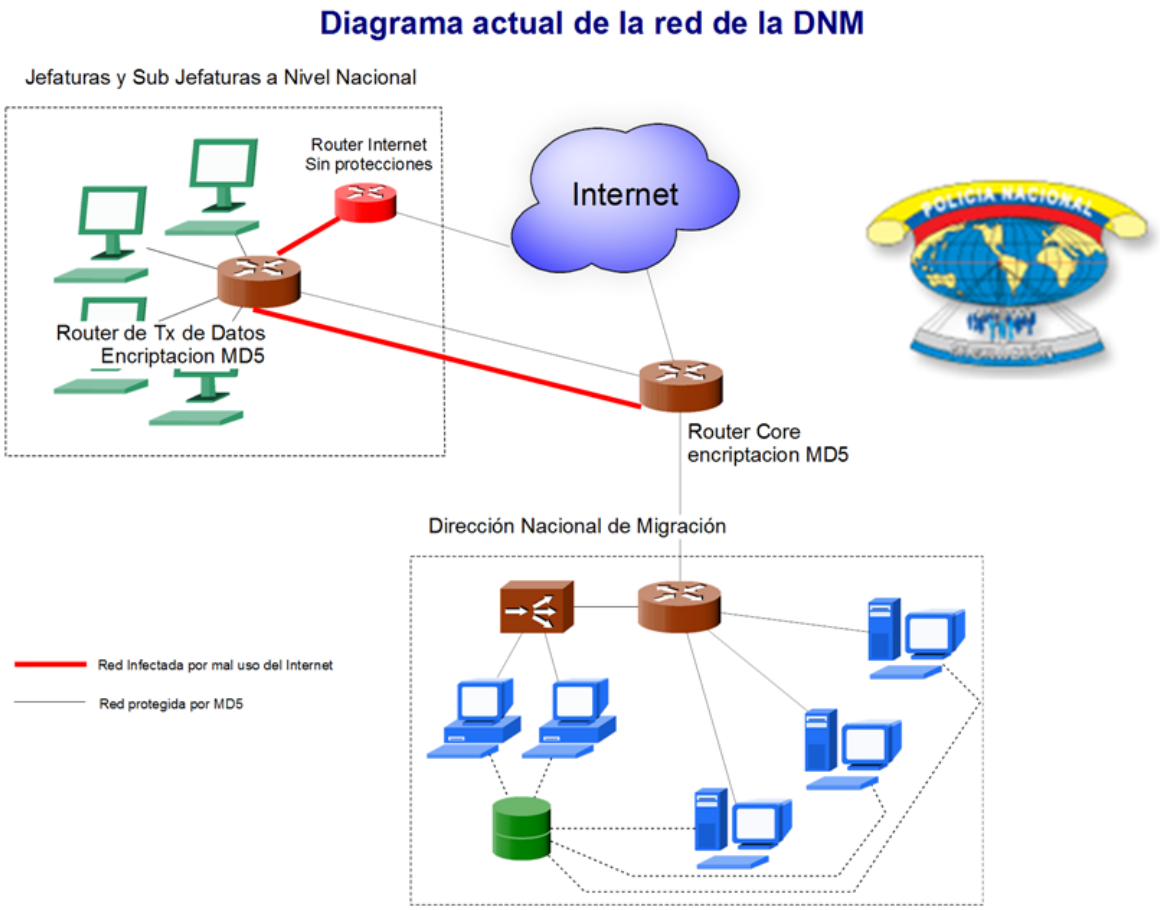


Figura 4.2 Diagrama actual de conexión Intranet e Internet

4.2.1.2 Procesos de conexión intranet e internet propuestos

Ademas de la protección de datos que le brinda el proveedor actual a la DIRECCIÓN NACIONAL DE MIGRACIÓN, se entregará la protección de acceso al internet. La propuesta es centralizar en la Direccion Nacional de Migracion ubicada en Quito, la totalidad de la capacidad del internet y configurar un servidor que de protección global del uso del Internet a la institución. Con esto se garantizará la integridad global de la información sin poner en riesgo la bases de datos de alta seguridad (ver Figura 4.3).

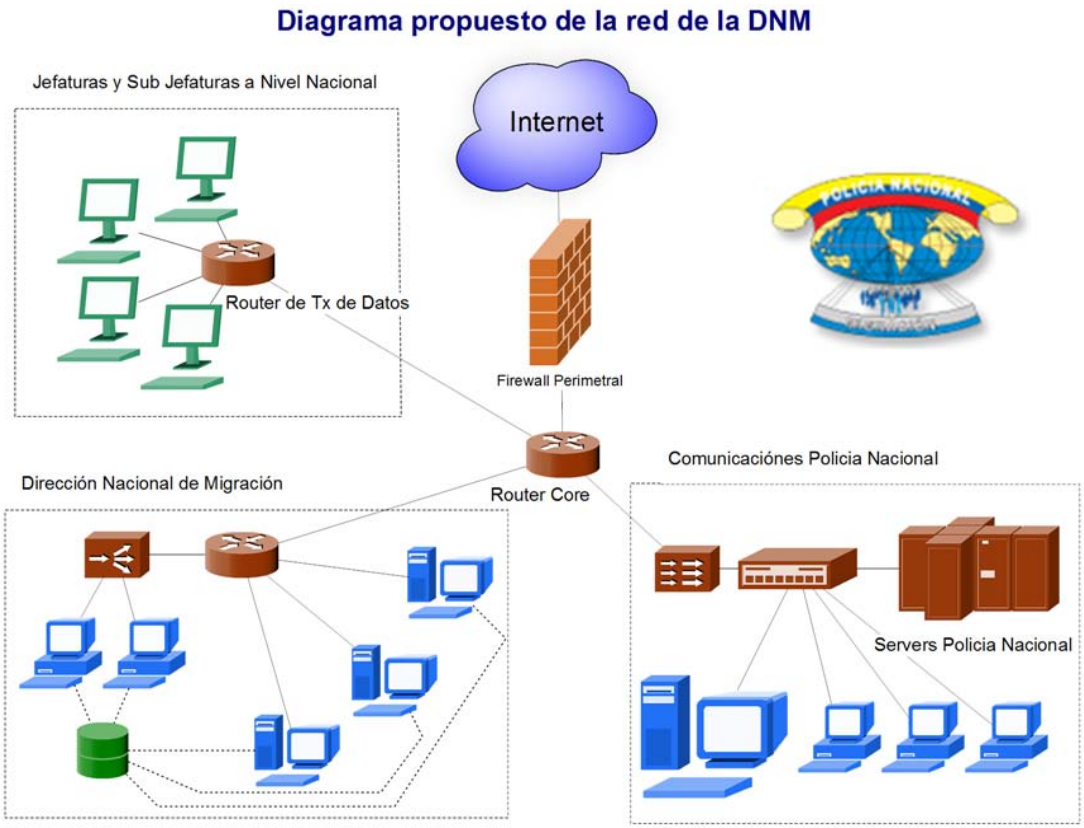


Figura 4.3 Diagrama propuesto de conexión intranet e internet

4.2.2 Diagrama de esquematización de los servidores

Este diagrama permite definir la estructura fundamental de los servidores.

4.2.2.1 Diagrama de ubicación de servidores

Los servidores se ubicarán estratégicamente, los más críticos estarán resguardados en el centro de comunicaciones de la Policia Nacional, y los sub siguientes se ubicarán en la Dirección Nacional de Migracion (ver Figura 4.4).

Todos los servidores están bajo S.O. Linux y ninguno tiene salida directa al internet, por lo que no hace falta hacer recomendaciones de seguridad extras al esquema lógico de los servidores con que se cuenta actualmente.

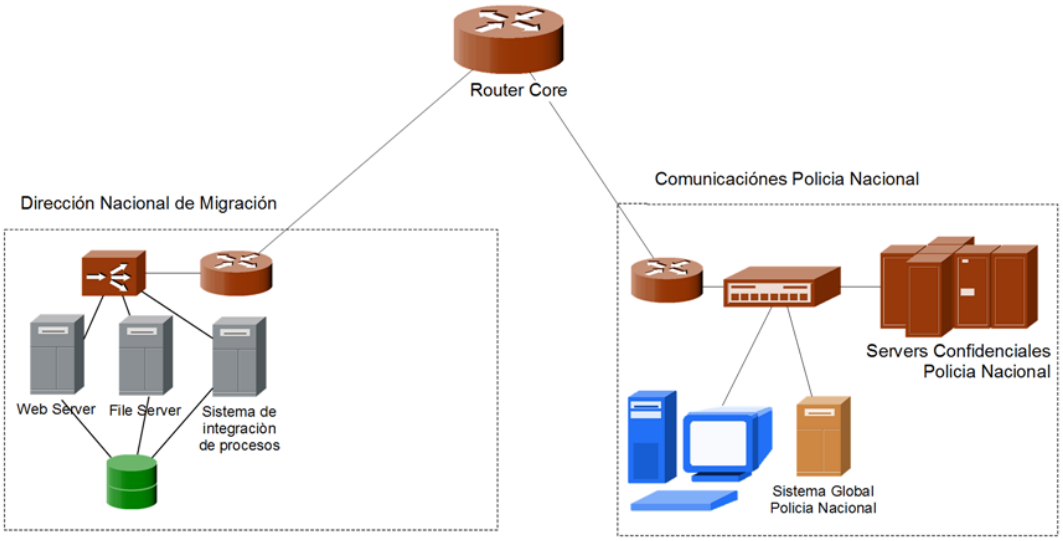


Figura 4.4 Diagrama de ubicación de servidores

CAPÍTULO V

5 IMPLEMENTACIÓN

Con los resultados de las fases anteriores se considerarán aspectos como el fundamento para la utilización del internet en la institución, los cuales estarán acordes a las necesidades del proyecto. Se configurará el servidor con las soluciones de: Proxy, Filtro de Contenidos, Firewall, Detección de Intrusos IDS, Prevención de Intrusos IPS, Controlador de Ancho de Banda y Anti Spam, Se hará pruebas con cada servicio configurado lo que garantizará el correcto funcionamiento del proyecto.

5.1 IMPLEMENTACION DE LA SOLUCIÓN PROXY

Se configurará este servicio por WEB para acceder al servidor de la siguiente manera: https://192.168.7.24. Lo que no haya como configurar en modo gráfico se hará a través del fichero de configuración de SQUID que se halla en /etc/squid/squid.conf y será editado con “nano” para realizar los cambios adecuados y conseguir que cumpla su tarea con toda la seguridad para el sistema.

Este fichero de configuración consta de una multitud de parámetros configurables que ajustan el servidor a las necesidades del proyecto. Se modificarán todos aquellos aspectos que sean indispensables para un óptimo funcionamiento.

5.1.1 Configuración de puerto para Squid

Por defecto, SQUID utilizará el puerto 3128, aunque puede configurarse para que use cualquier otro, incluso varios puertos simultáneamente. En la DIRECCIÓN NACIONAL DE MIGRACIÓN hay algunos programas utilizados por

los usuarios de alto nivel que traen de modo predefinido el puerto 8080 para utilizarse al configurar el servidor Proxy. Para optimizar aquello y ahorrar el tener que dar explicaciones innecesarias al usuario, se especificará que Squid escuche también peticiones en ese puerto. Por lo que la definición de http_port quedará así:

```
# Default: http_port 3128
http_port 3128
http_port 8080
```

Para incrementar la seguridad, se vinculará el servicio a una IP a la que sólo se pueda acceder desde la red autorizada. Considerando que el servidor utilizado posee una IP 192.168.7.24 en eth1, se hará lo siguiente:

```
# Default: http_port 3128
http_port 192.168.7.24:3128
http_port 192.168.7.24:8080
```

5.1.2 Configuración del tamaño del cache

En esta instrucción se fijará el espacio en disco que se usará para almacenar las páginas visitadas.

Por defecto SQUID usará 100 Mb, como límite para el tamaño del caché, pero en este caso se lo fijará en 1000 Mb o 1Gb, para lo que deberá fijarse la entrada correspondiente de la siguiente forma:

```
cache_dir ufs /usr/local/squid/cache 1000 16 256
```

En la línea anterior se selecciona el directorio de caché (/usr/local/squid/cache), indicando el tamaño máximo para éste (1000), la cantidad de subdirectorios de primer nivel que puede contener (16, el valor por defecto) y, el número de subdirectorios de segundo nivel (256, también por defecto) que puede almacenar.

En Modo Gráfico se entra a la configuración poniendo en el navegador https://192.168.7.24; en el menú software se escoge la opción Web Proxy (ver Figura 5.1) y luego se irá a la primera opción de la configuración, para fijar el valor del tamaño de cache (ver Figura 5.2):

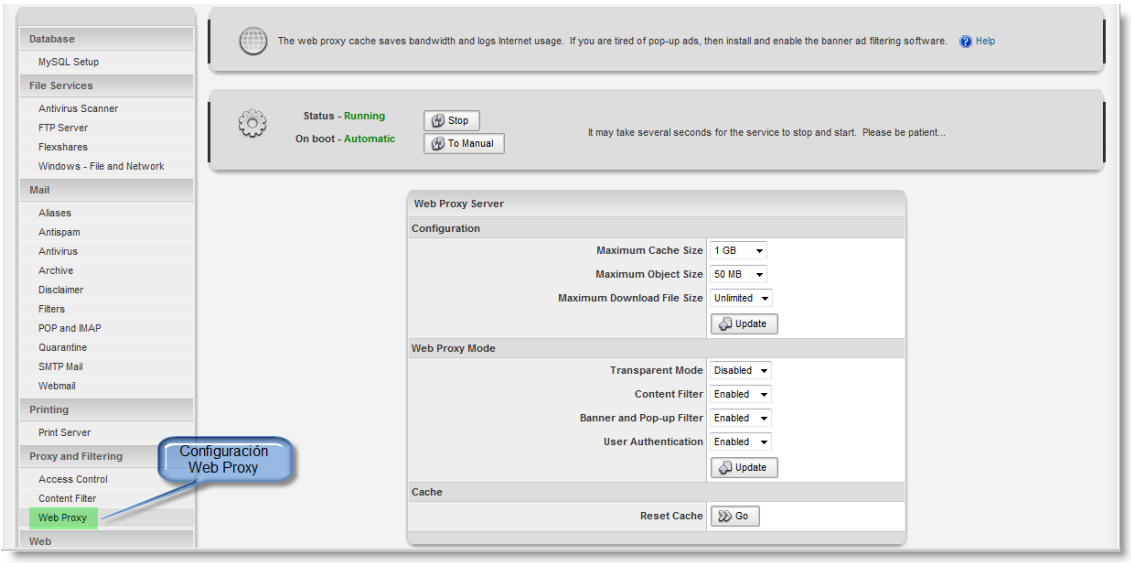


Figura 5.1 Entrada de configuración de Web Proxy

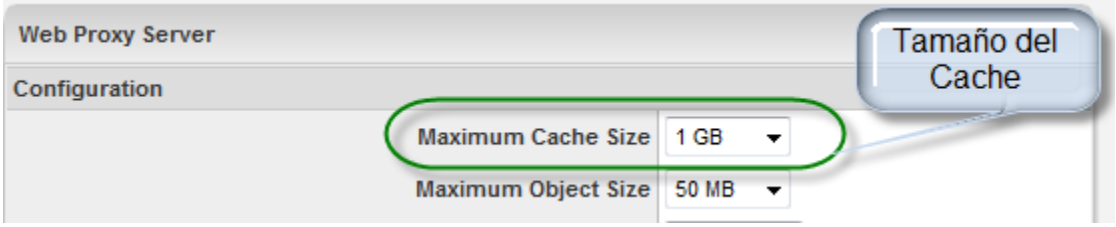


Figura 5.2 Configuración del tamaño del cache

5.1.3 Configuración de controles de acceso

Una de las características más importantes del servidor Proxy es la posibilidad de establecer reglas de control de acceso ACL´s que pueden complementar perfectamente el objetivo de filtrado de paquetes.

Se crearán listas de control de acceso para designar las redes que tienen permiso de navegar o no, el control individual no se hará por IP sino por autentificación de usuario con contraseña, ya que la red es demasiado extensa. Cada una de las ACL´s tendrá asociadas Reglas de Control que regularán esta actividad. Es decir, se definirán unas listas, por una parte estableciendo reglas específicas para cada una de ellas, se creará la ACL que dirá cuando es necesario usar password para poder navegar.

acl password proxy_auth REQUIRED

Es necesario establecer listas de control de acceso que definan una red. A cada lista se le asignará una Regla de Control de Acceso que permitirá o denegará el acceso a Squid. Se procederá a definir unas y otras.

5.1.4 Configuración de listas de controles de acceso

Regularmente una lista de control de acceso se establece con la siguiente sintaxis:

acl [nombre de la lista] src [lo que compone a la lista]

Si se desea establecer una lista de control de acceso que abarque a toda la red local, basta definir la IP correspondiente a la red y la máscara de la sub-red. Por ejemplo, si se define la red de la DIRECCIÓN NACIONAL DE MIGRACIÓN en Quito, donde las máquinas tienen direcciones IP 192.168.7.n con máscara de sub-red 255.255.255.0, se puede utilizar lo siguiente:

acl redlocal src 192.168.7.0/255.255.255.0

Sin embargo como lo que se busca es que naveguen a nivel nacional, las redes tienen el siguiente orden:

JEFATURA DE GUAYAS: 192.168.97.0

PUYO: 192.168.73.0

PUERTO BAQUERIZO MORENO GALAPAGOS: 192.168.229.0

ESMERALDAS: 192.168.42.0

OTAVALO: 192.168.241.0

SANTA CRUZ GALAPAGOS: 192.168.228.0

MANTA: 192.168.242.0

RIOBAMBA: 192.168.240.0

AEROPUERTO UIO: 192.168.16.260

JEFATURA DE PICHINCHA: 192.168.15.0

SANTO DOMINGO: 192.168.23.0

MIGRACION CUENCA: 192.168.243.0

MACHALA: 192.168.123.0

AMBATO: 192.168.67.0

BAÑOS: 192.168.70.0

HUAQUILLAS: 192.168.126.0

MACARA: 192.168.87.0

RUMICHACA: 192.168.36.0

LAGO AGRIO: 192.168.50.0

PUERTO GYE: 192.168.100.0

QUITO SUR: 192.168.203.0

BOYACA: 192.168.204.0

AEROPUERTO GYE: 192.168.99.0

IBARRA: 192.168.225.0

LOJA: 192.168.230.0

LATACUNGA: 192.168.232.0

COCA: 192.168.233.0

TENA: 192.168.234.0

QUEVEDO: 192.168.235.0

Se usará el siguiente ACL, que servirá para todas las redes, se usa la denominación /16 que es 16bits o lo que da lo mismo máscara de 255.255.0.0:

acl permitidos src 192.168.0.0/16

También puede definirse una lista de control de acceso especificando un archivo localizado, que para este caso es en /squid, la cual contiene la red IP que servirá para todas las localidades a nivel nacional:

acl permitidos src "/etc/squid/permitidos"

El archivo /etc/squid/permitido contiene lo siguiente:

192.168.0.0/16

Lo anterior estaría definiendo que la lista de control de acceso denominada permitidos, estaría compuesta por la o las redes IP incluidas en el fichero /etc/squid/permitidos.

Se creará el ACL para el control de navegación por horarios, esto se hará por configuración web, lo que permitirá entrar por medio del navegador web poniendo https://192.168.7.24. Luego en el menú software se irá a control de acceso, creando los periodos de tiempo respectivos (ver Figura 5.3). Se creará el periodo de tiempo denominado Horario-normal, que pertenece al horario de lunes a viernes de 08:00am a 18:00pm, y el otro periodo, que pertenece al horario del fin de semana, que se denominará Horario-fin-de-semana.

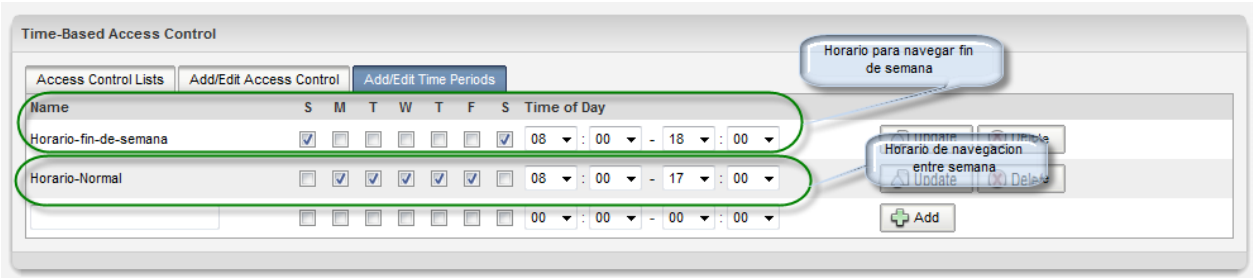


Figura 5.3 Creación de los periodos de tiempo

Una vez creados los periodos de tiempo se crearán las listas de control de acceso correspondientes a cada periodo.

Para el periodo Horario-normal se creará el ACL con las siguientes características (ver Figura 5.4):

Nombre del ACL: Nav-horario-normal.

Tipo de ACL: Permitido (Se pondrán las reglas que se definirán para el efecto).

Periodo de tiempo: Horario-normal (Periodo creado en el paso anterior).

Restricciones: se dejará vacio, porque se necesita que se cumpla el horario y nada más.

Método de Identificación: Nombre de usuario (permite controlar la navegación en la DIRECCIÓN NACIONAL DE MIGRACIÓN).

Aplicar ACL a los usuarios: se elije a los usuarios que deberán cumplir este ACL. En este caso son sólo 2 que pertenecen a los de frontera sur y norte. Esta política de horarios de trabajo, definida por la DIRECCIÓN NACIONAL DE MIGRACIÓN para la frontera, se debe cumplir de manera rigurosa.

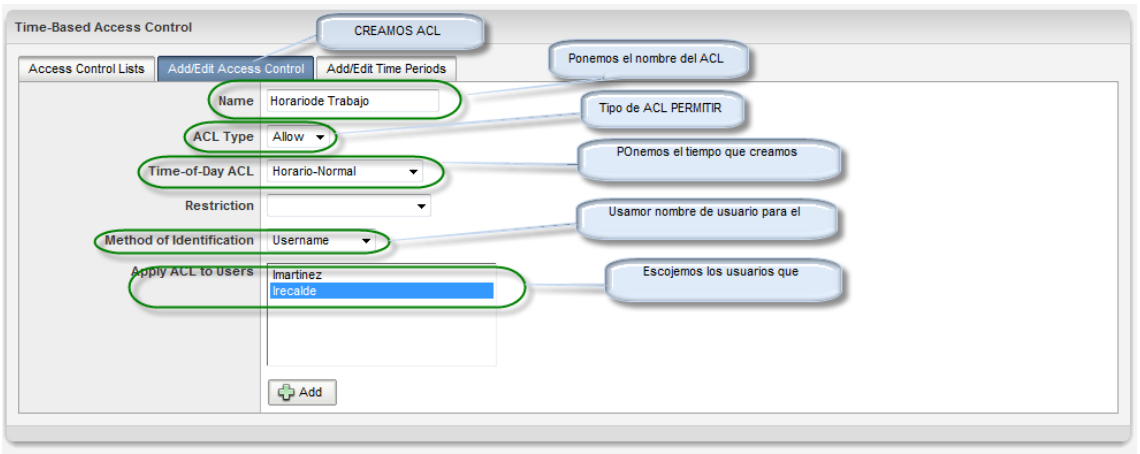


Figura 5.4 Configuración ACL para Horario-normal

Para el periodo Horario-fin-de-semana el ACL se creará con las siguientes características (ver Figura 5.5):

Nombre del ACL: Fin_de_semana.

Tipo de ACL: Permitido (Se pondrán las reglas que se definirán para el efecto).

Periodo de tiempo: Horario-fin-de-semana (Periodo creado en el paso anterior).

Restricciones: Outside time restriction (Restricción si se pasan de tiempo).

Método de Identificación: Nombre de usuario (Esto permite el control de navegación en la DIRECCIÓN NACIONAL DE MIGRACIÓN).

Aplicar ACL a los usuarios: se elije a los usuarios que deberán cumplar este ACL; la DIRECCIÓN NACIONAL DE MIGRACIÓN trabaja de forma normal los fines de semana en los aeropuertos y fronteras del país, por lo que el departamento de sistemas deberá cambiar estos ACL según los turnos de todos los fines de semana.

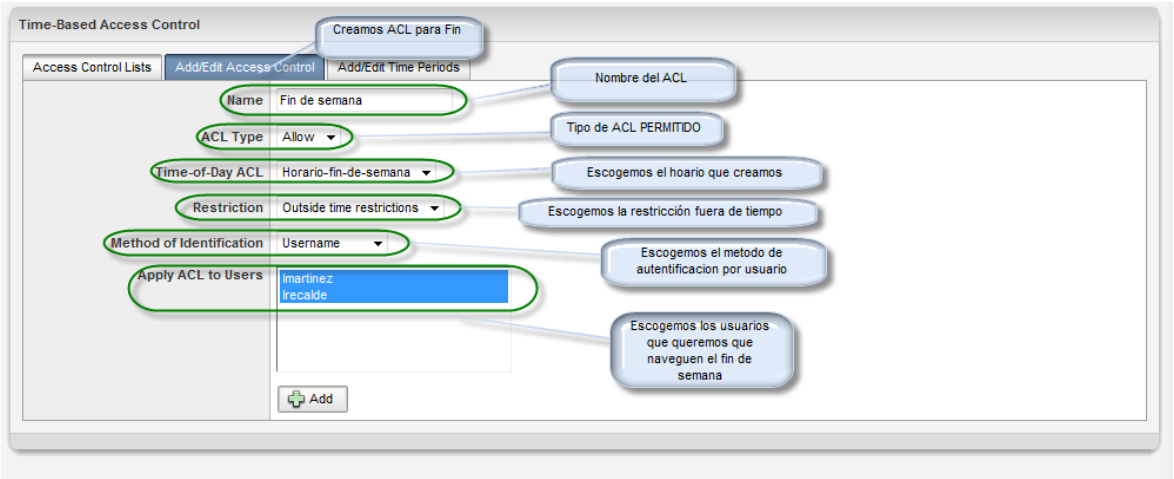


Figura 5.5 Configuración ACL para Horario-fin-de-semana

5.1.5 Configuración de reglas de control de acceso

Estas definen si se permite o no el acceso hacia Squid a través de políticas. Se aplican a las Listas de Control de Acceso creadas.

La sintaxis básica es la siguiente:

http_access [deny o allow] [lista de control de acceso]

A continuación se dará acceso con estado permitido a Squid a la Lista de Control de Acceso denominada “permitidos**”** la cual contiene la Red que permita

navegar a todos los usuarios a nivel nacional, seguida del ACL clave, la cual se creará para autentificar con password a cada usuario:
http_access allow permitidos clave

5.1.6 Configuración del parámetro cache_mgr

De modo predefinido, si algo ocurre con el caché, como por ejemplo que muera el proceso, se enviará un mensaje de aviso a la cuenta webmaster del servidor. En este caso se pondrá el mail del Director del Departamento de Sistemas Ing. Luis F. Martínez Martínez.

cache_mgr luis.martinez@migracion.gov.ec

5.1.7 Cambio de los mensajes mostrados por Squid

Squid incluye traducción a varios idiomas de las distintas páginas de error e informativas que son desplegadas en un momento dado durante su operación. Dichas traducciones se pueden encontrar en /usr/share/squid/errors/. Para poder hacer uso de las páginas de error, traducidas al español, es necesario cambiar un enlace simbólico localizado en /etc/squid/errors para que apunte hacia /usr/share/squid/errors/Spanish, en lugar de hacerlo hacia /usr/share/squid/errors/English.

Se elimina primero el enlace simbólico actual:
rm -f /etc/squid/errors

Se coloca un nuevo enlace simbólico apuntando hacia el directorio con los ficheros correspondientes a los errores traducidos al español.
ln -s /usr/share/squid/errors/Spanish /etc/squid/errors

Por último se modifica los errores para personalizarlos como DIRECCIÓN NACIONAL DE MIGRACIÓN (ver Figura 5.6 – 5.7):
nano /etc/squid/errors/ERR_ACCESS_DENIED

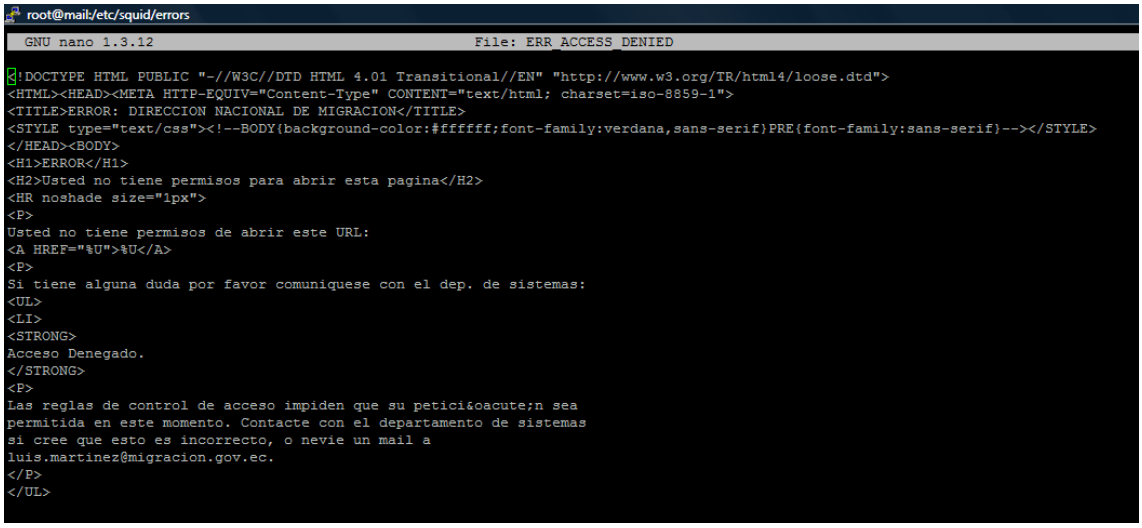


Figura 5.6 Modificación de pantalla de error

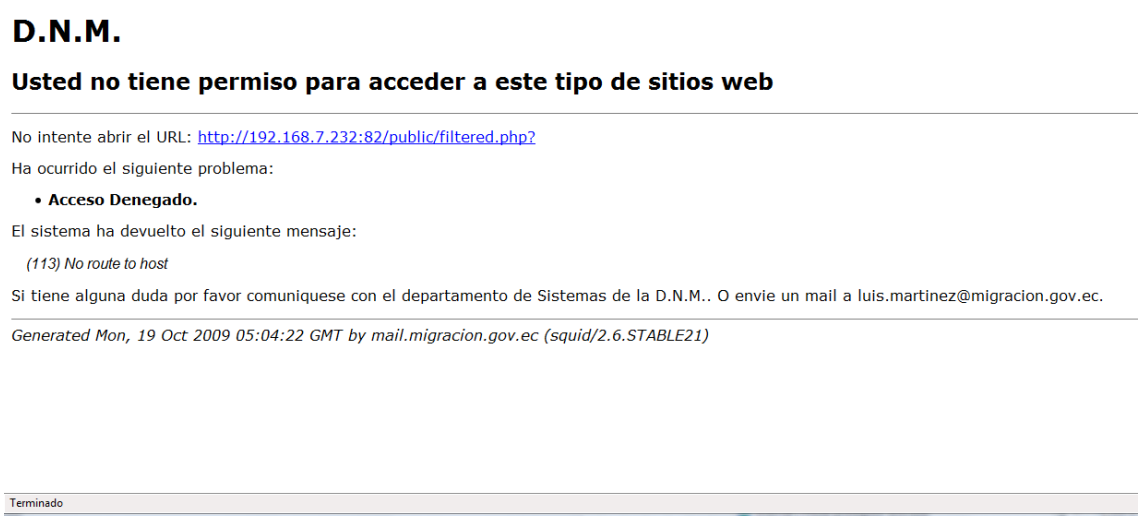


Figura 5.7 Mensaje personalizado en español

5.1.8 Iniciando, reiniciando y añadir el servicio al arranque del sistema

Una vez terminada la configuración, para ejecutar el siguiente mandato para iniciar por primera vez Squid, se deberá:

service squid start

O se podrá hacer en modo grafico entrando desde el navegador https://192.168.7.24, en el menú Software eligiendo la opción Web Proxy (ver Figura 5.8)

Para reiniciar, después de algún cambio hecho en la configuración, se utilizará lo siguiente:
service squid restart

Para que Squid comience de manera automática la próxima vez que inicie el sistema, se realiza de modo gráfico entrando desde el navegador https://192.168.7.24, en el menú Software eligiendo la opción Web Proxy (ver Figura 5.8):

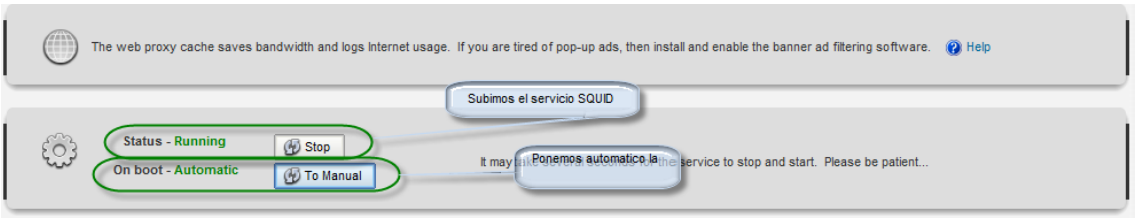


Figura 5.8 Subimos el servicio Squid, y lo dejamos en forma automática

Lo anterior habilitará a Squid en todos los niveles de corrida.

5.1.9 Depuración de errores

Cualquier error al inicio de Squid solo significa que hubo errores de sintaxis, errores de manipulación, o bien se están citando incorrectamente las rutas hacia los ficheros de las Listas de Control de Acceso.

Puede realizarse el diagnóstico de problemas indicándole a Squid que vuelva a leer la configuración, lo que devolverá los errores que existan en el fichero /etc/squid/squid.conf.
service squid reload

Cuando se trata de errores graves que no permiten iniciar el servicio, puede examinarse el contenido del fichero /var/log/squid/squid.out con el mandato **“**nano**”** o cualquier otro visor de texto:
nano /var/log/squid/squid.out

Para finalizar se comprobará que toda la configuración este de acuerdo a las necesidades (ver Figura 5.9)

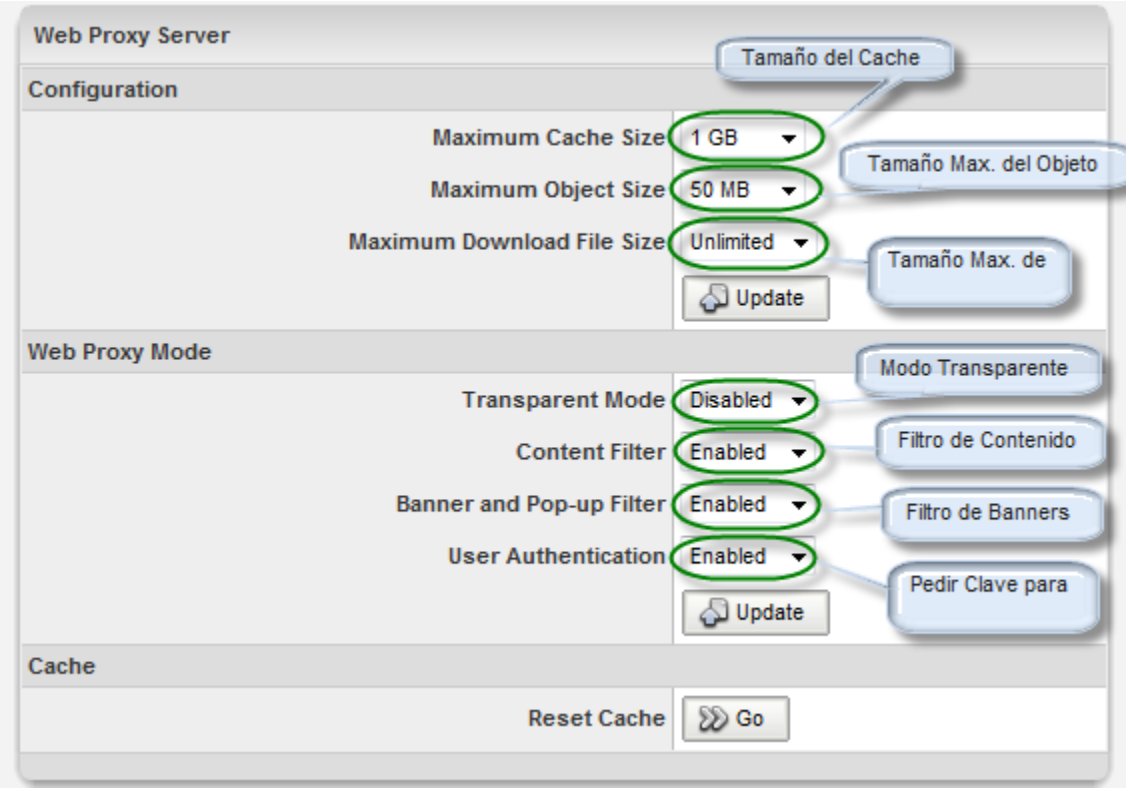


Figura 5.9 Comprobación de todos los parámetros

5.2 IMPLEMENTACIÓN DE LA SOLUCIÓN FILTRO DE CONTENIDO

Se configurará este servicio por web accediendo al servidor de la siguiente manera: https://192.168.7.24, y lo que no haya como configurar en modo gráfico se hará a través desde el fichero de configuración de DANSGUARDIAN que se halla en /etc/dansguardian-av/dansguardian.conf procediéndose a lo editar con la herramienta “nano” para realizar los cambios adecuados y conseguir que cumpla su tarea con toda la seguridad para el sistema.

DansGuardian tiene la particularidad de trabajar conjuntamente con el servidor Proxy SQUID. DansGuardian se encuentra en el intermedio de comunicación entre el navegador web del cliente y el servidor Proxy, de esta manera intercepta y modifica toda petición que se realiza y que el servidor deba atender.

5.2.1 Configuración de la lista exceptioniplist

Este archivo contiene una lista de direcciones IP de clientes que no usarán el filtro, por ejemplo, la dirección IP del director de sistemas. En este caso se usará sólo para el Director de Sistemas, ya que por reglas y normas de la institución todo el personal, sea cual sea el rango, deberá tener las mismas restricciones de internet.

La dirección IP del director es la 192.168.7.2 por lo que se instalará dentro de la lista, esto se realizará en modo grafico, ingresando al servidor por el navegador web, digitando en la url: https://192.168.7.24, luego en la solapa de software se elije la opción que dice **"**content Filter**"** y luego se pulsa en el botón que dice editar Banned User / Exempt IP List (Ver Figura 5.10)

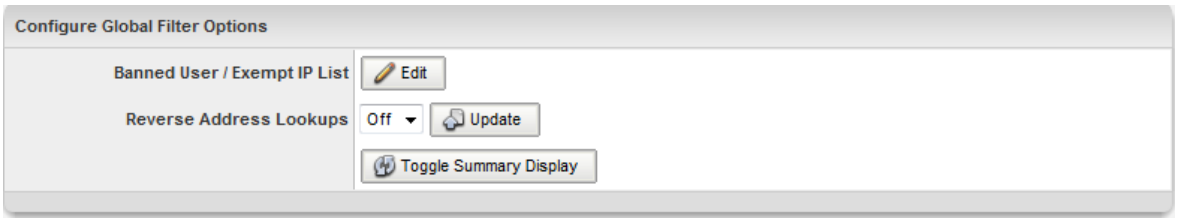


Figura 5.10 Opciones de configuración global

Luego en el área de la lista de excepción IP se pone la ip del director de sistemas de la DIRECCIÓN NACIONAL DE MIGRACIÓN, la cual es 192.168.7.2 (ver Figura 5.11).

Figura 5.11 Lista de excepción de usuario

5.2.2 Configuración de la lista bannedphraselist

Contiene la lista de frases prohibidas. Hay que evitar usar palabras genéricas como <sex> ya que de esta manera bloqueará páginas que contengan por

ejemplo "Departamento de Sexología". Las frases pueden contener espacios. Se usarán los espacios para obtener mayor beneficio del filtrado. Esta es la parte más útil de DansGuardian y filtrará más páginas que combinando los filtros de imagen y URL juntos.

También puede usarse combinaciones de frases, que de ser encontradas en una página, serán bloqueadas. En este caso se usarán servidores de blacklist existentes y que continuamente se están actualizando.

En presente caso se usarán servidores que enlistan y clasifican listas negras a nivel mundial. Para que sea más efectivo el control es mejor buscar una base de datos donde estén las paginas peligrosas por categorías, se bajará una lista de paginas prohibidas de la pagina http://urlblacklist.com, la que se descomprimirá en /etc/dansguardian-av/blacklist/, para permitir tener de forma automática la actualización de las paginas. Esto se logrará por consola de la siguiente manera:

Se coloca en la carpeta principal de dansguardia-av:
[root@secure ~]#cd /etc/dansguardian-av

El listado de la página mencionada se baja utilizando wget:
[root@secure ~]#wget http://urlblacklist.com/cgi-bin/commercialdownload.pl?type=download&file=bigblacklist

Luego se descomprime el listado:
[root@secure ~]#tar -zxfv bigblacklst.tar.gz
Se cambia los propietarios al listado y todo lo que esté dentro de ese directorio:
[root@secure ~]#chown -R root.root blacklist/

A partir de lo anterior se tendrá una lista general de blacklist que actualizará automáticamente, esta lista servirá para todas las listas de DansGuardian. Se hace en este punto porque el listado de frases es lo más importante en el control de filtro de contenidos, si esto funciona bien el resto no tendrá problema.

Luego se procederá a seleccionar frases de esta lista por medio de la configuración web, se procede a ingresar a la configuración por el navegador y dirigiéndose a la página https://192.168.7.24, en el menú Software se selecciona Content Filter y luego se hace click en el botón de edición de Phrase List (Ver Figura 5.12)

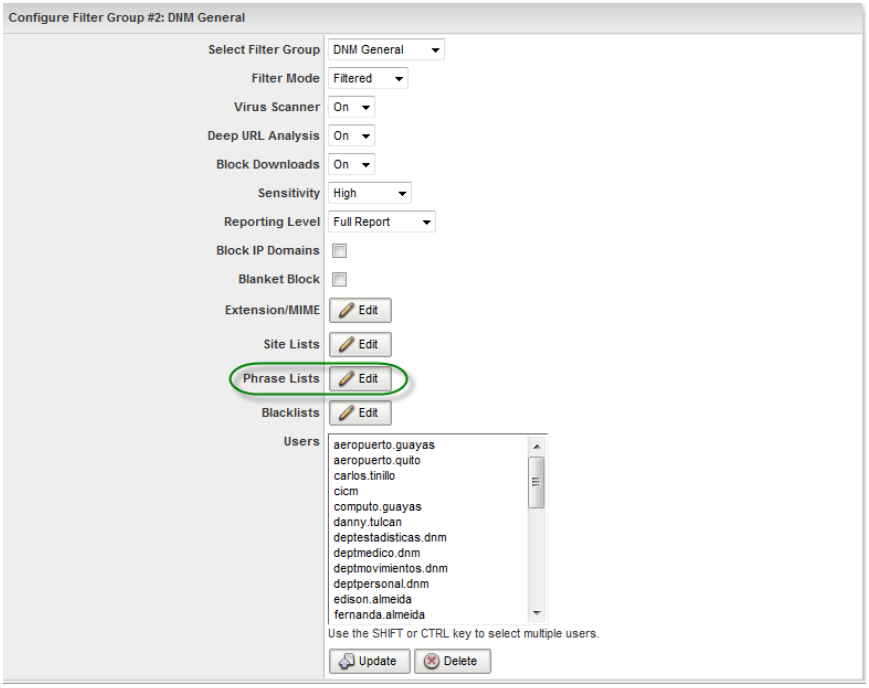


Figura 5.12 Selección configuración de Phrase List

Una vez adentro se elegen todas las frases excepto “forums” y “legaldrugs”, debido a que la DIRECCIÓN NACIONAL DE MIGRACIÓN puede entrar a foros realizados por el Gobierno Nacional y además tienen la opción de investigar sobre medicamentos legales y sus usos. El resto queda restringido por completo (ver Figura 5.13).

Figura 5.13 Selección frases bloqueadas

5.2.3 Configuración de la lista bannedmimetypelist

Contiene una lista de tipos MIME prohibidos. Si una URL retorna un tipo MIME, incluida en esta lista, DansGuardian lo bloqueará. Esta es una forma interesante de bloquear aplicaciones no deseadas, por ejemplo, videos, música, aplicaciones zip, etc. Es obvio que tendra sentido filtrar los tipos MIME text/html o image/*, porque simplemente no se abriría ninguna pagina.

Luego entrando a la configuración por web digitando https://192.168.7.24, se ingresa al menú de Software, luego se va a Content Filter, ahí se elige la opción Extension/MIME (ver Figura 5.14)

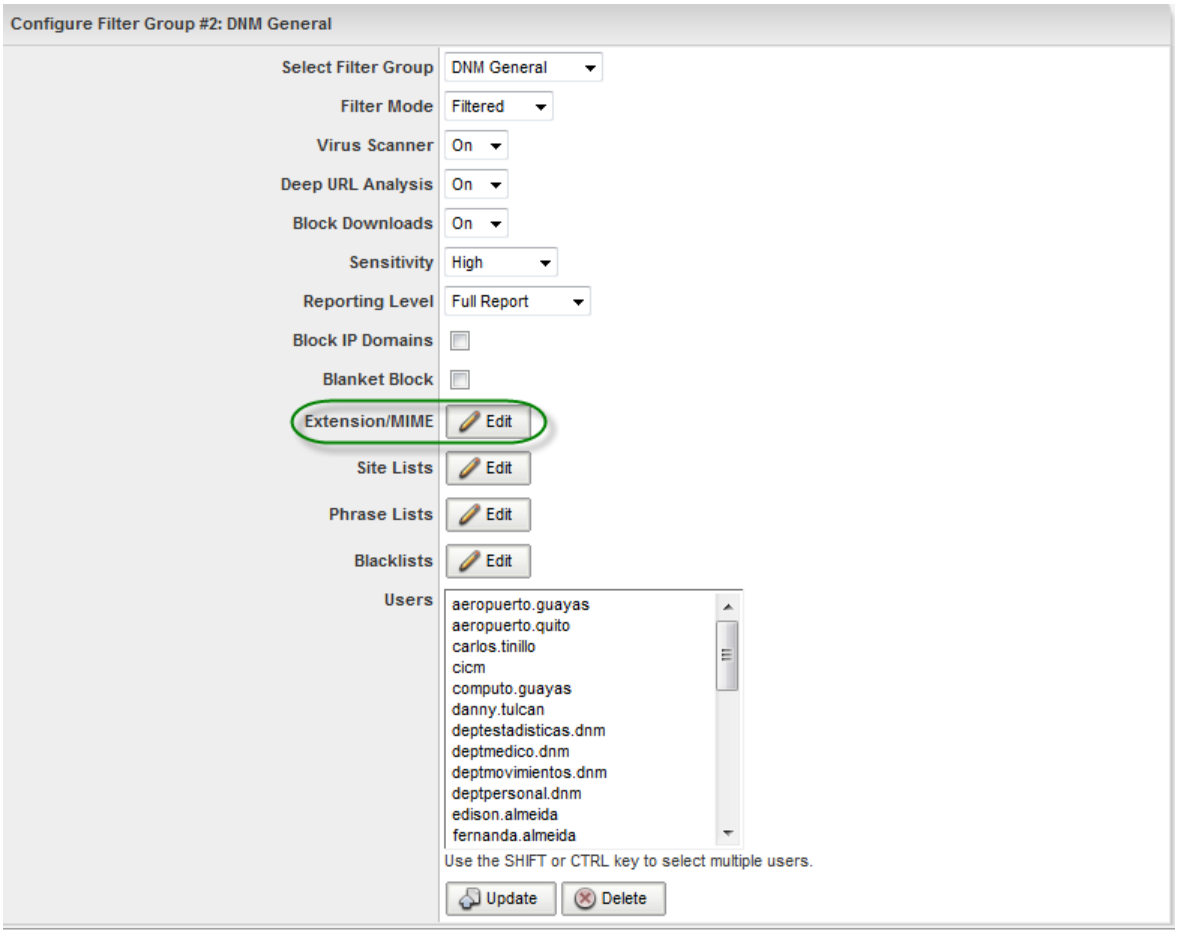


Figura 5.14 Selección configuración de MIME

Una vez adentro se eligen todas las opciones ya que el personal de la DIRECCIÓN NACIONAL DE MIGRACIÓN conoce que no hay permisos a ningún tipo de aplicación, acceso a videos o música. (Ver Figura 5.15)

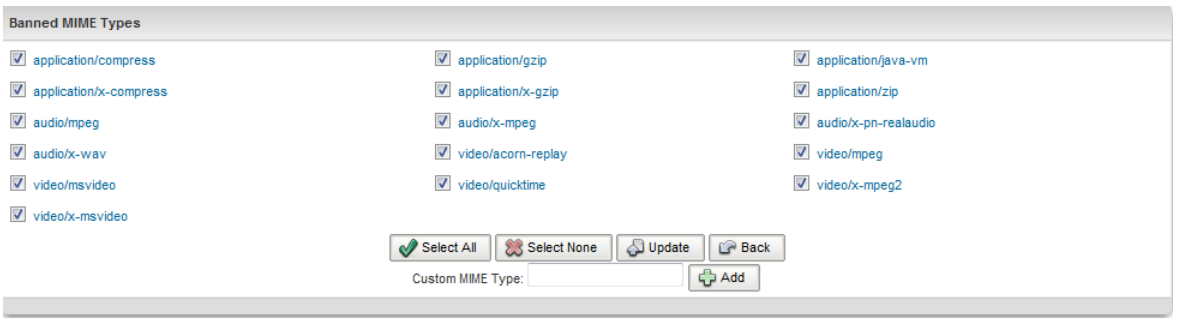


Figura 5.15 Selección tipos de MIME a ser bloqueados

5.2.4 Configuración de la lista bannedextensionlist

Contiene una lista de extensiones de archivos no permitidas. Si una dirección web termina con alguna extensión contenida en esta lista, DansGuardian la

bloqueará. Esta es una buena forma de evitar que se bajen protectores de pantalla y herramientas para hackers. Extensiones como .html o .jpg, no deben bloquearse porque muchas páginas no se abrirían sin ser necesariamente contenido no deseado.

Para seleccionar las extensiones que se deben bloquear hay que ingresar a la configuración web, digitando en el navegardor https://192.168.7.24, se elige el menú Software y la opción Content Filter, luego se escoge la opción de Extension/MIME (ver Figura 5.14).

Una vez adentro se selecciona las extenciones que van a estar prohibidas, para cumplir las políticas de seguridad de la DIRECCIÓN NACIONAL DE MIGRACIÓN, se escogerán todas las que aparecen en pantalla, ya que la única extencion que pueden abrir, en caso de que haya foros, son los archivos .pdf (ver Figura 5. 16).

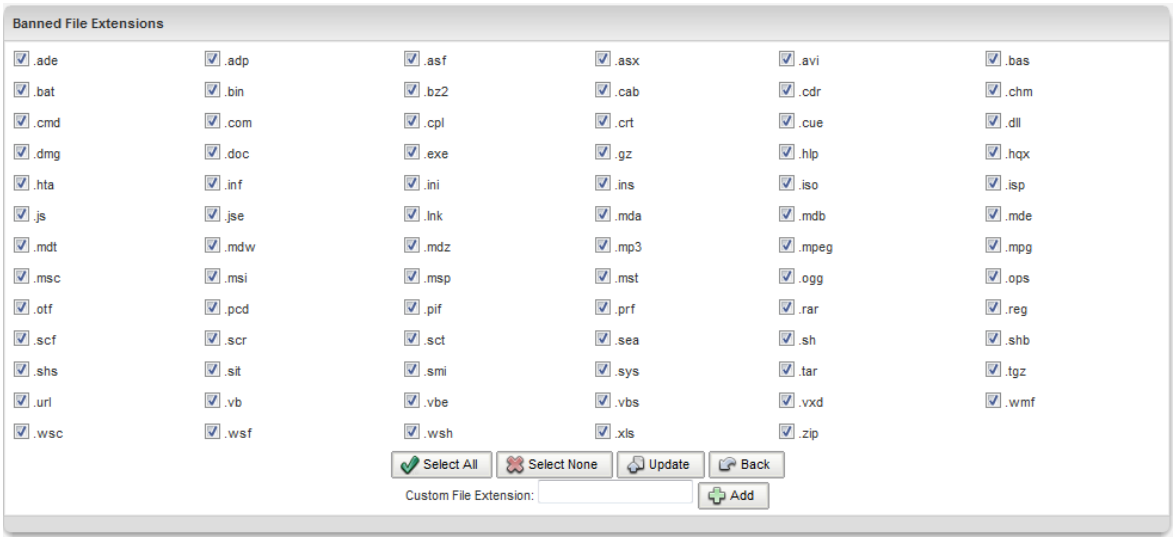


Figura 5.16 Selección configuración de Extensión de archivos

5.2.5 Configuración de la lista bannedsitelist

Este archivo contiene la lista de sitios prohibidos. Al ingresar un nombre de dominio aquí, todo el sitio correspondiente al dominio será bloqueado. Para bloquear partes especificas de un sitio, hay que hacerlo en "bannedurllist".

En base a las configuraciones anteriores, se encuentran bloqueadas todas las páginas que interesan, sin embargo, a algunas páginas hay como entrar por diferentes métodos, a éstas se deben poner en la lista de bannedsitelist (ver Figura5.17) para asegurar que no haya posibilidad alguna de entrar; estas páginas son:

- www.facebook.com
- www.hi5.com
- www.tweety.com
- www.gmail.com
- www.hotmail.com
- www.mercadolibre.com.ec
- www.yahoo.com

El departamento de sistemas deberá estar atento a la existencia de más páginas con este problema, las cuales deberán ponérselas en esta lista.

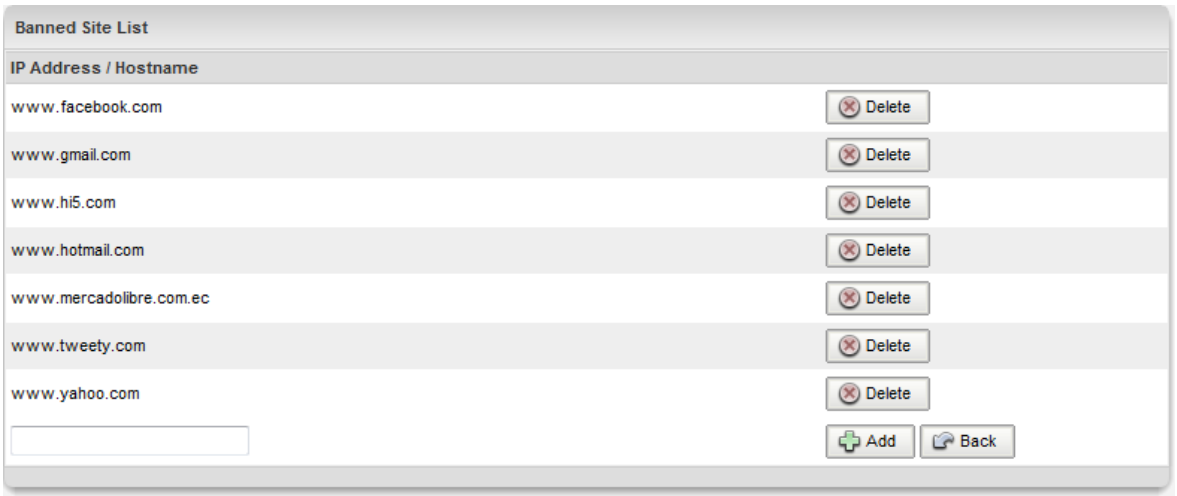


Figura 5.17 Ingreso de dominios en bannedsitelist

5.2.6 Configuración de la lista bannedurllist

Este archivo permite bloquear partes específicas de un sitio web en lugar del sito entero. Para bloquear un sitio entero, ver el apartado 5.2.5. Para habilitar el bloqueo de listas negras (Blacklist), se necesita entrar a la configuración web del servidor digitando en el navegador https://192.168.7.24, luego ir al menú de

Software y ahí elegir Filter Content. Luego se elige la opción Blacklist para ingresar a la configuración (ver Figura 5.18).

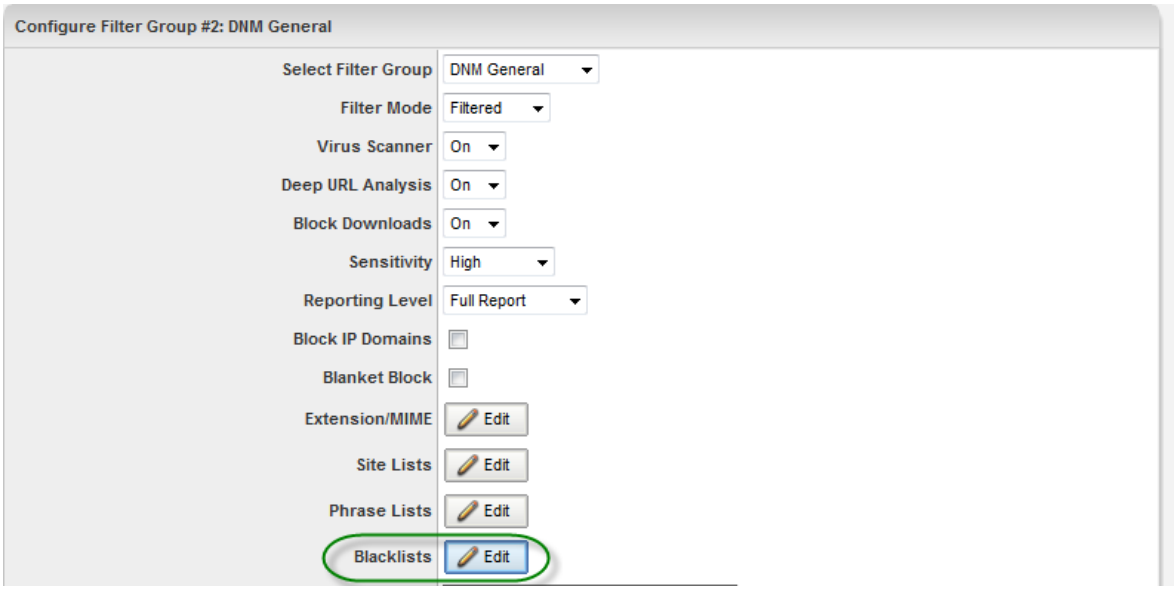


Figura 5.18 Ingreso a la configuración de Blacklist

Una vez adentro hay que elegir todos excepto los siguientes (Ver Figura 5.19, Figura 5.20 y Figura 5.21):

- ads: publicidad de sitios y servidores, ya que muchas páginas usan publicidad sin embargo no hay que filtrarlas.
- antispyware: las actualizaciones del anti virus Kaspesky baja actualizaciones de anti-spyware de su sitio denominado así.
- banking: ya que si tienen permisos de ingresar a páginas de bancos.
- cleanning: ya que el antivirus usa criterios de dominio denominados así.
- government: ya que si pueden entrar a toda página gubernamental.
- sexual_education: ya que si está permitido entrar a páginas educativas, sea cual sea el tema.
- whitelist: ya que pueden entrar a páginas denominadas en listas bancarias por servidores mundiales.

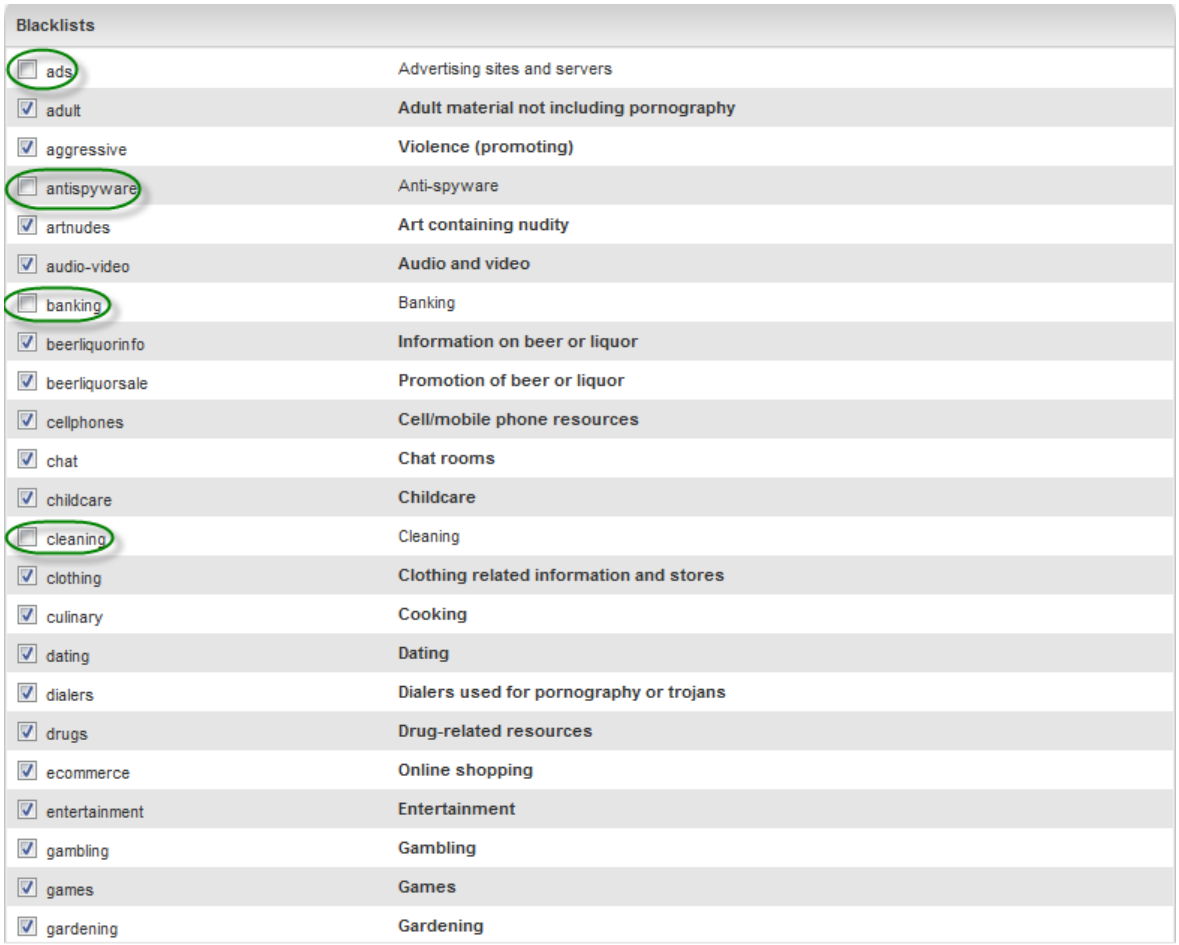


Figura 5.19 Configuración de Blacklist parte 1

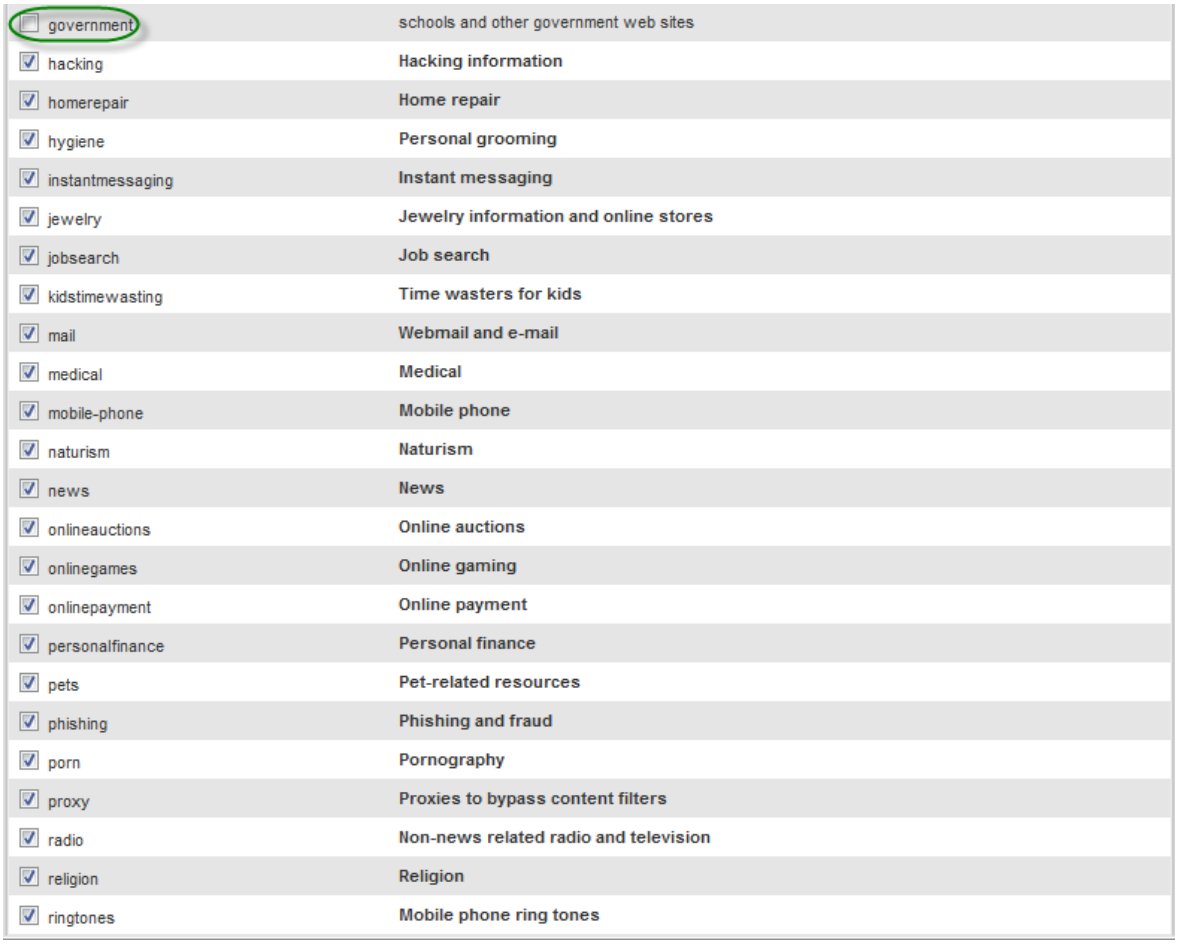


Figura 5.20 Configuración de Blacklist parte 2

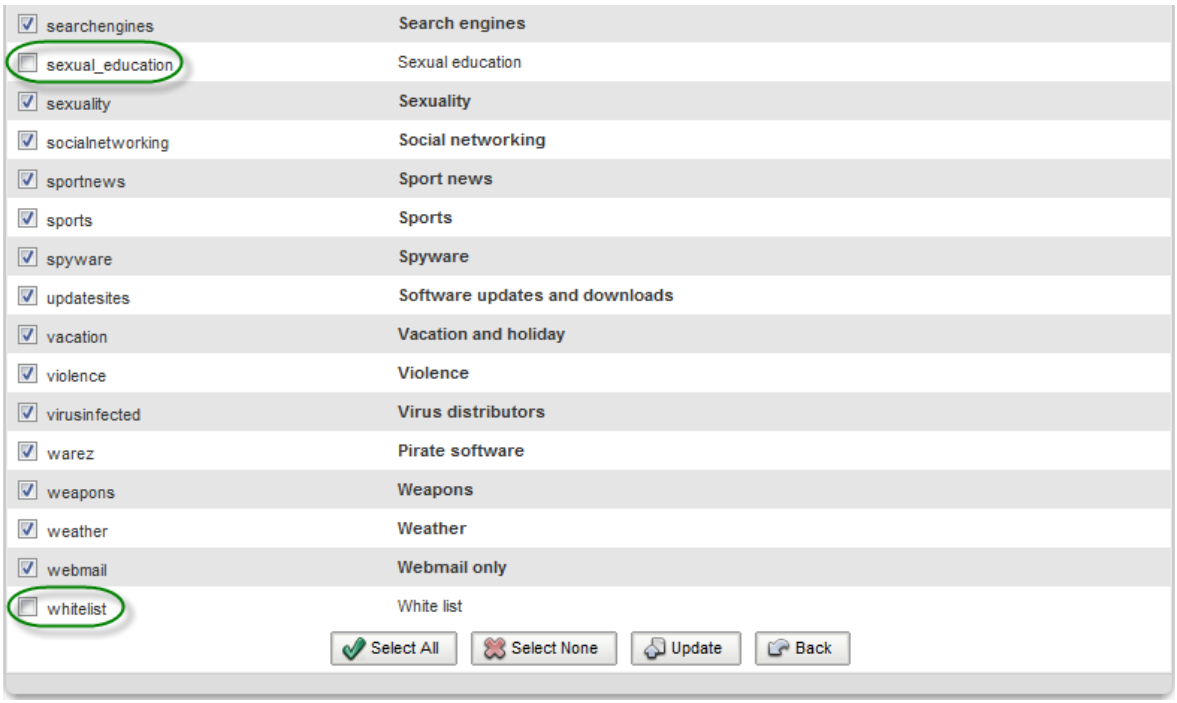


Figura 5.21 Configuración de Blacklist parte 3

5.2.7 Configuración del archivo dansguardian.conf

Este archivo se encuentra en /etc/dansguardian-av/dansguardian.conf. La única configuración que hay que cambiar aquí es el valor de accessdeniedaddress. El mismo debe equivaler a la dirección web del servidor Apache con el script perl de reporte de acceso denegado. Apache está instalado en el mismo servidor Squid y DansGuardian.

accessdeniedaddress = 'http://192.168.7.24/cgi-bin/dansguardian.pl'

Sin embargo a continuación se explicarán los parámetros más importantes de este fichero para entenderlos y configurarlos de la mejor manera.

5.2.7.1 Reporting Level

El nivel de reporte es configurable y éste aparece cuando una página es denegada. El reporte puede decir simplemente 'Acceso Denegado' op. 1, o mostrar detalles de porque ha sido denegado y que es lo que se ha denegado op 2. Esta última opción puede ser útil para analizar, pero puede ocurrir que no necesite tanto detalle en una aplicación de producción como en este caso. El modo Stealth agrega los detalles al histórico pero no bloquea nada op -1. En este caso se pondrá la opción 1.

reportinglevel = 1

5.2.7.2 Logging Settings

Esta permite configurar el nivel del reporte histórico (log). Puede no reportar nada, solamente las páginas denegadas o todos los requerimientos de páginas. Los requerimientos de páginas seguras (HTTPS) solo se registran en el histórico cuando el valor de logging equivale a 3 (todos los requerimientos) la cual en este caso se escogerá, para poder tener un reporte mucho más amplio.

loglevel = 3

5.2.7.3 Network Settings

Aqui se puede modificar la dirección IP en la que DansGuardian va a aceptar conexiones, el puerto en el que va a escuchar, la dirección de IP y el puerto del servidor Squid.

filterip =

filterport = 8080

proxyip = 127.0.0.1

proxyport = 3128

5.2.7.4 Content Filtering Settings

Aquí se especifica la ubicación de los archivos que contienen las listas de filtrado, las cuales fueron configuradas anteriormente. Por lo tanto no es recomendable modificar estos valores.

filtergroupslist = '/etc/dansguardian-av/lists/filtergroupslist'

bannediplist = '/etc/dansguardian-av/lists/bannediplist'

exceptioniplist = '/etc/dansguardian-av/lists/exceptioniplist'

banneduserlist = '/etc/dansguardian-av/lists/banneduserlist'

exceptionuserlist = '/etc/dansguardian-av/lists/exceptionuserlist'

5.2.7.5 Reverse Lookups for Banned Sites and URLs

Si se habilita esta opción, DansGuardian hará la resolución reversa DNS (Servidor de Nombre de Dominio) y buscarlo en las listas correspondientes de sitio y URL. Esto evitará, por ejemplo, que un usuario entre a una dirección IP para acceder a dominios prohibidos. Esta opción afecta a la velocidad de búsqueda, por lo que no será la activada. Es recomendable dejar esta opción deshabilitada y usar la opción Blanket IP Block option en el archivo bannedsitelist.

reverseaddresslookups = off

5.2.7.6 Build bannedsitelist and bannedurllist Cache Files

Esta opción compara las fechas de actualización de los archivos de las listas y archivos de cache, si encuentra inconsistencias los regenera de ser necesario. Esto incrementa el proceso de inicio en un 200%. En computadores lentos la diferencia es significativa.

createlistcachefiles = on

5.3 IMPLEMENTACION DE LA SOLUCION FIREWALL

Se procederá a configurar este servicio a través del fichero de configuración de IPTABLES que se halla en /sbin/iptables, con esto se conseguiráque cumpla su tarea con toda la seguridad para el sistema.

Iptables es la herramienta que permite configurar las reglas del sistema de filtrado de paquetes de Linux. Con esta herramienta, se podrá crear un firewall adaptado a las necesidades de la DIRECCIÓN NACIONAL DE MIGRACIÓN.

En el archivo iptables se crean reglas, dirigiendo a cada una de ellas diferentes características que deben cumplir todos los paquetes que entren o salgan del área perimetral del servidor. Además, para cada regla se especifica y se aplica una acción. Las reglas tienen un orden, y cuando se recibe o se envía un paquete, las reglas se verifican en orden hasta que las condiciones que pide una de ellas se cumplen en el paquete, y la regla se activa aplicando sobre el paquete la acción que se haya especificado.

Estas acciones se aplican en los denominados targets, que indican la acción que se debe aplicar a cada paquete. Los más usados son bastante evidentes: ACCEPT, DROP y REJECT, pero también hay targets que permiten funcionalidades extras y muchas veces interesantes: LOG, MIRROR.

El esquema de filtrado de paquetes de Linux se establece en tres tablas bien marcadas, cada una con distintas acciones a las que debe pertenecer un paquete, la estructura jerárquica se divide así.

filter: tabla por defecto, para los paquetes que se refieran a la máquina
    INPUT: paquetes recibidos para nuestro sistema
    FORWARD: paquetes enrutados a través del sistema propio
    OUTPUT: paquetes generados en el sistema propio y que son enviados
nat: tabla referida a los paquetes enrutados en un sistema con Masquerading
    PREROUTING: alteran los paquetes según entren
    OUTPUT: alteran paquetes generados localmente antes de enrutar
    POSTROUTING: alteran los paquetes cuando están a punto para salir
mangle: alteraciones más especiales de paquetes
    PREROUTING: alteran los paquetes entrantes antes de enrutar
    OUTPUT: alteran los paquetes generados localmente antes de enrutar

5.3.1 Creación de reglas con Iptables

Para configurar el servicio de firewall, se necesita ejecutar comandos sobre iptables, las cuales se señala a continuación:

Para crear una nueva regla al final de las ya existentes en una chain determinada:

$ /sbin/iptables -A [chain] [especificacion_de_la_regla] [opciones]

Para insertar una regla en una posición determinada de la lista de reglas de una chain determinada:

$ /sbin/iptables -I [chain] [posición] [especificacion_de_la_regla] [opciones]

Para borrar una regla en una posición determinada de la lista de reglas de una *chain* determinada:

$ /sbin/iptables -D [chain] [posición]

Para todas las reglas de una *chain* determinada:

$ /sbin/iptables -F [chain]

Para listar las reglas de una *chain* determinada:

$ /sbin/iptables -L [chain]

La especificación de reglas se hace con los siguientes parámetros (especificando aquellos que se necesite):

- **-p [protocolo]:** protocolo al que pertenece el paquete.

- **-s [origen]:** dirección de origen del paquete, puede ser un nombre de host, una dirección IP normal, o una dirección de red (con máscara, de forma dirección/máscara).
- **-d [destino]:** dirección de destino, puede ser un nombre de host, dirección de red o dirección IP singular.
- **-i [interfaz-entrada]:** especificación del interfaz por el que se recibe el paquete.
- **-o [interfaz-salida]:** interfaz por el que se va a enviar el paquete.
- **[!] -f:** especifica que la regla se refiere a los siguientes fragmentos de un paquete ya fragmentado: si se antepone !, se refiere sólo al primer paquete, o a los paquetes no fragmentados.

Para que permita elegir qué se hará con el paquete:

- **-j [target]:** permite elegir el target al que se debe enviar ese paquete, esto es, la acción a llevar a cabo con el.

Las opciones que se permiten en los comandos ya nombrados son:

- **-v:** modo verboso, útil sobre todo con iptables -L.
- **-n:** las direcciones IP y números de puertos se mostrarán numéricamente (sin resolver nombres).
- **--line-numbers:** muestra los números de regla, de manera que sea más fácil identificarlas para realizar operaciones de inserción y borrado.

5.3.1.1 Tráfico de la interfaz de loopback (Lo)

Permitirá cualquier tráfico que provenga de loopback (lo), para ello se insertará en el chain INPUT (que se encarga de los paquetes que llegan con destino a la máquina), de la tabla filter con la siguiente regla:

```
$ /sbin/iptables -A INPUT -i lo -j ACCEPT
```

5.3.1.2 Tráfico de la interfaz de intranet (eth1)

Se permitirá todo el tráfico que provenga del interfaz de red interna eth1, la cual controlará el tráfico efectuado por la intranet de la DIRECCIÓN NACIONAL DE MIGRACIÓN, ya que por esta interfaz navegarán al Internet todas las jefaturas y sub jefaturas de la Policía a nivel nacional.

```
$ /sbin/iptables -A INPUT -i eth1 -j ACCEPT
```

El hecho de omitir aquí la dirección de origen y de destino es porque se referieren a todas.

5.3.1.3 Tráfico de paquetes TCP

Se impedirá el paso de cualquier paquete TCP proveniente del exterior que intente establecer una conexión con el equipo ya que las conexiones de VPN no están permitidas en las políticas de la DIRECCIÓN NACIONAL DE MIGRACIÓN. Estos paquetes se reconocen por tener el flag SYN acertado y los flags ACK y FIN desacertados. Para decirle a la regla que reconozca específicamente estos paquetes, se usará la opción --syn que se puede aplicar cuando el protocolo del paquete es declarado como tcp de la siguiente manera:

```
$ /sbin/iptables -A INPUT -p tcp --syn -j REJECT --reject-with icmp-port-unreachable
```

También se ve el uso de una opción del target REJECT, que permite elegir de qué manera debe ser rechazado el paquete. Posibles valores son icmp-net-unreachable, icmp-host-unreachable, icmp-port-unreachable, icmp-proto-unreachable, icmp-net-prohibited y icmp-host-prohibited, en este caso se elige el primero para que el rechazo sea por puerto.

5.3.1.4 Tráfico de paquetes UDP

Antes de declarar que hay que prohibir cualquier tráfico UDP hacia la máquina, y dado que las reglas se recorren en orden hasta que una de ellas se activa con el paquete, se tendrá que añadir, ahora, una regla que permita recibir las respuestas

de los servidores DNS cuando el sistema les realice alguna consulta. Estas respuestas, vía UDP, saldrán del puerto 53 del servidor DNS. La regla es:

$ /sbin/iptables -A INPUT -p udp --source-port 53 -j ACCEPT

Donde --source-port es una opción presente cuando el protocolo es udp (también cuando es tcp) y permite, en este caso, especificar que la consulta provenga del puerto destinado al DNS.

En este momento se prohibirá el resto del tráfico UDP. La regla, de por sí, implica a todo el tráfico UDP, pero como un paquete sólo activará esta regla si no ha activado la anterior, los paquetes UDP referentes a una transacción con un servidor de nombres no se verán afectados.

$ /sbin/iptables -A INPUT -p udp -j REJECT --reject-with icmp-port-unreachable

Dado que los targets por defecto (denominados policy o política) en la tabla filter son ACCEPT, si un paquete no activa ninguna de las reglas, será aceptado, de manera que no habrá que preocuparse, por ejemplo, de los paquetes de tráfico normal de TCP, ya que estos serán aceptados al no activarse regla alguna.

5.3.1.5 Re direccionamiento de puertos (port forwarding)

Se obliga a que el kernel permita ip-forwarding.

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Permitimos el forward desde iptables (eth0 es la interface pública).

```
# iptables -A FORWARD -i eth0 -j ACCEPT
# iptables -A FORWARD -o eth0 -j ACCEPT
```

Se hará que las ips se enmascaren para no perder los filtros de seguridad por IP.

```
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Se definirán las reglas del Port Forwarding para los 2 servidores, Mail Server: 192.168.7.232 se redireccioná únicamente el puerto 110 para que puedan recibir mail`s; el puerto 25 de SMTP no se activará porque según las políticas de la DIRECCIÓN NACIONAL DE MIGRACIÓN nadie podrá revisar sus mail`s fuera de la institución y, la Web Server: 192.168.7.233 se redireccionará el puerto 80 del apache y el 81 de https, para poder publicar la pagina web (ver Figura 5.22).

iptables -t nat -A PREROUTING -p tcp -i eth0 --dport 110 -j DNAT –to destination 192.168.7.232:110

iptables -t nat -A PREROUTING -p tcp -i eth0 --dport 80 -j DNAT --to-destination 192.168.7.233:80

iptables -t nat -A PREROUTING -p tcp -i eth0 --dport 81 -j DNAT --to-destination 192.168.7.233

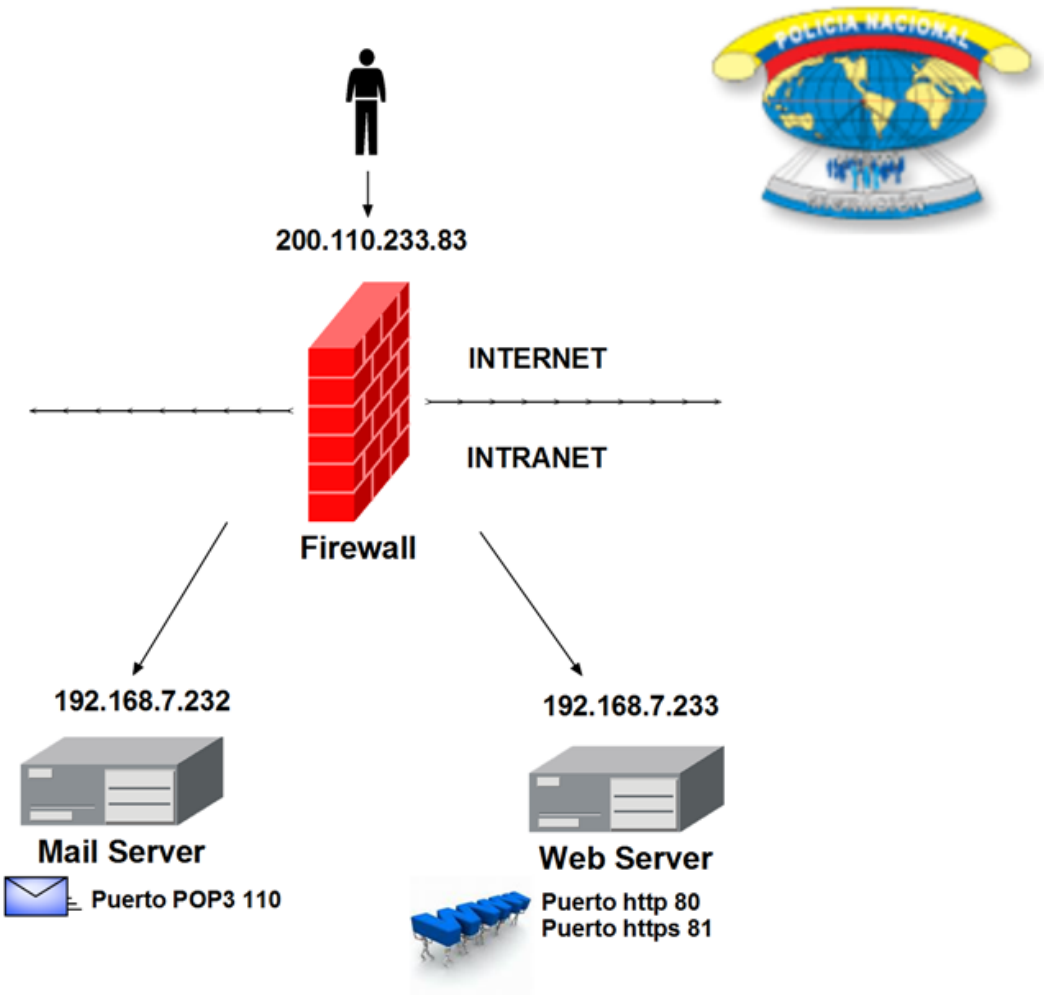


Figura 5.22 Diagrama propuesto para Port Forwarding

5.3.1.6 Guardar y reusar configuración de iptables

Si en este momento se apaga el servidor, toda la configuración que se ha realizado se perderá, y habrá que volver a realizar toda la configuración.

Iptables cuenta con dos programas auxiliares: iptables-save e iptables-restore, el primero permite guardar el contenido de las tablas IP, y el segundo permite, a partir de la última ejecución de iptables-save, recuperar la configuración de las tablas.

De manera que para guardar la configuración del firewall en un fichero ejecutaremos:

```
$ /sbin/iptables-save -c > [fichero]
```

Donde -c es una opción que permite guardar los contadores del número de paquetes que activaron cada regla.

Y, cuando se quiera, se podrá recuperar la configuración del firewall con:

```
$ /sbin/iptables-restore -c < [fichero]
```

En cuyo caso -c tiene el mismo significado que con iptables-save

Estas llamadas a iptables-save e ipatbles-restore podrán ser incluidas en los scripts adecuados para que se lleven a cabo de manera automática en el arranque y el cierre del sistema.

Una vez salvada la configuración con iptables-save en el archivo /etc/sysconfig/iptables, se pueden activar los scripts que arrancarán y cerrarán el firewall automáticamente al arrancar y apagar el equipo, mediante la Text Mode Setup Utility (/usr/sbin/setup), en la sección System Services (ver Figura 5.23).

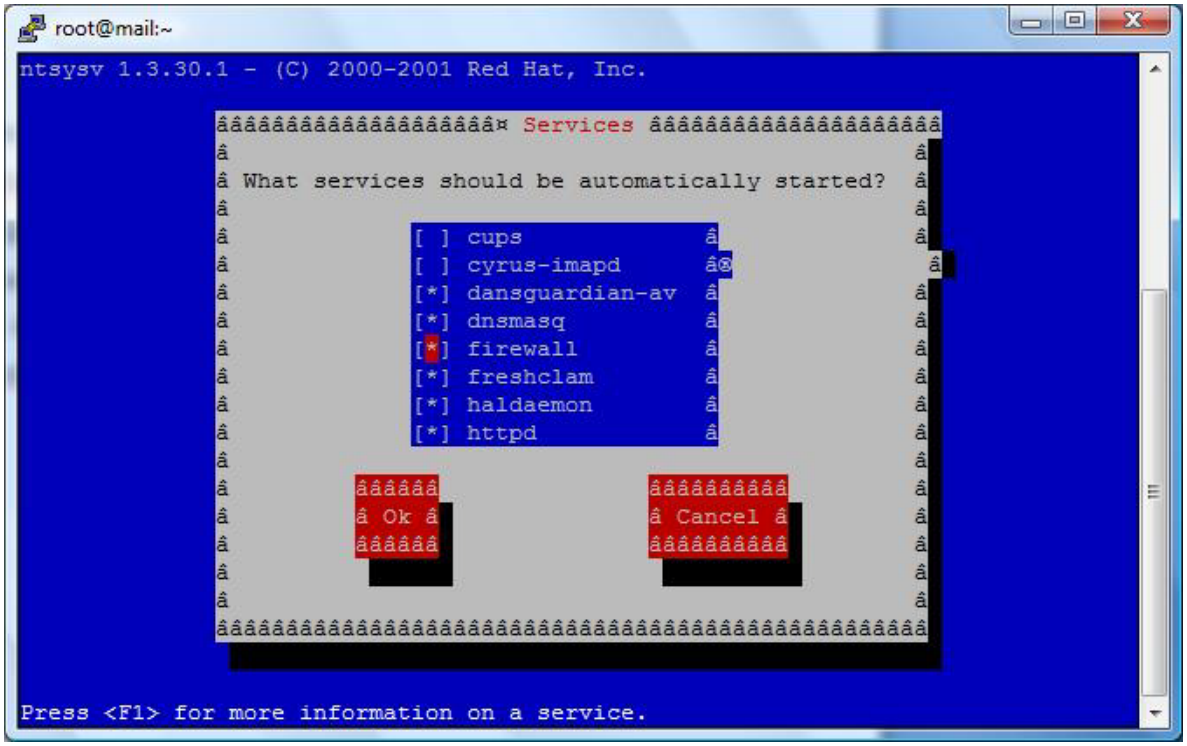


Figura 5.23 Arranque automático del firewall

5.4 IMPLEMENTACIÓN DE LA SOLUCIÓN DETECCIÓN DE INTRUSOS

Se procederá a configurar este servicio por web accediendo al servidor de la siguiente manera: https://192.168.7.24. Lo que no haya como configurar en modo gráfico se lo hará a través del fichero de configuración de SNORT que se halla en /etc/snort.conf y será lo editado con la herramienta “nano” para realizar los cambios adecuados y conseguir que cumpla su tarea con toda la seguridad para el sistema.

Snort rastrea los paquetes que circulan por la red y al encontrar un paquete sospechoso (según unas reglas previamente definidas), lo loguea en MySQL.

Los usos y posibilidades de esta herramienta son realmente variados aunque lo más común es utilizarlo como "packet logger" o sniffer, con grabación automática a texto plano o BD MySQL/PostgreSQL.

5.4.1 Funcionamiento de Snort

Snort funciona como un sniffer realizando un escaneo por pantalla de todo el tráfico (la opción -vd muestra más información).

snort -v (-vd)

Ejecuta snort y guarda el log en la ruta indicada en el formato predeterminado (binario). Para visualizar este fichero se utiliza la opción –r

snort -l ruta_fichero_log –d

snort -r ruta_fichero_log

Para una configuración inicial con reglas de detección originales, se descargan las establecidas por la comunidad desde el site oficial de la aplicación http://dl.snort.org/sub-rules/snortrules-snapshot-CURRENT_s.tar.gz, en formato comprimido tar.gz.

Para habilitar estas reglas se copiarán (descomprimidas) al directorio de configuración de snort (/etc/snort/rules/) y se editará el fichero de configuración del programa asegurándo que las reglas estén visibles:

nano /etc/snort.conf

var RULE_PATH rules

include $RULE_PATH/sql.rules

include $RULE_PATH/tcp.rules

Ahora se debe cargar la nueva configuración:

snort -c /etc/snort.conf

5.4.2 Configuración de MySql para Snort

Para que Snort deje sus logs en la base de datos, primero hay que crear una nueva base de datos con sus tablas correspondientes, así como un usuario que sólo tenga acceso a esa base de datos.

mysql -u root

Lo primero que deberá hacerse es establecer una contraseña para el acceso del administrador:

mysql> GRANT ALL PRIVILEGES ON mysql.* TO root@localhost IDENTIFIED BY ’migra#3454’;

De este modo, el siguiente paso será crear una base de datos para Snort: mysql> CREATE DATABASE snort;

Una vez creada la base de datos de Snort, hay que establecer un usuario con todos los permisos sobre esa base de datos, para no tener que utilizar el usuario "root", ya que esto supondrá un riesgo innecesario. Se creará un usuario "snort" al que se le dará permisos sobre su base de datos:

mysql> GRANT ALL PRIVILEGES ON snort.* TO snort@localhost IDENTIFIED BY 'migra#3454';

Creada la base de datos y creado el usuario, se podrá entonces salir de la MySQL y seguir con la configuración. Las tablas de la base de datos que se crearon, serán las tablas que Snort necesite para dejar sus logs según la información contenida en cada tipo de log. Para crearlas se grabará el contenido de un fichero que ya contiene la estructura:

mysql snort -u root -p < ./contrib/create_mysql

5.4.3 Configuración de reglas de detección en Snort

Se editará el archivo de configuración copiado antes en /etc. Al editar el fichero /etc/snort.conf se podra ver que está muy bien comentado, y antes de cada opción hay una explicación de varias líneas.

Primero hay que definir el rango de direcciones de la red interna. Hay tres maneras de hacerlo. La primera define un rango de ip's, la segunda define el rango de ip's del cual forma parte la ip que tiene la tarjeta de red en el momento de lanzar Snort, y la tercera especifica varios rangos de ip's (si hay subredes, por ejemplo).De este mismo modo se definen ciertas máquinas importantes de nuestra red:

var HOME_NET 192.168.7.0/24
var HOME_NET $eth0_ADDRESS
var HOME_NET [192.168.7.0/24,192.168.2.0/24…..]
var SMTP 192.168.7.10
var HTTP_SERVERS [192.168.7.10,192.168.7.2]
var SQL_SERVERS [192.168.7.10,192.168.7.2]

var LOCAL_HOSTS [192.168.7.1,192.168.7.100,192.168.7.110,192.168.7.254]

También se define la red externa (Internet):
var EXTERNAL_NET any

A partir de aquí, hay que definir los preprocesadores. Esto es, plug-ins o partes del programa que definen una manera de escanear los paquetes y detectar un mal funcionamiento o un tipo de ataque. Los preprocesadores están sobradamente comentados y explicados antes de cada línea de código.

La manera de declarar cada preprocesador es la siguiente:

preprocessor nombre: argumento1,argumento2,argumento3,argumento4

Cabe destacar un preprocesador especial, SPADE (Statistical Package Anomaly Detection Engine), que estudia el tráfico en las máquinas que se especifiquen. A partir de ese estudio se sacan conclusiones de lo que es un paquete anómalo y lo que no lo es. Es decir, la probabilidad de que un paquete se dirija a la dirección IP 192.168.7.233, al puerto 8080, es de un 10%.... mientras que la probabilidad de que un paquete se dirija de esa misma IP al puerto 8079 es de un 0,1 %. El grado de anomalía de un paquete se mide según la siguiente fórmula: A(X) = -Log2(P(X))

Por lo que el grado de anomalía de 192.168.7.233:8080 es de 3.32 (casi no es anómalo), mientras que para 192.168.7.233:8079 es de 9.97 (muy anómalo).

Por último, deberemos configurar los Output Plugins, que definen a donde tienen que ir a parar los logs que Snort genera. Deciden si van a ficheros de texto (logs) o a una base de datos, y también en que formato irán escritos (binario, texto plano, xml...). Se establecerá que guarde la salida en la base de datos MySQL:

output database: log, mysql, user=snort dbname=snort password=migra#3454 host=localhost

Aparte de eso, hay que especificar que también guarde los logs en otros formatos y localizaciones (syslog).

Finalmente, hay que escribir reglas de logging. Snort tiene ya diversos archivos con reglas escritas, que para empezar ya están bien definidas. Se añadirán al final del snort.conf, y habrá que especificar la ruta, es decir, en /etc/snort-rules, hay que especificar esa ruta antes de cada fichero de reglas. Es importante saber qué ficheros de reglas se deben guardar en los logs antes de incluirlos, puesto que las reglas por defecto son muy restrictivas, y logean todo (hasta los echo-request y echo-reply de los pings) por lo que es posible que en una semana estén sin un solo Mb libre en el disco duro.

Sólo se deben guardar aquellos tipos de paquetes que concuerden con ataques, o intentos de intrusión, por ejemplo buffer overflows en los servicios, intentos de FTP como root, login erróneo por telnet, etc.

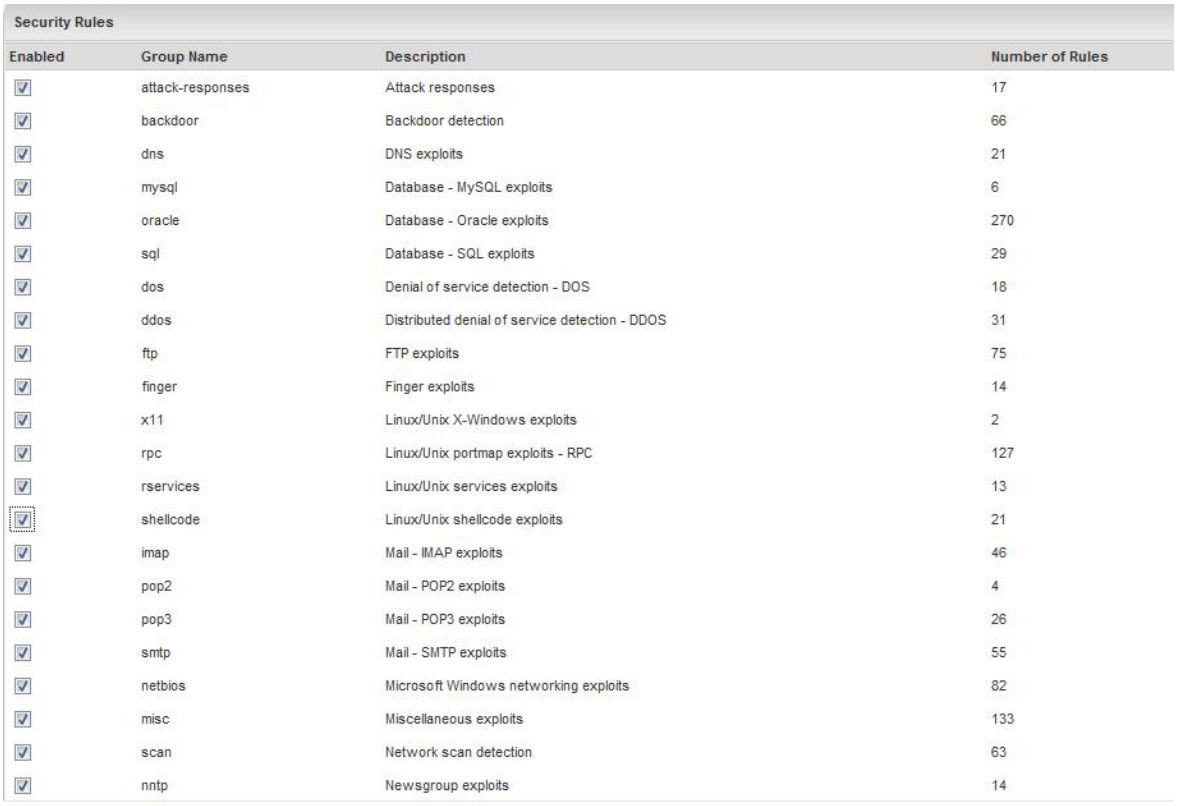
Ahora se procederá a correr Snort del siguiente modo:

```
# snort -dev -l /var/log/snort -h 192.168.7.0/24 -c /etc/snort.conf &
```

El argumento '-l' define el directorio donde se deben guardar los logs en formato de texto plano o binario. Esto se lo hará por seguridad en caso de que MySql falle.

5.4.4 Despliegue de reglas en la configuración grafica

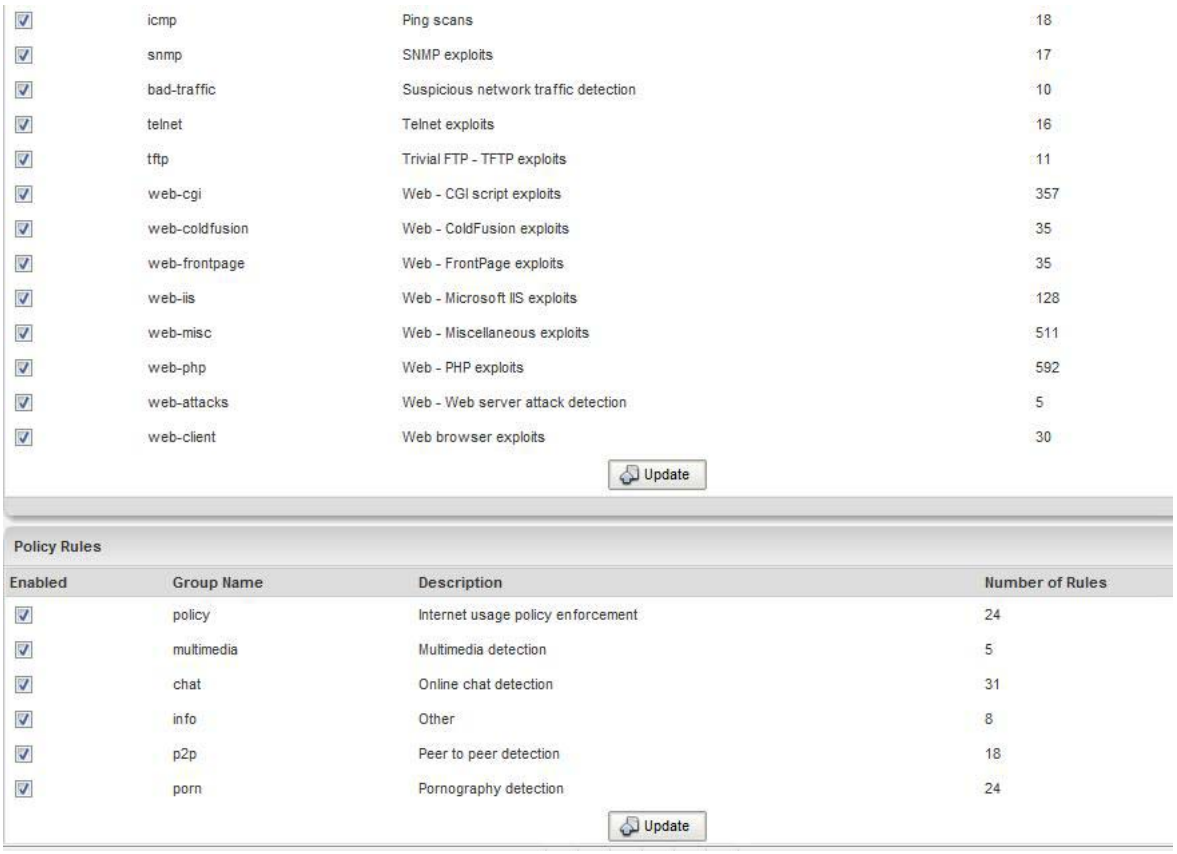
Luego de cargar el archivo de reglas de seguridad y políticas de seguridad definidas por la organización de Snort se logrará cargar y pre definir cada una de estas reglas, como se ve en las Figura 5.24 y Figura 5.25, donde están seleccionadas todas las reglas y políticas de seguridad para que el sistema de detección de intrusos quede configurado por completo.



Security Rules

Enabled	Group Name	Description	Number of Rules
☑	attack-responses	Attack responses	17
☑	backdoor	Backdoor detection	66
☑	dns	DNS exploits	21
☑	mysql	Database - MySQL exploits	6
☑	oracle	Database - Oracle exploits	270
☑	sql	Database - SQL exploits	29
☑	dos	Denial of service detection - DOS	18
☑	ddos	Distributed denial of service detection - DDOS	31
☑	ftp	FTP exploits	75
☑	finger	Finger exploits	14
☑	x11	Linux/Unix X-Windows exploits	2
☑	rpc	Linux/Unix portmap exploits - RPC	127
☑	rservices	Linux/Unix services exploits	13
☑	shellcode	Linux/Unix shellcode exploits	21
☑	imap	Mail - IMAP exploits	46
☑	pop2	Mail - POP2 exploits	4
☑	pop3	Mail - POP3 exploits	26
☑	smtp	Mail - SMTP exploits	55
☑	netbios	Microsoft Windows networking exploits	82
☑	misc	Miscellaneous exploits	133
☑	scan	Network scan detection	63
☑	nntp	Newsgroup exploits	14

Figura 5.24 Reglas de seguridad de Snort



☑	icmp	Ping scans	18
☑	snmp	SNMP exploits	17
☑	bad-traffic	Suspicious network traffic detection	10
☑	telnet	Telnet exploits	16
☑	tftp	Trivial FTP - TFTP exploits	11
☑	web-cgi	Web - CGI script exploits	357
☑	web-coldfusion	Web - ColdFusion exploits	35
☑	web-frontpage	Web - FrontPage exploits	35
☑	web-iis	Web - Microsoft IIS exploits	128
☑	web-misc	Web - Miscellaneous exploits	511
☑	web-php	Web - PHP exploits	592
☑	web-attacks	Web - Web server attack detection	5
☑	web-client	Web browser exploits	30

Update

Policy Rules

Enabled	Group Name	Description	Number of Rules
☑	policy	Internet usage policy enforcement	24
☑	multimedia	Multimedia detection	5
☑	chat	Online chat detection	31
☑	info	Other	8
☑	p2p	Peer to peer detection	18
☑	porn	Pornography detection	24

Update

Figura 5.25 Reglas de las políticas de Snort

Así se habrá logrado implementar de forma exitosa el IDS en el servidor de seguridad de la DIRECCIÓN NACIONAL DE MIGRACIÓN.

5.5 IMPLEMENTACIÓN DE LA SOLUCIÓN PREVENCIÓN DE INTRUSOS

Para implementar de forma adecuada la solución de prevención de intrusos se usará SNORTSAM, para esto hay que modificar el fichero /etc/snortsam.conf.

La herramienta SnortSam sirve para bloquear ataques la cual está dividida en 2 partes:

- Una herramienta que amplia Snort añadiendo un nuevo módulo de salida: alert_fwsam.
- Otra herramienta que habla directamente con el firewall.

SnortScan funciona de la siguiente manera: Snort observa el tráfico, cuando una regla se incumple manda la salida al modulo fwsam. El módulo fwsam manda un mensaje encriptado a SnortSam. SnortSam chequea el mensaje, si proviene de una fuente autorizada entonces desencripta el mensaje. Una vez que el mensaje está desencriptado, SnortSam chequea la petición para ver la dirección IP que se está pidiendo que bloquee SnortSam. SnortSam chequea la dirección con una lista de direcciones IP que nunca deberían ser bloqueadas. Si la dirección IP no está en la lista, SnortSam le comunica al firewall que bloquee dicha dirección durante un tiempo determinado.

5.5.1 Configuración Snort para SnortSam

El primer paso es indicarle a Snort que tiene un nuevo módulo de salida para usar, añadiendo la siguiente línea al fichero snort.conf.

Output alert_fwsam: 192.168.7.24

Donde 192.168.7.24 es la dirección IP donde se encuentra SnortSam ejecutándose.

Ahora hay que configurar las reglas de Snort para usar SnortSam. Para ello se deberá encontrar la siguiente regla en el archivo /etc/snort/web-misc.rules, editándolo en este caso con “nano”.

Alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:”WEB-MISC /.root access”; flow:to_server,established; uricontent:”/.root”; nocase; classtype:attempted-recon; sid:1145; rev:7;)

Y modificarla de la siguiente manera:

Alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:”WEB-MISC /.root access”; flow:to_server,established; uricontent:”/.root”; nocase; classtype:attempted-recon; sid:1145; rev:7; fwsam: src,10 minutes;)

5.5.2 Configuración SnortSam para el firewall

En el fichero snortsam.conf no indica el path del fichero donde hay que poner la lista de sistemas que nunca serán bloqueados. Se debe hacer mediante el comando include en el fichero de listas blancas de snortsam ubicada en /etc/Snort/snortsam/ webconfig-whitelist.conf; para este caso la única IP que nunca deberá ser bloqueda es la del director de sistemas, la cual es 192.168.7.2 (ver Fig 5.26):

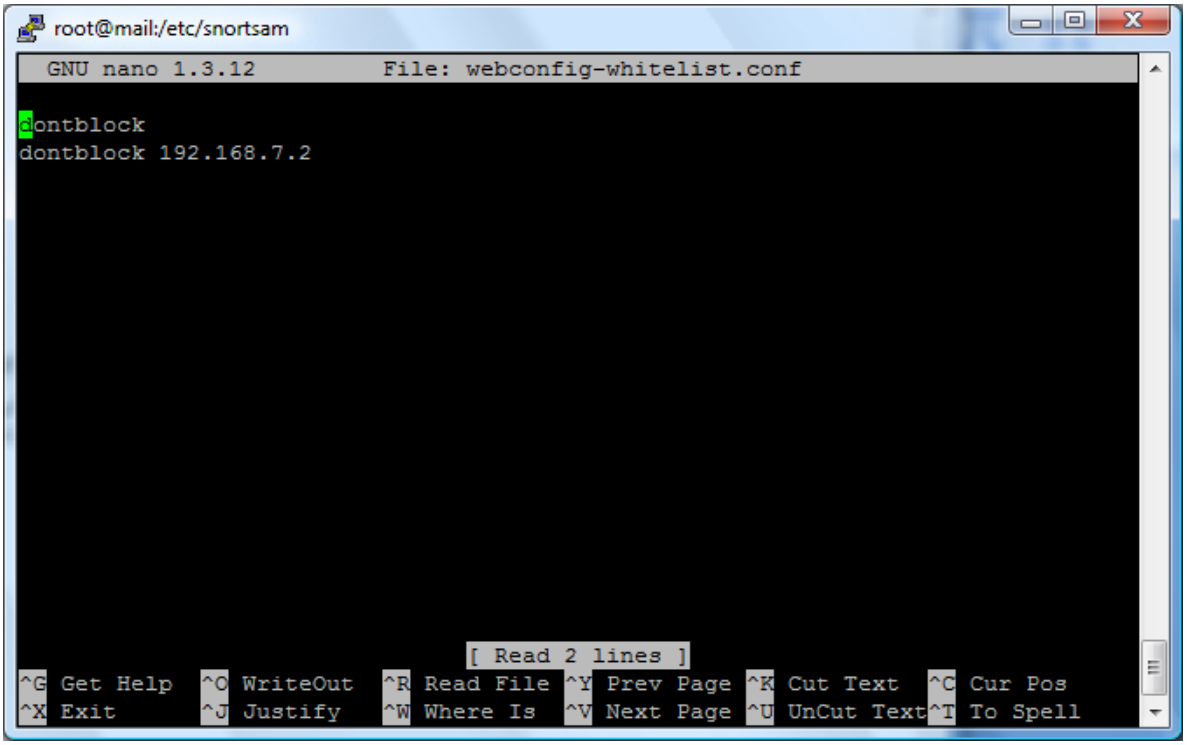


Figura 5.26 Sistemas no bloqueados de SnortSam

Una vez que todo está configurado correctamente se puede ejecutar SnortSam mediante:

/usr/local/bin/snortsam /etc/snortsam.conf &

5.6 IMPLEMENTACIÓN DE LA SOLUCIÓN CONTROLADOR ANCHO DE BANDA

Esta configuración se la hará netamente en modo gráfico a través del navegador, ingresando a https://192.168.7.24, ya que allí se tiene la herramienta completa de CBQ y sobre todo que para el usuario común es muy fácil de entender y utilizar.

5.6.1 Configuración del ancho de banda global de la DNM

Hay que dirigirse a Network, Bandwidth (ver Figura 5.27) y poner el ancho de banda global que tiene contratada la institución quel es 3E1, es decir 6144/6144kbps, y luego pulsar Update para grabar la modificación.

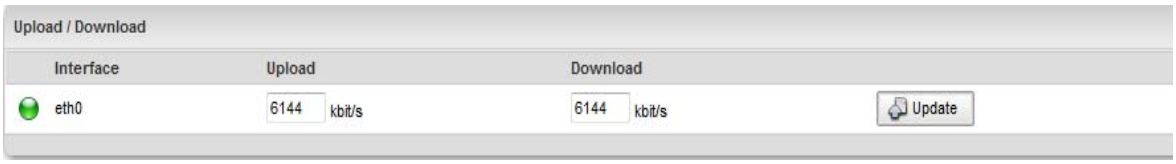


Figura 5.27 Configuración del ancho de banda global

5.6.2 Configuración de reglas globales de Bandwidth Controler

Ya que en la implementación de la solución de Filtro de contenidos fue bloquedo prácticamente todo, solo queda controlar el ancho de banda en el tamaño de los paquetes de entrada y salida en lo que a correo electrónico se refiere; para esto la institución decidió poner un máximo de 1024kbps para el protocolo de recepción de mail pop3 (ver. Figura 5.28), y 1024kbps para el protocolo de envío de mail SMTP (ver Figura 5.29). Este ancho de banda es para todas las sucursales a nivel nacional, ya que se considera que el correo electrónico en un porcentaje mayor a 90% es dirigido dentro de la institución por lo que no necesita para su flujo salir al internet.

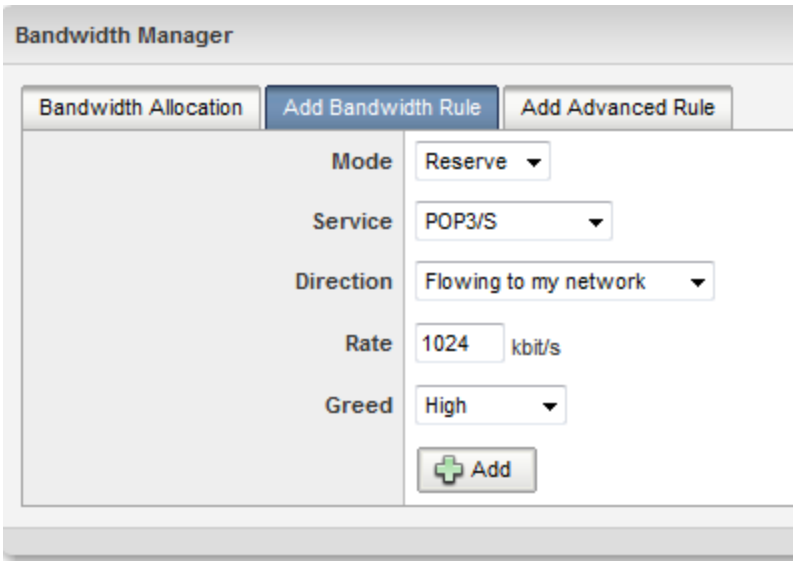


Figura 5.28 Configuración de regla para POP3 en BW.

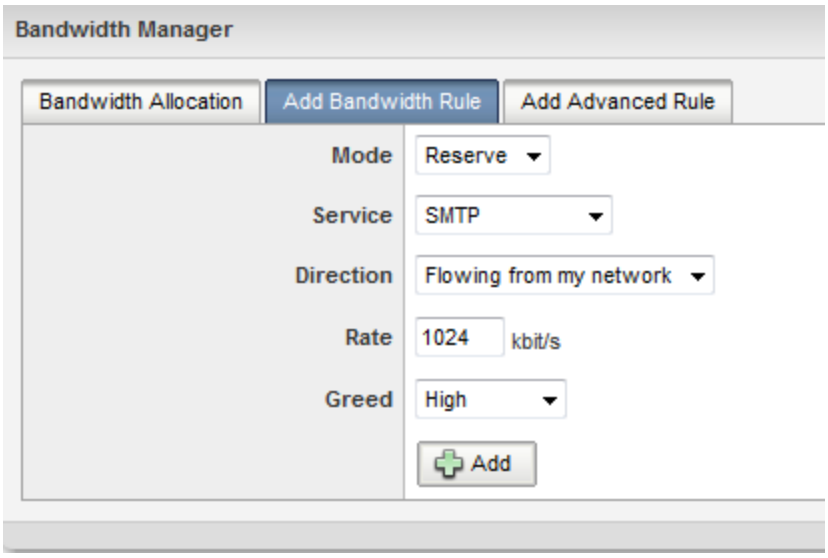


Figura 5.29 Configuración de regla para SMTP en BW

5.6.3 Configuración de reglas avanzadas para Bandwidth Controler

Se decidió controlar el ancho de banda de cada uno de los usuarios de internet a nivel nacional a 128/128kbps sin excepción, esto quiere decir que nadie podrá usar más de 128/128kbps cuando este navegando por WWW.

Esta configuración se la hizo en el tab que dice Add Advanced Rule, definiendo un Nickname general “Nacional”, introduciendo toda la subred de

origen utilizada en la DIRECCIÓN NACIONAL DE MIGRACIÓN a nivel nacional, la cual es 192.168.0.0/16, con esto se configura una sola vez la regla general de Internet definida.

Se escogió el puerto de destino el cual es 80, luego en direction esgemos download, que es el ancho de banda que interesa controlar, y por último se definió el Rate y el Ceiling en 128kbps cada una (ver Figura 5.30).

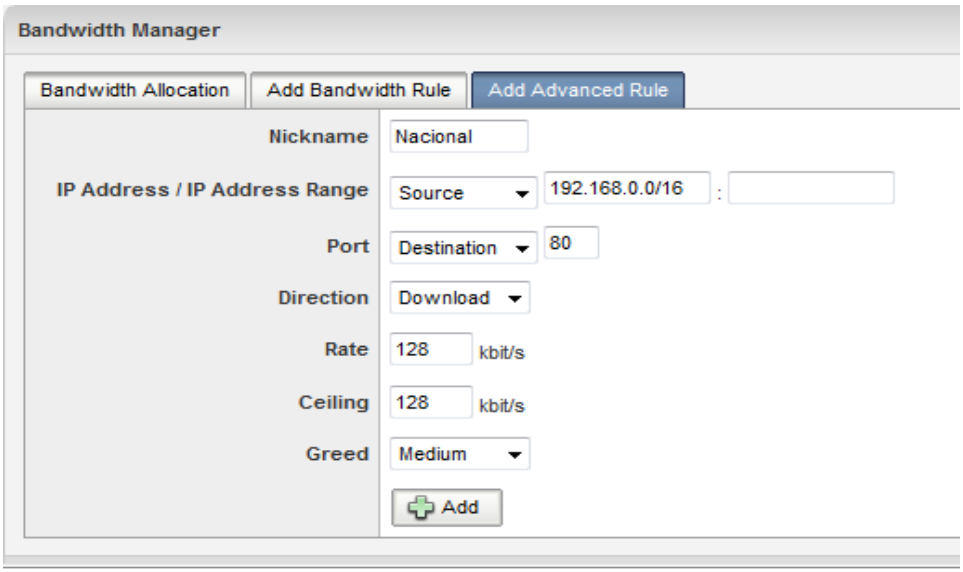


Figura 5.30 Configuración de regla de Control de BW para Internet

Ahora ya se tiene lista la configuración de control de ancho de banda, definiendo los parámetros que pide la institución.

Para revisar que todo quedo bien hay que ir a Bandwidth Allocation y verificar los parámetros ingresados (ver Figura 5.31)

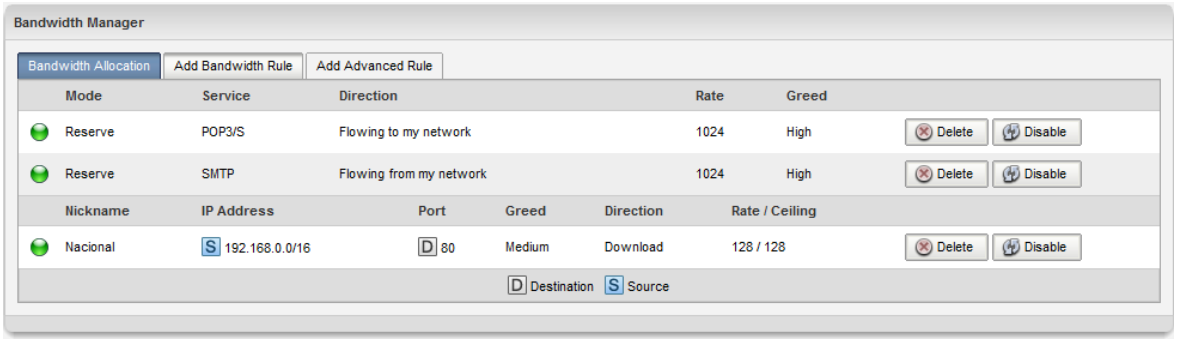


Figura 5.31 Resultado de la configuración de BW

5.7 PLAN DE PRUEBAS

5.7.1 Introducción

Este documento contiene las especificaciones para cumplir las pruebas de funcionalidad y manejo de las herramientas configuradas bajo Linux.

5.7.1.1 Objetivos y Alcance

Las Especificaciones de Prueba de la administración y optimización de los recursos para el proyecto verificaran que la funcionalidad de cada configuración satisfaga los requerimientos de la DIRECCIÓN NACIONAL DE MIGRACIÓN.

5.7.1.2 Estrategia

El encargado de realizar las pruebas preparará las especificaciones y ejecutará las pruebas. La especificación de requerimientos será la base para iniciar la evaluación de cada módulo configurado, combinando con el escenario lógico que corresponde a la secuencia de los procesos requeridos.

5.7.1.3 Organización del Documento

Este documento define el plan para conducir las pruebas de acuerdo con las especificaciones de la Prueba en las áreas siguientes:

- Objetivos: identifica las categorías de las pruebas que van a ser incluidas o excluidas desde la Especificación de Prueba.
- Cronograma de Pruebas: una lista de tareas y actividades de alto nivel indicando las fechas de inicio y terminación.
- Las responsabilidades: identifica los recursos disponibles y sus responsabilidades.
- Los recursos: identifica los recursos y los requisitos de software y hardware.
- Los procedimientos: describe los procedimientos a seguir en la preparación, desarrollo y verificación de los resultados de la prueba.

- Supuestos: documenta los supuestos hechos en la preparación de la especificación de la prueba.
- Los apéndices: contienen una secuencia de los escenarios de prueba, y una muestra de los documentos que resultan de las pruebas definidas.

5.7.2 Definición general de las pruebas

Las especificaciones para las pruebas de administración y optimización proveerán una metodología formal para las pruebas de cada configuración. Al identificar los tipos de prueba necesarios para esta aplicación, colocando un X en Si o No, si se va a ejecutar o no ese Tipo de prueba (esto si el Tipo de prueba aplica para el proyecto), o N.A. si la prueba no aplica para el proyecto.

Probar			Tipo de prueba	Descripción del Prueba	Duración
Si	No	NA			
X			Procesos e Interfase de Usuario	Procesamiento Lógico en el servidor: actualización de la configuración, modificaciones y que las configuraciones satisfagan lo descrito en el documento de especificaciones funcionales.	
X			Interfase con otras redes.	Respuesta a peticiones de páginas web por las redes remotas	
X			Volúmen	Simulación de volúmenes para peticiones de páginas web esperados en ambiente de producción.	
X			Concurrencia	Usuarios simultáneos accediendo a Internet.	
	X		Recuperación	Procedimientos de Backup y recuperación de la configuración.	
X			Seguridad	Especificaciones de Seguridad de acuerdo con las especificaciones	

				requeridas.	
	X		Documentación	Concordancia de la documentación, con respecto a la configuración.	
		X	Procedimientos Administrativos	Pruebas de Formas y procedimientos requeridos en el ambiente de producción.	

Tabla 5.1 Tipos de pruebas

5.7.3 Recursos

La siguiente sección define los recursos necesarios, personas, hardware o software.

5.7.3.1 Miembros y responsabilidades del equipo de pruebas

El equipo de pruebas es el siguiente:

Nombre	Tipo de prueba	Responsabilidad
Patricio Esteban Avila	Procesos e Interfase de Usuario	Hacer uso del Internet, probando así todas las funciones del servidor.
Patricio Esteban Avila	Interfase con otras redes.	Hacer uso del Internet en puntos remotos, probando así todas las funciones del servidor con redes remotas.
Patricio Esteban Avila	Volúmen	Acceder al Internet de todas las máquinas posibles a nivel nacional para probar el rendimiento de cada módulo de configuración.
Patricio Esteban Avila	Concurrencia	Acceder al Internet, desde varios equipos terminales con el fin de verificar que no se bloqueen las configuraciones.
Patricio Esteban Avila	Seguridad	Verificar que todas las funciones de seguridad impuestas en la fase

Nombre	Tipo de prueba	Responsabilidad
		de implantación se cumplan a cabalidad para los usuarios.

Tabla 5.2 Personal de pruebas y responsabilidades

5.7.3.2 Requerimientos de Recursos

El hardware y el software requerido es el siguiente:

Tipo de prueba	Cantidad	Nombre del Recurso
Procesos e Interfase de Usuario	1	PC Pentium Core 2 Duo → 1Gb RAM
	1	Windows XP Internet Explorer 9.x o superior Firefox 3.5
Interfase con otras redes.	1	PC Pentium Core 2 Duo → 1Gb RAM
	1	Windows XP Internet Explorer 9.x o superior Firefox 3.5
Volúmen	34	PC Pentium Core 2 Duo → 1Gb RAM
	34	Windows XP Internet Explorer 9.x o superior Firefox 3.5
Concurrencia	34	PC Pentium Core 2 Duo → 1Gb RAM
	34	Windows XP Internet Explorer 9.x o superior Firefox 3.5
Seguridad	1	PC Pentium Core 2 Duo → 1Gb RAM
	1	Windows XP Internet Explorer 9.x o superior Firefox 3.5

Tabla 5.3 Requerimientos de recursos

5.7.4 Procedimiento para escenarios de prueba

El siguiente es el procedimiento para la preparación de la ejecución de los escenarios de las pruebas:

5.7.4.1 Preparación de la Prueba

Múltiples casos deben ser preparados, uno por cada proceso definido en las especificaciones funcionales.

Los casos serán combinados en los escenarios. A cada escenario corresponde:

- Una o más tareas dentro del proceso.
- Secuencias Lógicas que pueden ser repetidas.
- Excepciones del proceso.

5.7.4.2 Ambiente de prueba

Para las pruebas al servidor se lo colocará en paralelo al esquema actual de la red WAN, pondiendo como dirección IP de la WAN la dirección 200.110.232.234/48 y como dirección IP de la LAN la 192.168.7.24. A las maquinas que se usarán para las pruebas se les configurará el proxy en el navegador, poniendo la dirección LAN del servidor y como puerto el 8080.

5.7.4.3 Ejecución y evaluación de las pruebas

Los escenarios de prueba serán efectuados en la secuencia enumerados en el Apéndice A.

El encargado de ejecutar un escenario de prueba, evaluará y escribirá los resultados de la prueba. La documentación de apoyo (pantallas e informes) debe conservarse para cada corrida de prueba, al igual que los registros de las pruebas efectuadas y de los problemas encontrados. Una copia del formato para el Registro y Control de estas fallas se encuentra en el Apéndice C.

Las fallas presentadas deberán ser archivadas en el Fólder del Proyecto e informadas en la reunión de control semanal con el personal de la DIRECCIÓN NACIONAL DE MIGRACIÓN.

Cada falla debe calificarse de acuerdo con su gravedad y determinar si afecta la secuencia de las pruebas programadas, de acuerdo con la siguiente tabla:

Gravedad	Descripción
1	Error grave que causa la suspensión del trabajo, es un error crítico y su solución debe ser de inmediata.
2	Error medio, es posible continuar con otras pruebas, pero el error corresponde a una funcionalidad esencial. La solución a estas situaciones debe tener prioridad alta.
3	Errores leves de presentación que no afectan la operación de la aplicación.

Tabla 5.4 Descripción de la gravedad de los errores

Cuando la falla se soluciona la prueba debe volverse a correr y todos los escenarios relacionados.

5.7.4.4 Supuestos

El Cronograma de pruebas está basado en los siguientes supuestos:

- El ambiente para la prueba va a estar disponible en la fecha de inicio de acuerdo con el cronograma de pruebas.
- La conexión a Internet estará disponible y será probada.
- Los documentos de referencia fueron la base para la elaboración de los casos de prueba y estarán disponibles durante la prueba.

Todos los escenarios tendrán un mecanismo de aprobación que asegure que el caso a probar cumple con los requerimientos, y de no ser así serán modificados hasta que cumplan con los requisitos.

5.7.5 Criterios de aceptación

El proyecto será aceptado cuando todas las pruebas especificadas en el Apéndice B sean ejecutadas satisfactoriamente y:

a. Los Resultados esperados estén de acuerdo con las especificaciones funcionales.
b. Todos los problemas hayan sido corregidos y los escenarios asociados a estas fallas se hayan ejecutado satisfactoriamente.

5.7.6 Apéndices

5.7.6.1 Apéndice A: Secuencia de ejecución de los escenarios

Orden / Sec	Escr No.	Nombre Escenario	Escenarios Previos Requeridos
1	1	Ingreso de usuarios	
2	2	Permisos de navegación.	Ingreso de Usuarios
3	3	Intento de ingreso al servidor por puertos.	Ingreso de Usuarios
4	4	Intento de ataques externos.	
5	5	Pruebas de ancho de banda.	Ingreso de Usuarios

Tabla 5.5 Secuencia de ejecución de escenarios

5.7.6.2 Apéndice B: Escenarios de prueba

Escenario de Prueba		
Proyecto:	Administración y Optimización del Internet en la DIRECCIÓN NACIONAL DE MIGRACIÓN	
Escenario:	**Ingreso de usuarios.**	**No. 1**
Módulo:	Proxy Server	
Caso de prueba:	Ingreso usuario a Internet.	
Tipo de prueba:	Interfase con otras redes	**Pág.** 1
Definido por:	Patricio Esteban Avila	**Fecha Creación:** 2009-10-01
Participantes:	Patricio Esteban Avila	
Descripción de la prueba:	Ingreso al Internet con un usuario previamente definido.	

Tabla 5.6 Escenario ingreso de usuarios

Escenario de Prueba		
Proyecto:	Administración y Optimización del Internet en la DIRECCIÓN NACIONAL DE MIGRACIÓN	
Escenario:	**Permisos de navegación.**	**No. 2**
Módulo:	Filtro de Contenidos (Dansguardian)	

Caso de prueba:	Ingreso a páginas web no permitidas	
Tipo de prueba:	Procesos e interfase de usuario	**Pág. 1**
Definido por:	Patricio Esteban Avila	**Fecha Creación:** 2009-10-01
Participantes:	Subte. Ing. Luis Martínez	
Descripción de la prueba:	Ingreso a páginas Web previamente autorizadas.	

Tabla 5.7 Escenario permisos de navegación

Escenario de Prueba		
Proyecto:	Administración y Optimización del Internet en la DIRECCIÓN NACIONAL DE MIGRACIÓN	
Escenario:	**Intento de ingreso al servidor por puertos.**	**No. 3**
Módulo:	Firewall	
Caso de prueba:	Intento de ataque exterior hacia el servidor por puerto	
Tipo de prueba:	Seguridad	**Pág. 1**
Definido por:	Patricio Esteban Avila	**Fecha Creación:** 2009-10-10
Participantes:	Subte. Ing. Luis Martínez	
Descripción de la prueba:	Intento de ingreso al servidor utilizando puertos bloqueados por IPTABLES.	

Tabla 5.8 Escenario intento de ingreso al servidor por puertos

Escenario de Prueba		
Proyecto:	Administración y Optimización del Internet en la DIRECCIÓN NACIONAL DE MIGRACIÓN	
Escenario:	**Intento de ataques externos.**	**No. 4**
Módulo:	Sistema de identificación de Intrusos (Snort)	

Caso de prueba:	Mandar comandos externos al servidor para quw los tome como ataques.	
Tipo de prueba:	Concurrencia	**Pág. 1**
Definido por:	Patricio Esteban Avila	**Fecha Creación:** 2009-10-20
Participantes:	Patricio Esteban Avila Subte. Ing. Luis Martínez	
Descripción de la prueba:	Atacar a puertos de Bases de Datos y aplicaciones propias de la DIRECCIÓN NACIONAL DE MIGRACIÓN desde el Internet.	

Tabla 5.9 Escenario intento de ataques externos

Escenario de Prueba		
Proyecto:	Administración y Optimización del Internet en la DIRECCIÓN NACIONAL DE MIGRACIÓN	
Escenario:	**Pruebas de ancho de banda.**	**No. 5**
Módulo:	Control ancho de banda (CBQ)	
Caso de prueba:	Ingresar a 25 páginas web de forma consecutiva para examinar el comportamiento del ancho de banda.	
Tipo de prueba:	Volumen	**Pág. 1**
Definido por:	Patricio Esteban Avila	**Fecha Creación:** 2009-11-01
Participantes:	Patricio Esteban Avila Subte. Ing. Luis Martínez	
Descripción de la prueba:	Ingresar a múltiples páginas web de forma simultánea para ver el comportamiento del ancho de banda y comprobar que se están controlando.	

Tabla 5.10 Escenario pruebas de ancho de banda

5.7.6.3 Apéndice C: Resumen de la ejecución de las pruebas

No.	Escr	Usuarios	Resultado	Fecha	Grav
1	1	Patricio Avila	La prueba de ingreso de usuarios registrados, brindó resultados satisfactorios en cuanto a validación y registro de usuarios en redes remotas.	2006-10-03	Ninguna
2	2	Patricio Esteban Avila	La prueba de validación de las páginas web fue satisfactoria ya que las páginas no permitidas no se abrieron, y las páginas permitidas si abrieron.	2009-10-14	Ninguna
3	3	Patricio Esteban Avila	La prueba de ataques por puertos desde el exterior fue satisfactoria ya que se observó que todos los puertos se encuentran cerrados excepto el 22 que pertenece al de SSH el cual está abierto por cuestiones de validación.	2009-10-16	Ninguna
4	4	Patricio Esteban Avila	Al utilizar programas que hagan flush de puertos críticos de aplicaciones como bases de datos, y al tratar de acceder al sistema Web internos por medio del puerto 2232 el servidor mostró un gráfico de intento de ataques el cual dice que el servicio Snort está funcionando adecuadamente y sin problemas el rato de identificar intrusos.	2009-10-25	Ninguna

5	5	Patricio Esteban Avila	Esta prueba resultó satisfactoria ya que el ancho de banda nunca subió de 128/128kbps, se abrieron múltiples paginas haciendo descargas de imágenes validas para el sistema, lo que dio como resultado la multiplexación de la velocidad de descarga, sumado siempre el ancho de banda asignado.	2009-11-04	Ninguna

Tabla 5.11 Resumen de ejecución de las pruebas

5.7.6.4 Apéndice D: Muestra gráfica de los escenarios de pruebas

Escenario 1

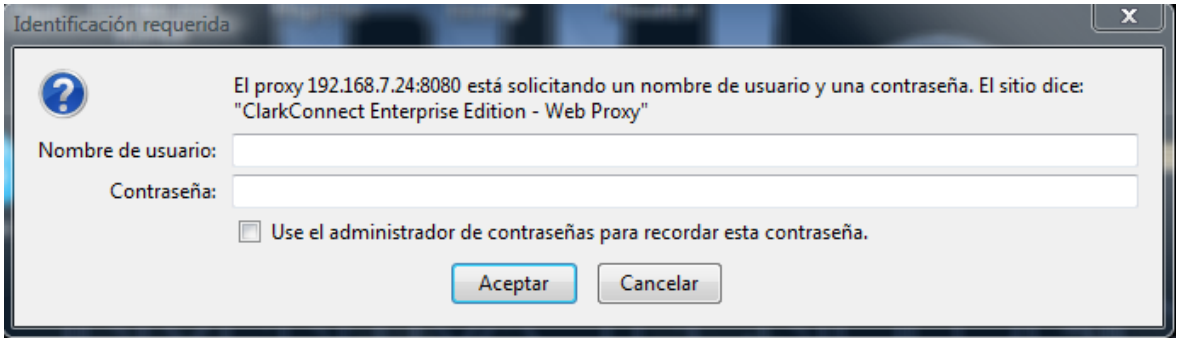


Figura 5.32 Ingreso de un usuario definido

Figura 5.33 Ingreso al Internet después de autentificarse

Escenario 2

Figura 5.34 Bloqueo de páginas no permitidas

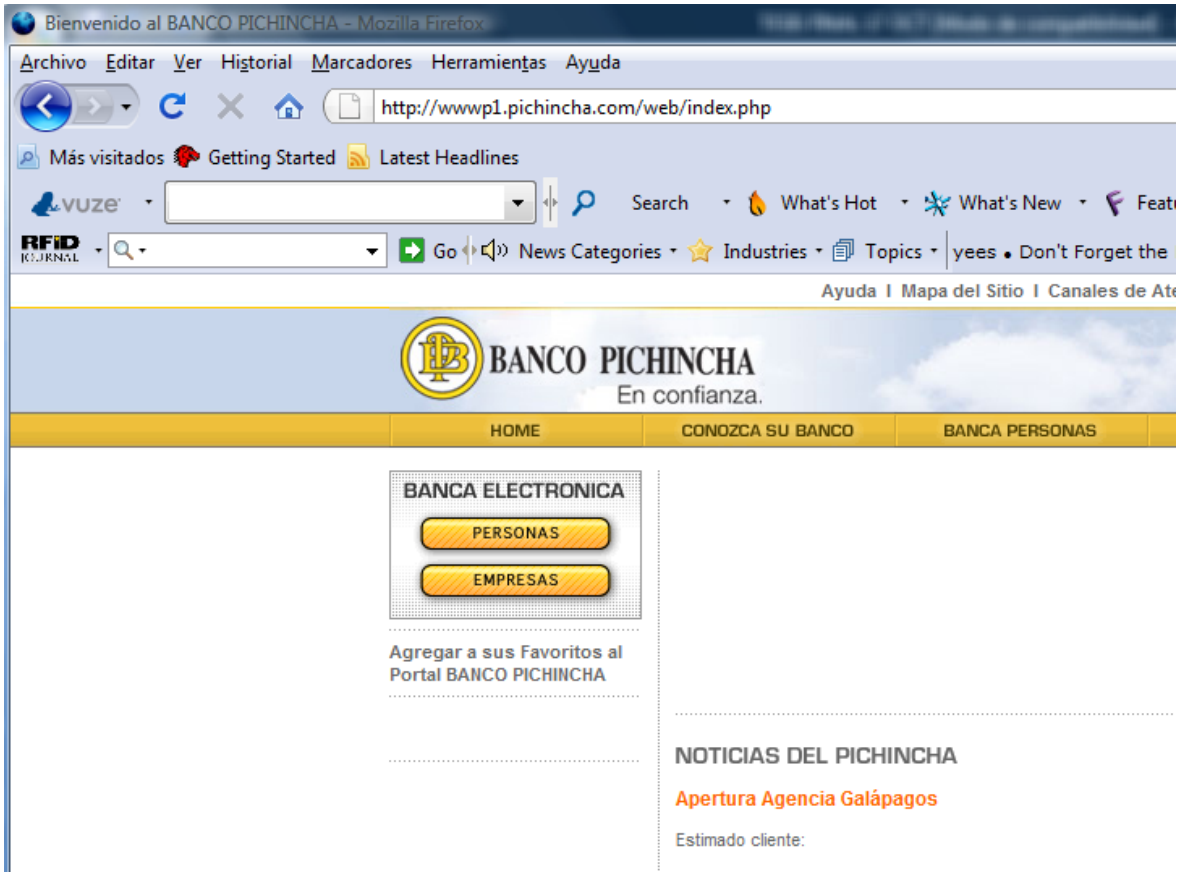


Figura 5.35 Permiso a páginas permitidas

Escenario 3

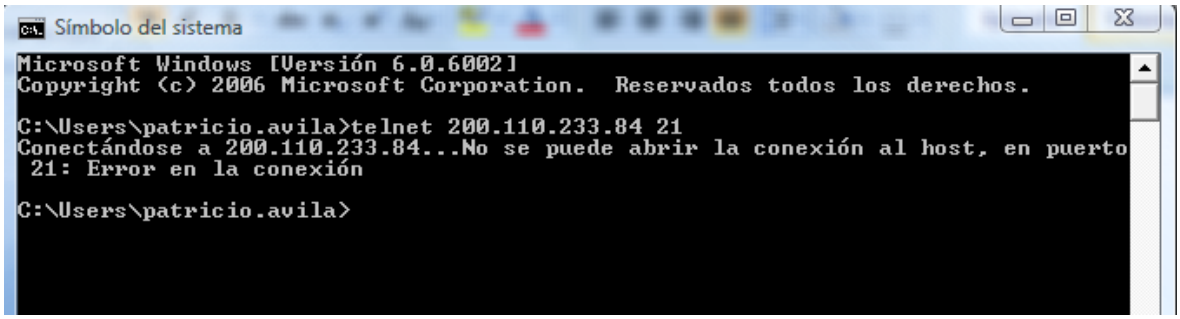


Figura 5.36 Intento de ingreso al servidor por el puerto 21 FTP

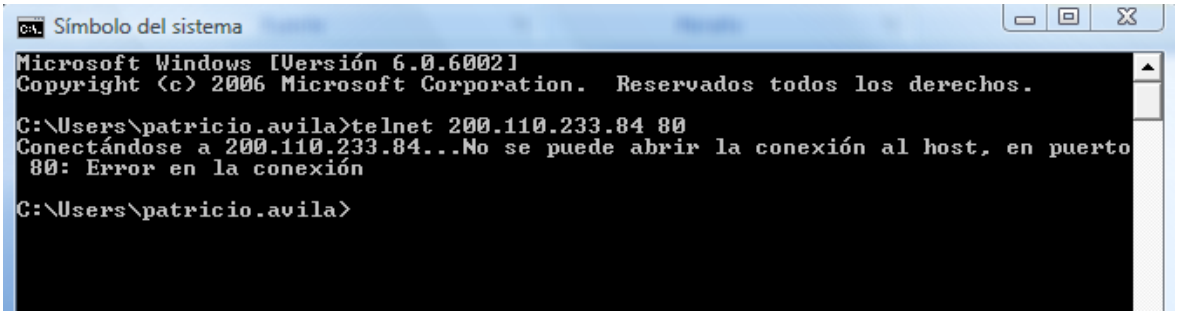


Figura 5.37 Intento de ingreso al servidor por el puerto 80 HTTP

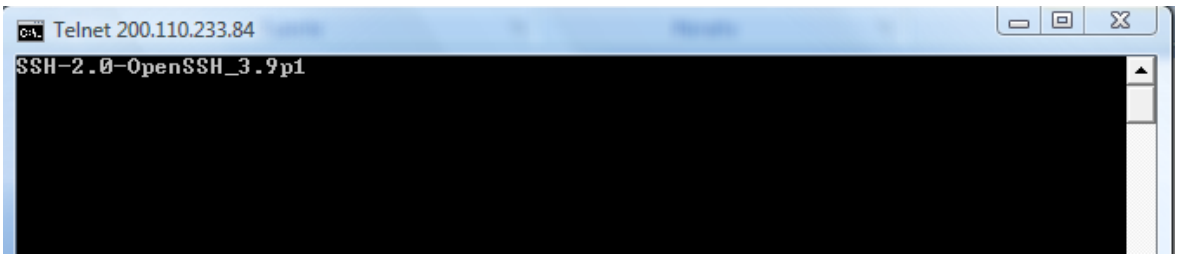


Figura 5.38 Ingreso al servidor por el puerto 22 SSH

Escenario 4

Misc Attack			
ID	Alerts	Hits	Date
2003	MS-SQL Worm propagation attempt	69	1 2 3 4 5 6 7
A Network Trojan Was Detected			
ID	Alerts	Hits	Date
2182	BACKDOOR typot trojan traffic	45	1 2 3
Attempted User Privilege Gain			
ID	Alerts	Hits	Date
1841	WEB-CLIENT Javascript URL host spoofing attempt	28	2 5 6
3192	WEB-CLIENT Windows Media Player directory traversal via Content-Disposition attempt	1	3
Attempted Information Leak			
ID	Alerts	Hits	Date
1201	ATTACK-RESPONSES 403 Forbidden	12	1 2 3 4 6

Figura 5.39 Ataques detectados por el IDS

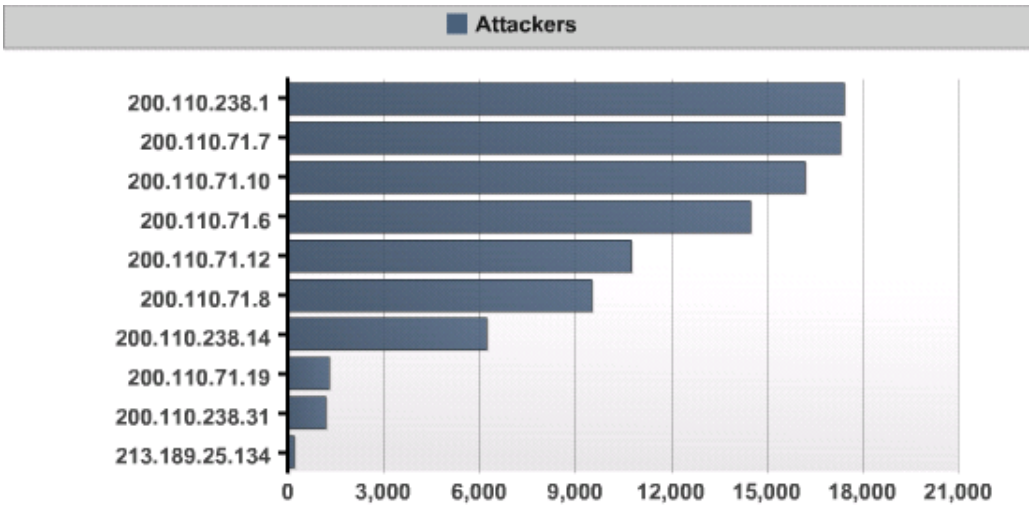


Figura 5.40 Direcciones IP de los Intrusos que intentaron atacar

Escenario 5

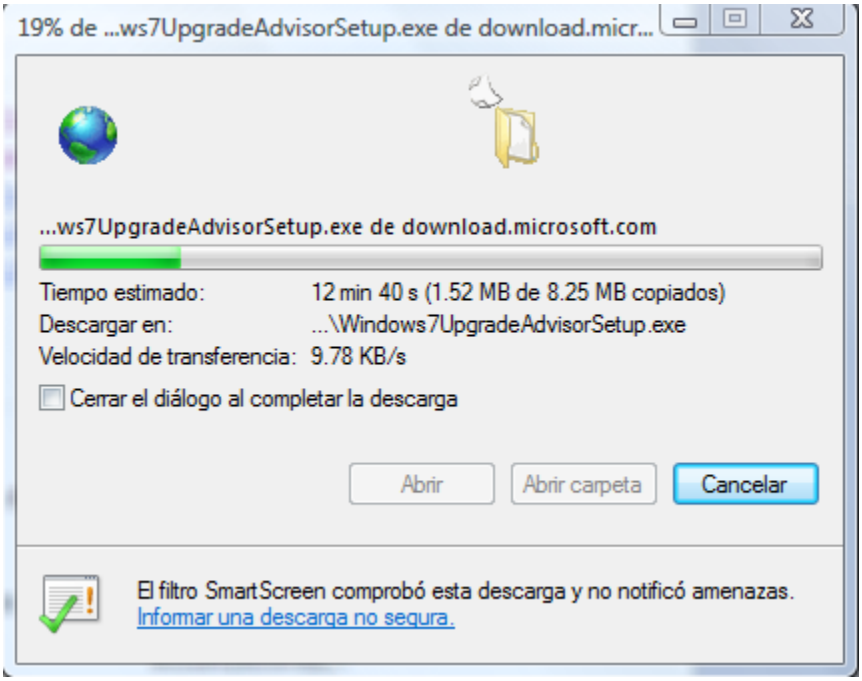


Figura 5.41 Ancho de banda primera descarga

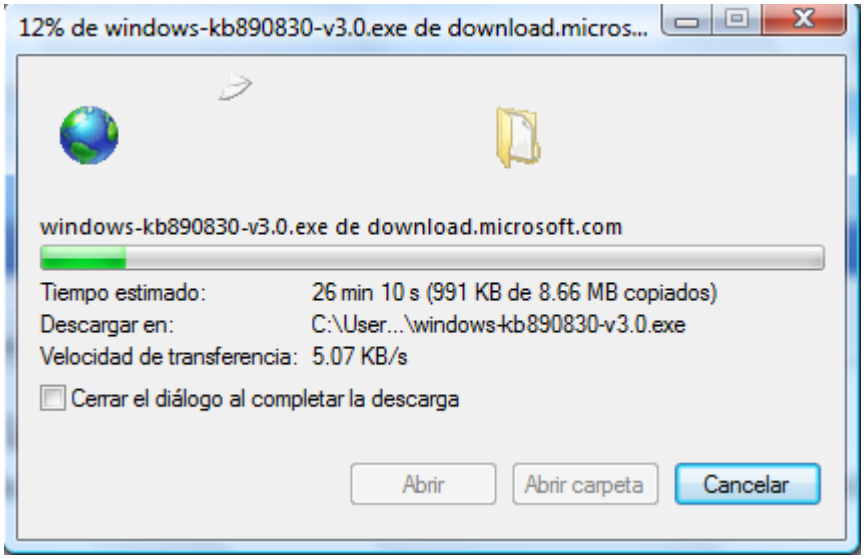


Figura 5.42 Ancho de banda segunda descarga

5.7.6.5 Apéndice E: Resultados de las Pruebas

Escenario 1

Requisitos		
Procedimiento	**Descripción**	**ok**

Pruebas Previas Requeridas:	Ninguna	Ok
Requisitos Funcionales:	Usuarios: personal registrado en el servidor.	Ok
Ambiente Técnico Previo Requerido:	PC Pentium Core 2 Duo → 1Gb RAM Windows XP Internet Explorer 9.x o superior Firefox 3.5	Ok

Comentarios: Las pruebas serán realizadas desde un computador con el navegador Firefox 3.5.
La máquina de pruebas estará conectada a la red y configurada en el mismo dominio/grupo de trabajo que el servidor. Desde el explorador WEB, el equipo de pruebas usará la dirección IP 192.168.7.24 con puerto 8080 como Proxy.

Secuencia de la Prueba

Procedimientos	Resultados Esperados	ok
Ingresar al Internet agregando usuario y contraseña.	Ingresar a página principal www.migracion.gov.ec.	Ok
Fallas Encontradas	**Descripción**	**Gravedad**

Comentarios de la prueba :

La prueba de ingreso de un usuario registrado, brindo resultados satisfactorios en cuanto a validación y registro del navegador.

Nombre Ejecutor de la Prueba:

Patricio Esteban Avila

Firma Ejecutor de la Prueba

Tabla 5.12 Resultados del Escenario 1

Escenario 2

Requisitos		
Procedimiento	**Descripción**	**ok**
Pruebas Previas Requeridas:	Ingreso de usuarios	Ok
Requisitos Funcionales:	Usuarios: personal registrado en el servidor.	Ok
Ambiente Técnico Previo Requerido:	PC Pentium Core 2 Duo → 1Gb RAM Windows XP Internet Explorer 9.x o superior Firefox 3.5	Ok
Comentarios: Las pruebas serán realizadas desde un computador con el navegador para intranet Firefox 3.5.		

Secuencia de la Prueba		
Procedimientos	**Resultados Esperados**	**ok**
Ingresar al Internet como usuario registrado.	Ingresar con los permisos y verificar que se abra el navegador.	Ok
Ingresar a páginas no deseadas.	Abrir página de error, el cual diga que no tienen permisos para navegar en ese tipo de página.	Ok
Ingresar a páginas deseadas.	Abrir la página web deseada.	Ok
Descargar archivos no permitidos.	Abrir página de error, el cual diga que no tienen permisos para descargar ese tipo de archivos.	Ok
Fallas Encontradas	**Descripción**	**Gravedad**
Comentarios de la prueba :		

La prueba demostró que el filtro de contenidos funciona satisfactoriamente y que los mensajes de error son los adecuados según la ocasión.
Nombre Ejecutor de la Prueba: Patricio Esteban Avila **Firma Ejecutor de la Prueba**

Tabla 5.13 Resultados del Escenario 2

Escenario 3

Requisitos		
Procedimiento	**Descripción**	**ok**
Pruebas Previas Requeridas:	Ninguna	Ok
Requisitos Funcionales:	Usuarios: persona externa al servidor.	Ok
Ambiente Técnico Previo Requerido:	PC Pentium Core 2 Duo → 1Gb RAM Windows XP Firefox 3.5	Ok
Comentarios: Las pruebas serán realizadas desde un computador remoto que tratará de ingresar a través de puerto 21 y 80.		

Secuencia de la Prueba		
Procedimientos	**Resultados Esperados**	**ok**
Abrir un navegador y tratar de ingresar al servidor por ftp. ftp://200.110.233.84.	Rechazo del servidor a la conexión por el puerto 21.	Ok
Abrir el navegador y tratar de ingresar al servidor por la dirección http://200.110.233.84:8080 o http://200.110.233.84.	Rechazo del servidor a la conexión por el puerto 8080.	Ok
Fallas Encontradas	**Descripción**	**Gravedad**

Comentarios de la prueba :		
La prueba demostró que un usuario externo que trate de ingresar al servidor por algún puerto no autorizado por el firewall será rechazado de inmediato.		
Nombre Ejecutor de la Prueba: Patricio Esteban Avila **Firma Ejecutor de la Prueba**		

Tabla 5.14 Resultados del Escenario 3

Escenario 4

Requisitos		
Procedimiento	**Descripción**	**ok**
Pruebas Previas Requeridas:	Ninguna	Ok
Requisitos Funcionales:	Usuarios: personal externa al servidor, usuario frecuente del Internet.	Ok
Ambiente Técnico Previo Requerido:	PC Pentium Core 2 Duo → 1Gb RAM Windows XP Firefox 3.5	Ok
Comentarios: Las pruebas serán realizadas desde computadores remotos que representarán ataques de operación para el servidor.		
Secuencia de la Prueba		
Procedimientos	**Resultados Esperados**	**ok**
Ingreso a la pagina web http://www.t1shopper.com/tools/scan.php4, desde por lo menos 25 usuarios remotos.	Los resultados deben decir que los puertos están cerrados.	Ok
Ingresar a los reportes de IDS del servidor.	Debe marcar ataques provocados por flush de puertos	Ok

	críticos como de base de datos.	
Fallas Encontradas	**Descripción**	**Gravedad**
Comentarios de la prueba :		
La prueba demostró que el sistema IDS e IPS funciona exitosamente ya que los reportes muestran posibles ataques a puertos críticos del sistema.		
Nombre Ejecutor de la Prueba: Patricio Esteban Avila		**Firma Ejecutor de la Prueba**

Tabla 5.15 Resultados del Escenario 4

Escenario 5

Requisitos		
Procedimiento	**Descripción**	**ok**
Pruebas Previas Requeridas:	Ingreso de usuarios	Ok
Requisitos Funcionales:	Usuarios: personal registrado en el servidor	Ok
Ambiente Técnico Previo Requerido:	PC Pentium Core 2 Duo → 1Gb RAM Windows XP Internet Explorer 9.x o superior Firefox 3.5	Ok
Comentarios: La prueba se hará realizando múltiples descargas de páginas permitidas para esta prueba como Microsoft.com.		
Secuencia de la Prueba		
Procedimientos	**Resultados Esperados**	**ok**
Ingreso con usuario y contraseña al servidor.	Abrirá la página de inicio autorizada www.migracion.gov.ec.	Ok

Dirigirse a la página de descargas de actualizaciones de Microsoft, http://www.microsoft.com/downloads/Search.aspx?displaylang=es.	Abrirá la página ya que esta autorizada.	Ok
Descargar múltiples aplicaciones a la vez.	La suma de todas las descargas será máximo de 128/128kbps que es la velocidad máxima permitida por usuario registrado.	Ok
Fallas Encontradas	**Descripción**	**Gravedad**
Comentarios de la prueba :		
La prueba demostró que la suma total de todas las transferencias de descarga sumo como máximo 123kbps, por lo que la prueba fue exitosa.		
Nombre Ejecutor de la Prueba: Patricio Esteban Avila		**Firma Ejecutor de la Prueba**

Tabla 5.16 Resultados del Escenario 5

CAPÍTULO VI

6 CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

El objetivo general indica que se debe desarrollar un sistema de firewall perimetral asistido a cada realidad institucional, la configuración debe ser realizada de forma minuciosa aclarando las necesidades reales en el plan de pruebas.

6.1.1 Conclusiones generales

La teoría es punto de partida esencial para el desarrollo de la tesis, pero en el momento de la práctica no tiene validez universal, ya que se debe adaptar esa teoría al ambiente en el cual se esté trabajando.

El uso de un sistema operativo como Linux permite tener una extensa flexibilidad en las diferentes configuraciones ya que los paquetes utilizados pueden correr bajo cualquier versión de Kernel, esto universaliza la funcionalidad de las configuraciones en cualquier sistema Linux.

El uso de un sistema ya programado como ClarkConnect facilita la intervención del administrador de la red, mucho más, si este no tiene experiencia en sistemas Linux, sin embargo en el proceso inicial de configuración se dificultó el hecho de unificar los parámetros con el formato de reportes y configuración simple ya establecidos por ClarkConnect.

La configuración del sistema se lo hace por medio de web browser lo que mejora el rendimiento de la aplicación y minimiza los posibles errores en el procesamiento de nuevas configuraciones en el servidor.

6.1.2 Cumplimiento de objetivos

6.1.2.1 Integración

Todos los módulos configurados se integran entre sí para realizar un verdadero trabajo de seguridad perimetral, para esto se debió hacer una labor ordenada en la configuración, comenzando por el firewall, IDS y terminando en el IPS, creando así una dependencia entre paquetes para el correcto funcionamiento de las políticas de la institución.

6.1.2.2 Metodología de desarrollo

La metodología de especificación de requerimientos mostró ser una metodología útil y fácil de integrar en todo el proceso de desarrollo, la manera de pensar del personal sobre el uso de Internet abrió un abanico de opciones para entender la importancia de implementar la solución global.

6.1.2.3 Tecnologías utilizadas

ClarkConnect es una base de Linux robusta y eficaz para la administración de la seguridad del uso del Internet, posee una interfaz gráfica denominada web config, la cual permite al usuario Administrador de la red modificar y ampliar las configuraciones teniendo un control completo y genérico sobre el servidor.

6.2 RECOMENDACIONES

Realizar una investigación de campo detallada para saber la factibilidad en el uso de algunas tecnologías y requerimientos específicos del sistema de control.

Se debe recopilar una base de datos de los ataques recibidos y del uso del Internet en la institución para tener un reporte histórico, el cual servirá a futuro para analizar el comportamiento del usuario, y sobre todo tener el histórico de los ataques que han tratado de hacer y transformalos en tablas de prevención de intrusos.

Cuando se trabaja dentro de un sistema de alta seguridad se recomienda tomar en cuenta como están configurados los módulos, y la comunicación entre estos.

Para mejorar la usabilidad del sistema es necesario dar al usuario un navegador robusto como Firefox 3.5 y tener valores por defecto.

Trabajar siempre en base a los procesos estipulados por la DIRECCIÓN NACIONAL DE MIGRACIÓN, así se encaminará a una configuración estable y transparente.

Probar continuamente las comunicaciones en los puntos remotos de la red WAN para comprobar que siempre esté activo el enrutamiento hacia la matriz donde se encuentra la conexión global de Internet.

Utilizar los estándares descritos en este documento cuando se requiera modificar la configuración de los diferentes módulos instalados, ya que cada configuración tiene un proceso y un orden el cual une la estructura de cada módulo, solo así se podrá tener un sistema robusto y adecuado a la realidad de la DIRECCIÓN NACIONAL DE MIGRACIÓN.

BIBLIOGRAFÍA

Hernández, Roberto; Fernández, Carlos; Baptista, Pilar. Metodología de la Investigación. MEXICO. McGRAW-HILL. Octubre, 1994.

ARMSTRONG, Bruce; BROWN, Millard. Linux clustering. USA. SAMS; 1ra edición. Julio 25, 2002

DHANJANI, Nitesh. Hacking, the next generation. USA. O'Reilly;. Abril 12, 2009

JAMES RUMBAUGH, OMT Insights: Perspective on Modeling from the Journal of Object-Oriented Programming (SIGS Reference Library). 2003.

JON HOLT. UML for Systems Engineering: Watching the Wheels. Institution of Electrical Engineers. 2001.

BLUMHAS, Richard. Linux command lineand shell scripting, John Wiley & Sons, 2008.

BEALE'S, Jay. Snort IDS & IPS Toolkit. Syngress. 2007.

ALISTAIR, Croll. Complete Web Monitoring. O'Reilly. 2009.

WEBBIBLIOGRAFÍA

The Linux Home Page **Internet:** http://www.linux.org/ **Último Acceso:** 15/08/2009

Clarkconnect **Internet:** http://www.clarkconnect.com/ **Último Acceso:** 16/10/2009

IEEE **Internet:** http://www.ieee.org **Último Acceso:** 16/10/2009

Human-Computer Interaction Resourses **Internet:** http://www.hcibib.org **Último Acceso:** 16/10/2009

Squid **Internet:** http://www.squid-cache.org/ **Último Acceso:** 18/10/2009

Dansguardian **Internet:** http://www.dansguardian.org/ **Último Acceso:** 18/10/2009

Snort **Internet:** http://www.snort.org/ **Último Acceso:** 21/10/2009

CBQ (Class-Based Queueing) **Internet:** http://www.icir.org/floyd/**cbq**.html **Último Acceso:** 21/10/2009

ANEXO A

A. MANUAL DE INSTALACIÓN CLARKCONNECT ENTERPRISE 5.0

Para la instalación del sistema operativo ClarkConnect 5.0 es necesario los siguientes requisitos:

- Un equipo servidor con un CPU Dual-Core con 1 GB en RAM y 200Gb de Disco duro.
- Dos tarjetas de red 10/100.

Pasos para la instalación

Para empezar, hay que descargar la imagen ISO y quemarla en un disco en blanco. Luego, encender el equipo e introducir nuestro disco de instalación recién creado. Hay que modificar la secuencia de arranque en el BIOS, para dar prioridad a la unidad óptica sobre el disco duro. Si lo hicimos bien, veremos la pantalla de inicio del instalador de ClarkConnect.

Figura D.1 Ventana de inicio de instalación

Para continuar, debemos escribir la palabra “linux” y presionar la tecla Enter. En la siguiente ventana, debemos seleccionar el idioma que utilizaremos en el proceso de instalación.

Fig. E.1 Ventana verificación

Seleccionamos la opción “Spanish”, y presionamos la tecla “Enter”. Pasamos a seleccionar el idioma del teclado.

Fig. E.2 Ventana idioma S.O.

Seleccionamos “es” y presionamos la tecla “Enter”. En la siguiente ventana hay que elegir el medio de instalación.

Fig. E.3 Ventana idioma teclado

Seleccionamos “Local CDROM” y presionamos la tecla “Enter”. Ahora hay que elegir entre dos opciones: realizar una instalación limpia o una actualización.

Fig. E.4 Ventana selección origen de la instalación

Acabamos de armar una computadora que obviamente no tiene sistema operativo aún, así que seleccionamos la primera opción (“Install”). Aparece una ventana advirtiendo que estamos a punto de borrar el contenido de nuestro disco duro.

Fig. E.5 Ventana elección install o update

Para continuar, se debe escribir la palabra “ClarkConnect” y presionar el botón “OK”. Ahora, hay que seleccionar el modo de funcionamiento. ClarkConnect posee dos modos de funcionamiento: el modo “Gateway”, donde el sistema puede funcionar como un proxy o un firewall dentro de una LAN. Este modo requiere la instalación de dos tarjetas de red. El segundo modo es “Standalone”, en donde el sistema trabaja como un servidor dentro de la red local. Para este modo, se requiere únicamente una tarjeta de red. Usaremos el segundo modo en nuestra instalación.

Fig. E.6 Ventana modo de funcionamiento

Es hora de realizar la configuración TCP/IP de nuestro servidor. Primero, indicaremos al servidor que le asignaremos una dirección IP manualmente. Luego, agregaremos la dirección IP específica para el servidor.

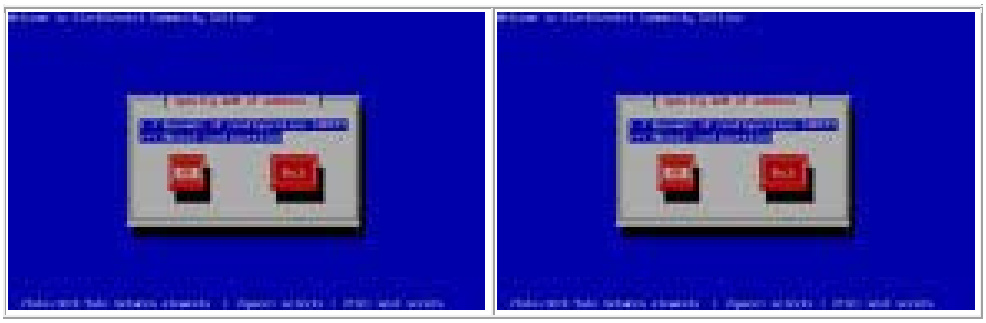


Fig. E.7 Ventana asignación dirección IP

El siguiente paso es asignar la contraseña de root. En lo personal, utilizo contraseñas de por lo menos ocho caracteres, que incluyan números y letras minúsculas y mayúsculas (en este ejemplo, utilizo una contraseña más sencilla, de siete caracteres). Presionen el botón “OK” para continuar.

Fig. E.8 Ventana asignar contraseña al root

Llegamos a la sección de las particiones del disco. Usaremos el esquema por defecto que para este caso es el apropiado.

Fig. E.9 Ventana particionamiento de discos

Ahora seleccionamos las aplicaciones a instalar. Para empezar, mi servidor proveerá direcciones IP a los equipos de la red y servicios básicos de almacenamiento de archivos. Así que debemos instalar los servicios DHCP,

Intrusion Detection and Prevention, DMZ and 1-to-1 NAT Firewall, Multi-WAN Support, Bandwidth Manager, Web Proxy Server, Content Filter Server, VPN – PPTP Server, Server Antivirus.

Fig. E.10 Ventana selección de aplicaciones

Para continuar agregando funciones, hay que presionar el botón “OK”. En la siguiente ventana, seleccionamos los módulos Mail – SMTP Server and Gateway, Mail – POP and IMAP Server, Mail – Antivirus Server, Mail – Antispam Server, Webmail, Flexshare file manager, Web Server, FTP Server, File server (Samba), Database Server.

Fig. E.11 Ventana agregar funciones

Al terminar de agregar módulos, presionamos el botón “Done”. Aparecerá otra ventana de advertencia, avisando que esa es nuestra última oportunidad de revisar nuestras opciones, antes de efectuar cambios en el sistema.

Fig. E.12 Ventana terminar agregar módulos

Al presionar el botón “Done”, el asistente de instalación prepara las particiones del disco y luego, inicia el proceso de instalación del sistema operativo. El tiempo que tome la instalación dependerá de las características del equipo y de la cantidad de módulos seleccionados para la instalación.

Fig. E.13 Ventana proceso instalación

Cuando finalice el proceso de instalación, es necesario retirar el disco de instalación y reiniciar el sistema. Al reiniciar, seremos recibidos por la pantalla de inicio de sesión del usuario Administrador.

Fig. E.14 Ventana ingreso Password

ANEXO B

B. LISTA DE PUERTOS MÁS USADOS

Oficial	Combinación Puerto/Aplicación que son registrados por la IANA
No Oficial	Combinación Puerto/Aplicación que no son registrados por la IANA
Conflicto	Puertos en uso por múltiples aplicaciones.

Puerto	Descripción	Estado
0/TCP,UDP	Reservado	Oficial
1/TCP,UDP	TCP Port Service Multiplexer	Oficial
2/TCP,UDP	Management Utility	Oficial
3/TCP,UDP	Compression Process	Oficial
5/TCP,UDP	Remote Job Entry	Oficial
7/TCP,UDP	Echo	Oficial
8/TCP,UDP	ICMP (Ping)	Oficial
9/TCP,UDP	Discard	Oficial
11/TCP,UDP	Active Users	Oficial
13/TCP,UDP	DAYTIME – (RFC 867)	Oficial
17/TCP,UDP	Quote of the Day	Oficial

18/TCP,UDP	Message Send Protocol	Oficial
19/TCP,UDP	Character Generator	Oficial
20/TCP	FTP – data	Oficial
21/TCP	FTP—control (command)	Oficial
22/TCP,UDP	Secure Shell (SSH)—used for secure logins, file transfers (scp, sftp) and port Forwarding	Oficial
23/TCP	Telnet protocol—unencrypted text communications	Oficial
25/TCP,UDP	Simple Mail Transfer Protocol (SMTP)—used for e-mail routing between mail servers	Oficial
34/TCP,UDP	Remote File (RF)—used to transfer files between machines	No Oficial
35/TCP,UDP	Any private printer server protocol	Oficial
35/TCP,UDP	QMS Magicolor 2 printer server protocol	No Oficial
37/TCP,UDP	TIME protocol	Oficial
39/TCP,UDP	Resource Location Protocol[2] (RLP)—used for determining the location of higher level services from hosts on a network	Oficial
41/TCP,UDP	Graphics	Oficial
42/TCP,UDP	nameserver, ARPA Host Name Server Protocol	Oficial
42/TCP,UDP	WINS	No Oficial
43/TCP	WHOIS protocol	Oficial

47/TCP	GRE protocol	Oficial
49/TCP,UDP	TACACS Login Host protocol	Oficial
52/TCP,UDP	XNS (Xerox Network Services) Time Protocol	Oficial
53/TCP,UDP	Domain Name System (DNS)	Oficial
54/TCP,UDP	XNS (Xerox Network Services) Clearinghouse	Oficial
55/TCP,UDP	ISI-GL (ISI Graphics Language)	No Oficial
56/TCP,UDP	XNS (Xerox Network Services) Authentication	Oficial
56/TCP,UDP	RAP (Route Access Protocol)[3]	No Oficial
57/TCP	MTP, Mail Transfer Protocol	No Oficial
58/TCP,UDP	XNS (Xerox Network Services) Mail	Oficial
67/UDP	Bootstrap Protocol (BOOTP) Server; also used by Dynamic Host Configuration Protocol (DHCP)	Oficial
68/UDP	Bootstrap Protocol (BOOTP) Client; also used by Dynamic Host Configuration Protocol (DHCP)	Oficial
69/UDP	Trivial File Transfer Protocol (TFTP)	Oficial
70/TCP	Gopher protocol	Oficial
79/TCP	Finger protocol	Oficial
80/TCP,UDP	Hypertext Transfer Protocol (HTTP)	Oficial

81/TCP	Torpark—Onion routing	No Oficial
82/UDP	Torpark—Control	No Oficial
83/TCP	MIT ML Device	Oficial
88/TCP,UDP	Kerberos—authentication system	Oficial
90/TCP,UDP	dnsix (DoD Network Security for Information Exchange) Securit Attribute Token Map	Oficial
90/TCP,UDP	Pointcast	No Oficial
99/TCP	WIP Message Protocol	No Oficial
101/TCP	NIC host name	Oficial
102/TCP	ISO-TSAP (Transport Service Access Point) Class 0 protocol[4]	Oficial
104/TCP,UDP	ACR/NEMA Digital Imaging and Communications in Medicine	Oficial
107/TCP	Remote TELNET Service[5] protocol	Oficial
109/TCP	Post Office Protocol 2 (POP2)	Oficial
110/TCP	Post Office Protocol 3 (POP3)	Oficial
111/TCP,UDP	Sun Remote Procedure Call	Oficial
113/UDP	ident—user identification system, used by IRC servers to identify users	Oficial
113/TCP,UDP	Authentication Service (auth)	Oficial

115/TCP	Simple File Transfer Protocol (SFTP)	Oficial
117/TCP	UUCP Path Service	Oficial
118/TCP,UDP	SQL (Structured Query Language) Services	Oficial
119/TCP	Network News Transfer Protocol (NNTP)—used for retrieving newsgroup messages	Oficial
123/UDP	Network Time Protocol (NTP)—used for time synchronization	Oficial
135/TCP,UDP	DCE endpoint resolution	Oficial
135/TCP,UDP	Microsoft EPMAP (End Point Mapper), also known as DCE/RPC Locator service[6], used to remotely manage services including DHCP server, DNS server and WINS. Also used by DCOM	No Oficial
137/TCP,UDP	NetBIOS NetBIOS Name Service	Oficial
138/TCP,UDP	NetBIOS NetBIOS Datagram Service	Oficial
139/TCP,UDP	NetBIOS NetBIOS Session Service	Oficial
143/TCP,UDP	Internet Message Access Protocol (IMAP)—used for retrieving, organizing, and synchronizing e-mail messages	Oficial
152/TCP,UDP	Background File Transfer Program (BFTP)[7]	Oficial
153/TCP,UDP	SGMP, Simple Gateway Monitoring Protocol	Oficial
156/TCP,UDP	SQL Service	Oficial
158/TCP,UDP	DMSP, Distributed Mail Service Protocol	No Oficial

161/TCP,UDP	Simple Network Management Protocol (SNMP)	Oficial
162/TCP,UDP	Simple Network Management Protocol Trap (SNMPTRAP)[8]	Oficial
170/TCP	Print-srv, Network PostScript	Oficial
177/TCP,UDP	X Display Manager Control Protocol (XDMCP)	Oficial
179/TCP	BGP (Border Gateway Protocol)	Oficial
194/TCP,UDP	IRC (Internet Relay Chat)	Oficial
199/TCP,UDP	SMUX, SNMP Unix Multiplexer	Oficial
201/TCP,UDP	AppleTalk Routing Maintenance	Oficial
209/TCP,UDP	The Quick Mail Transfer Protocol	Oficial
210/TCP,UDP	ANSI Z39.50	Oficial
213/TCP,UDP	IPX	Oficial
218/TCP,UDP	MPP, Message Posting Protocol	Oficial
220/TCP,UDP	IMAP, Interactive Mail Access Protocol, version 3	Oficial
256/TCP,UDP	2DEV "2SP" Port	No Oficial
259/TCP,UDP	ESRO, Efficient Short Remote Operations	Oficial
264/TCP,UDP	BGMP, Border Gateway Multicast Protocol	Oficial
311/TCP	Mac OS X Server Admin (Oficially AppleShare IP Web	Oficial

	administration)	
308/TCP	Novastor Online Backup	Oficial
318/TCP,UDP	PKIX TSP, Time Stamp Protocol	Oficial
323/TCP,UDP	IMMP, Internet Message Mapping Protocol	No Oficial
350/TCP,UDP	MATIP-Type A, Mapping of Airline Traffic over Internet Protocol	Oficial
351/TCP,UDP	MATIP-Type B, Mapping of Airline Traffic over Internet Protocol	Oficial
366/TCP,UDP	ODMR, On-Demand Mail Relay	Oficial
369/TCP,UDP	Rpc2portmap	Oficial
370/TCP,UDP	codaauth2 – Coda authentication server	No Oficial
370/TCP,UDP	securecast1 – Outgoing packets to NAI's servers, http://www.nai.com/asp_set/anti_virus/alerts/faq.as	No Oficial
371/TCP,UDP	ClearCase albd	Oficial
383/TCP,UDP	HP data alarm manager	Oficial
384/TCP,UDP	A Remote Network Server System	Oficial
387/TCP,UDP	AURP, AppleTalk Update-based Routing Protocol	Oficial
389/TCP,UDP	Lightweight Directory Access Protocol (LDAP)	Oficial
401/TCP,UDP	UPS Uninterruptible Power Supply	Oficial
402/TCP	Altiris, Altiris Deployment Client	No Oficial

411/TCP	Direct Connect Hub	No Oficial
412/TCP	Direct Connect Client-to-Client	No Oficial
427/TCP,UDP	Service Location Protocol (SLP)	Oficial
443/TCP,UDP	Hypertext Transfer Protocol over TLS/SSL (HTTPS)	Oficial
444/TCP,UDP	SNPP, Simple Network Paging Protocol (RFC 1568)	Oficial
445/TCP	Microsoft-DS Active Directory, Windows shares	Oficial
445/UDP	Microsoft-DS SMB file sharing	Oficial
464/TCP,UDP	Kerberos Change/Set password	Oficial
465/TCP	Cisco protocol	No Oficial
465/TCP	SMTP over SSL	No Oficial
475/TCP	tcpnethaspsrv (Hasp services, TCP/IP version)	Oficial
497/TCP	Dantz Retrospect	Oficial
500/UDP	Internet Security Association and Key Management Protocol (ISAKMP)	Oficial
501/TCP	STMF, Simple Transportation Management Framework – DOT NTCIP 1101	No Oficial
502/TCP,UDP	Modbus, Protocol	No Oficial
504/TCP,UDP	Citadel – multiservice protocol for dedicated clients for the Citadel groupware system	Oficial

510/TCP	First Class Protocol	No Oficial
512/TCP	Rexec, Remote Process Execution	Oficial
512/UDP	comsat, together with biff	Oficial
513/TCP	Login	Oficial
513/UDP	Who	Oficial
514/TCP	Shell—used to execute non-interactive commands on a remote system	Oficial
514/UDP	Syslog—used for system logging	Oficial
515/TCP	Line Printer Daemon—print service	Oficial
517/UDP	Talk	Oficial
518/UDP	NTalk	Oficial
520/TCP	efs, extended file name server	Oficial
520/UDP	Routing—RIP	Oficial
524/TCP,UDP	NCP (NetWare Core Protocol) is used for a variety things such as access to primary NetWare server resources, Time Synchronization, etc.	Oficial
525/UDP	Timed, Timeserver	Oficial
530/TCP,UDP	RPC	Oficial
531/TCP,UDP	AOL Instant Messenger, IRC	No Oficial

532/TCP	Netnews	Oficial
533/UDP	netwall, For Emergency Broadcasts	Oficial
540/TCP	UUCP (Unix-to-Unix Copy Protocol)	Oficial
542/TCP,UDP	commerce (Commerce Applications)	Oficial
543/TCP	klogin, Kerberos login	Oficial
544/TCP	kshell, Kerberos Remote shell	Oficial
545/TCP	OSIsoft PI (VMS), OSISoft PI Server Client Access	No Oficial
546/TCP,UDP	DHCPv6 client	Oficial
547/TCP,UDP	DHCPv6 server	Oficial
548/TCP	Apple Filing Protocol (AFP) over TCP	Oficial
550/UDP	new-rwho, new-who	Oficial
554/TCP,UDP	Real Time Streaming Protocol (RTSP)	Oficial
556/TCP	Remotefs, RFS, rfs_server	Oficial
560/UDP	rmonitor, Remote Monitor	Oficial
561/UDP	Monitor	Oficial
563/TCP,UDP	NNTP protocol over TLS/SSL (NNTPS)	Oficial
587/TCP	e-mail message submission[9] (SMTP)	Oficial

591/TCP	FileMaker 6.0 (and later) Web Sharing (HTTP Alternate, also see port 80)	Oficial
593/TCP,UDP	HTTP RPC Ep Map, Remote procedure call over Hypertext Transfer Protocol, often used by Distributed Component Object Model services and Microsoft Exchange Server	Oficial
604/TCP	TUNNEL profile[10], a protocol for BEEP peers to form an application layer tunnel	Oficial
623/UDP	ASF Remote Management and Control Protocol (ASF-RMCP)	Oficial
631/TCP,UDP	Internet Printing Protocol (IPP)	Oficial
636/TCP,UDP	Lightweight Directory Access Protocol over TLS/SSL (LDAPS)	Oficial
639/TCP,UDP	MSDP, Multicast Source Discovery Protocol	Oficial
641/TCP,UDP	SupportSoft Nexus Remote Command (control/listening): A proxy gateway connecting remote control traffic	Oficial
646/TCP,UDP	LDP, Label Distribution Protocol, a routing protocol used in MPLS networks	Oficial
647/TCP	DHCP Failover protocol[11]	Oficial
648/TCP	RRP (Registry Registrar Protocol)[12]	Oficial
652/TCP	DTCP, Dynamic Tunnel Configuration Protocol	No Oficial
653/TCP,UDP	SupportSoft Nexus Remote Command (data): A proxy gateway connecting remote control traffic	Oficial
654/TCP	AODV (Ad-hoc On-demand Distance Vector)	Oficial
655/TCP	IEEE MMS (IEEE Media Management System)[13][14]	Oficial

657/TCP,UDP	IBM RMC (Remote monitoring and Control) protocol, used by System p5 AIX Integrated Virtualization Manager (IVM)[15] and Hardware Management Console to connect managed logical partitions (LPAR) to enable dynamic partition reconfiguration	Oficial
660/TCP	Mac OS X Server administration	Oficial
665/TCP	sun-dr, Remote Dynamic Reconfiguration	No Oficial
666/UDP	Doom, first online first-person shooter	Oficial
674/TCP	ACAP (Application Configuration Access Protocol)	Oficial
691/TCP	MS Exchange Routing	Oficial
692/TCP	Hyperwave-ISP	Oficial
694/TCP,UDP	Linux-HA High availability Heartbeat	Oficial
695/TCP	IEEE-MMS-SSL (IEEE Media Management System over SSL)[16]	Oficial
698/UDP	OLSR (Optimized Link State Routing)	Oficial
699/TCP	Access Network	Oficial
700/TCP	EPP (Extensible Provisioning Protocol), a protocol for communication between domain name registries and registrars (RFC 4934)	Oficial
701/TCP	LMP (Link Management Protocol (Internet))[17], a protocol that runs between a pair of nodes and is used to manage traffic engineering (TE) links	Oficial
702/TCP	IRIS[18][19] (Internet Registry Information Service) over BEEP (Blocks Extensible Exchange Protocol)[20] (RFC 3983)	Oficial

706/TCP	SILC, Secure Internet Live Conferencing	Oficial
711/TCP	Cisco TDP, Tag Distribution Protocol[21][22][23]—being replaced by the MPLS Label Distribution Protocol[24]	Oficial
712/TCP	TBRPF, Topology Broadcast based on Reverse-Path Forwarding routing protocol (RFC 3684)	Oficial
712/UDP	Promise RAID Controller	No Oficial
720/TCP	SMQP, Simple Message Queue Protocol	No Oficial
749/TCP,UDP	Kerberos administration	Oficial
750/TCP	Rfile	Oficial
750/UDP	Loadav	Oficial
750/UDP	kerberos-iv, Kerberos version IV	Oficial
751/TCP,UDP	Pump	Oficial
751/TCP,UDP	kerberos_master, Kerberos authentication	No Oficial
752/TCP	Qrh	Oficial
752/UDP	Qrh	Oficial
752/UDP	userreg_server, Kerberos Password (kpasswd) server	No Oficial
753/TCP	Reverse Routing Header (rrh)[25]	Oficial
753/UDP	Reverse Routing Header (rrh)	Oficial

753/UDP	passwd_server, Kerberos userreg server	No Oficial
754/TCP	tell send	Oficial
754/TCP	krb5_prop, Kerberos v5 slave propagation	No Oficial
754/UDP	tell send	Oficial
760/TCP,UDP	Ns	Oficial
760/TCP,UDP	krbupdate [kreg], Kerberos registration	No Oficial
782/TCP	Conserver serial-console management server	No Oficial
783/TCP	SpamAssassin spamd daemon	No Oficial
829/TCP	CMP (Certificate Management Protocol)	No Oficial
843/TCP	Adobe Flash socket policy server	No Oficial
860/TCP	iSCSI (RFC 3720)	Oficial
873/TCP	rsync file synchronisation protocol	Oficial
888/TCP	cddbp, CD DataBase (CDDB) protocol (CDDBP)—unassigned but widespread use	No Oficial
901/TCP	Samba Web Administration Tool (SWAT)	No Oficial
901/TCP, UDP	VMware Virtual Infrastructure Client (UDP from server being managed to management console)	No Oficial
902/TCP	VMware Server Console (TCP from management console to server being Managed)	No Oficial

902/UDP	VMware Server Console (UDP from server being managed to management console)	No Oficial
903/TCP	VMware Remote Console [26]	No Oficial
904/TCP	VMware Server Alternate (if 902 is in use, i.e. SUSE linux)	No Oficial
911/TCP	Network Console on Acid (NCA)—local tty redirection over OpenSSH	No Oficial
953/TCP,UDP	Domain Name System (DNS) RDNC Service	No Oficial
981/TCP	SofaWare Technologies Remote HTTPS management for firewall devices running embedded Check Point FireWall-1 software	No Oficial
989/TCP,UDP	FTPS Protocol (data): FTP over TLS/SSL	Oficial
990/TCP,UDP	FTPS Protocol (control): FTP over TLS/SSL	Oficial
991/TCP,UDP	NAS (Netnews Administration System)	Oficial
992/TCP,UDP	TELNET protocol over TLS/SSL	Oficial
993/TCP	Internet Message Access Protocol over SSL (IMAPS)	Oficial
995/TCP	Post Office Protocol 3 over TLS/SSL (POP3S)	Oficial
999/TCP	ScimoreDB Database System	No Oficial
1001/TCP	JtoMB	No Oficial
1023/TCP,UDP	Reserved	Oficial

Puerto	Descripcion	Estado
1024/TCP,UDP	Reserved[1]	Oficial
1025/TCP	NFS-or-IIS	No Oficial
1026/TCP	Often utilized by Microsoft **DCOM** services	No Oficial
1029/TCP	Often utilized by Microsoft **DCOM** services	No Oficial
1058/TCP,UDP	nim, **IBM AIX Network Installation Manager** (NIM)	Oficial
1059/TCP,UDP	nimreg, **IBM AIX Network Installation Manager** (NIM)	Oficial
1080/TCP	**SOCKS** proxy	Oficial
1085/TCP,UDP	**WebObjects**	Oficial
1098/TCP,UDP	rmiactivation, **RMI** Activation	Oficial
1099/TCP,UDP	rmiregistry, **RMI** Registry	Oficial
1109/TCP,UDP	Reserved[1]	Oficial
1109/TCP	**Kerberos** Post Office Protocol (**KPOP**)	No Oficial
1111/UDP	**EasyBits** School network discovery protocol (for Intel's CMPC platform)	No Oficial
1140/TCP,UDP	**AutoNOC** protocol	Oficial
1167/UDP	phone, conference calling	No Oficial

1169/TCP,UDP	Tripwire	Oficial
1176/TCP	**Perceptive Automation Indigo Home automation** server	Oficial
1182/TCP,UDP	**AcceleNet Intelligent Transfer Protocol**	Oficial
1194/TCP,UDP	**OpenVPN**	Oficial
1198/TCP,UDP	The **cajo project** Free dynamic transparent distributed computing in Java	Oficial
1200/TCP	scol, protocol used by SCOL 3D virtual worlds server to answer world name resolution client request[27]	Oficial
1200/UDP	scol, protocol used by SCOL 3D virtual worlds server to answer world name resolution client request	Oficial
1200/UDP	**Steam Friends Applet**	No Oficial
1214/TCP	**Kazaa**	Oficial
1220/TCP	**QuickTime Streaming Server** administration	Oficial
1223/TCP,UDP	TGP, **TrulyGlobal** Protocol, also known as "The Gur Protocol" (named for Gur Kimchi of TrulyGlobal)	Oficial
1234/UDP	**VLC media player** Default port for UDP/RTP stream	No Oficial
1236/TCP	**Symantec BindView Control UNIX** Default port for TCP management server connections	No Oficial
1241/TCP,UDP	**Nessus** Security Scanner	Oficial
1248/TCP	NSClient/NSClient++/NC_Net (Nagios)	No Oficial

1270/TCP,UDP	**Microsoft System Center Operations Manager** (SCOM) (formerly Microsoft Operations Manager (MOM)) agent	Oficial
1293/TCP,UDP	**IPSec** (Internet Protocol Security)	Oficial
1311/TCP	Dell Open Manage HTTPS	No Oficial
1313/TCP	Xbiim (Canvii server)	No Oficial
1337/TCP	**PowerFolder** P2P Encrypted File Synchronization Program	No Oficial
1337/TCP	**WASTE** Encrypted File Sharing Program	No Oficial
1352/TCP	**IBM Lotus Notes/Domino Remote Procedure Call (RPC)** protocol	Oficial
1387/TCP,UDP	cadsi-lm, **LMS International** (formerly Computer Aided Design Software, Inc. (CADSI)) LM	Oficial
1414/TCP	**IBM WebSphere MQ** (formerly known as **MQSeries**)	Oficial
1417/TCP,UDP	Timbuktu Service 1 Port	Oficial
1418/TCP,UDP	Timbuktu Service 2 Port	Oficial
1419/TCP,UDP	Timbuktu Service 3 Port	Oficial
1420/TCP,UDP	Timbuktu Service 4 Port	Oficial
1431/TCP	**Reverse Gossip Transport Protocol (RGTP)**, used to access a General-purpose Reverse-Ordered Gossip Gathering System (**GROGGS**) **bulletin board**, such as that implemented on the **Cambridge University**'s **Phoenix system**	Oficial
1433/TCP	MSSQL (**Microsoft SQL Server database management system**) Server	Oficial

1434/UDP	MSSQL (**Microsoft SQL Server database management system**) Monitor	Oficial
1494/TCP	**Citrix XenApp Independent Computing Architecture** (ICA) **thin client protocol**	Oficial
1500/TCP	**NetGuard GuardianPro** firewall (NT4-based) Remote Management	No Oficial
1501/UDP	**NetGuard GuardianPro** firewall (NT4-based) Authentication Client	No Oficial
1503/TCP,UDP	**Windows Live Messenger** (Whiteboard and Application Sharing)	No Oficial
1512/TCP,UDP	**Microsoft Windows Internet Name Service (WINS)**	Oficial
1521/TCP	nCube License Manager	Oficial
1521/TCP	**Oracle database** default listener, in future releases Oficial port 2483	No Oficial
1524/TCP,UDP	ingreslock, ingres	Oficial
1526/TCP	**Oracle database** common alternative for listener	No Oficial
1533/TCP	IBM **Sametime** IM—Virtual Places Chat **Microsoft SQL Server**	Oficial
1547/TCP,UDP	**Laplink**	Oficial
1550	**Gadu-Gadu** (direct client-to-client)	No Oficial
1581/UDP	**MIL STD 2045-47001 VMF**	Oficial
1589/UDP	Cisco **VQP** (VLAN Query Protocol) / **VMPS**	No Oficial
1645/TCP,UDP	radius/radacct, **RADIUS** authentication protocol (**default** for **Cisco**	No Oficial

	and **Juniper Networks** RADIUS servers)	
1627	iSketch	No Oficial
1677/TCP,UDP	**Novell GroupWise** clients in client/server access mode	Oficial
1701/UDP	**Layer 2 Forwarding Protocol** (L2F) & **Layer 2 Tunneling Protocol** (L2TP)	Oficial
1716/TCP	**America's Army Massively multiplayer online game** (**MMO**)	No Oficial
1719/UDP	**H.323** Registration and alternate communication	Oficial
1720/TCP	**H.323** Call signalling	Oficial
1723/TCP,UDP	Microsoft **Point-to-Point Tunneling Protocol** (PPTP)	Oficial
1725/UDP	Valve Steam Client	No Oficial
1755/TCP,UDP	**Microsoft Media Services** (MMS, ms-streaming)	Oficial
1761/TCP,UDP	cft-0	Oficial
1761/TCP	**Novell Zenworks** Remote Control utility	No Oficial
1762–1768/TCP,UDP	cft-1 to cft-7	Oficial
1812/TCP,UDP	radius, **RADIUS** authentication protocol	Oficial
1813/TCP,UDP	radacct, **RADIUS** accounting protocol	Oficial
1863/TCP	**MSNP** (**Microsoft Notification Protocol**), used by the **.NET Messenger Service** and a number of **Instant Messaging clients**	Oficial

1900/UDP	Microsoft **SSDP** Enables discovery of **UPnP** devices	Oficial
1920/TCP	IBM Tivoli Monitoring Console (https)	No Oficial
1935/TCP	**Adobe Systems Macromedia Flash Real Time Messaging Protocol (RTMP)** "plain" protocol	Oficial
1970/TCP,UDP	**Danware NetOp** Remote Control	Oficial
1971/TCP,UDP	**Danware NetOp** School	Oficial
1972/TCP,UDP	**InterSystems Caché**	Oficial
1975–1977/UDP	Cisco **TCO** (**Documentation**)	Oficial
1984/TCP	Big Brother—network monitoring tool	Oficial
1985/UDP	**Cisco HSRP**	Oficial
1994/TCP,UDP	**Cisco** STUN-SDLC (Serial Tunneling—**Synchronous Data Link Control**) protocol	Oficial
1998/TCP,UDP	**Cisco** X.25 over TCP (**XOT**) service	Oficial
2000/TCP,UDP	**Cisco SCCP (Skinny)**	Oficial
2001/UDP	**CAPTAN Test Stand System**	No Oficial
2002/TCP	Secure Access Control Server (ACS) for Windows	No Oficial
2030	**Oracle** Services for **Microsoft Transaction Server**	No Oficial
2031/TCP,UDP	mobrien-chat—obsolete (**ex-http://www.mobrien.com**)	Oficial

2041/TCP	Mail.Ru Agent communication protocol	No Oficial
2049/UDP	**Network File System**	Oficial
2049/UDP	Shilp	Oficial
2053/UDP	lot105-ds-upd Lot105 DSuper Updates	Oficial
2053/TCP	lot105-ds-upd Lot105 DSuper Updates	Oficial
2053/TCP	knetd **Kerberos** de-multiplexor	No Oficial
2056/UDP	**Civilization 4** multiplayer	No Oficial
2073/TCP,UDP	DataReel Database	Oficial
2074/TCP,UDP	Vertel VMF SA (i.e. App.. SpeakFreely)	Oficial
2082/TCP	Infowave Mobility Server	Oficial
2082/TCP	**CPanel** default	No Oficial
2083/TCP	Secure Radius Service (radsec)	Oficial
2083/TCP	**CPanel** default **SSL**	No Oficial
2086/TCP	**GNUnet**	Oficial
2086/TCP	**WebHost Manager** default	No Oficial
2087/TCP	**WebHost Manager** default **SSL**	No Oficial
2095/TCP	**CPanel** default Web mail	No Oficial

2096/TCP	**CPanel** default **SSL** Web mail	No Oficial
2102/TCP,UDP	zephyr-srv **Project Athena** Zephyr Notification Service server	Oficial
2103/TCP,UDP	zephyr-clt **Project Athena** Zephyr Notification Service serv-hm connection	Oficial
2104/TCP,UDP	zephyr-hm **Project Athena** Zephyr Notification Service hostmanager	Oficial
2105/TCP,UDP	**IBM** MiniPay	Oficial
2105/TCP,UDP	eklogin **Kerberos** encrypted remote login (rlogin)	No Oficial
2105/TCP,UDP	zephyr-hm-srv **Project Athena** Zephyr Notification Service hm-serv connection (should use port 2102)	No Oficial
2144/TCP	Iron Mountain LiveVault Agent	No Oficial
2145/TCP	Iron Mountain LiveVault Agent	No Oficial
2161/TCP	**APC** Agent	Oficial
2181/TCP,UDP	**EForward**-document transport system	Oficial
2190/UDP	TiVoConnect Beacon	No Oficial
2200/UDP	Tuxanci game server[28]	No Oficial
2210/TCP,UDP	NOAAPORT Broadcast Network	Oficial
2210/TCP	**MikroTik** Remote management for "The Dude"	No Oficial
2211/TCP,UDP	EMWIN	Oficial

2211/TCP	**MikroTik** Secure management for "The Dude"	No Oficial
2212/TCP,UDP	LeeCO POS Server Service	Oficial
2212/TCP	**Port-A-Pour** Remote WinBatch	No Oficial
2219/TCP,UDP	**NetIQ** NCAP Protocol	Oficial
2220/TCP,UDP	**NetIQ** End2End	Oficial
2222/TCP	**DirectAdmin** default & ESET	No Oficial
2223/UDP	Microsoft Office OS X antipiracy network monitor	No Oficial
2301/TCP	HP System Management Redirect to port 2381	No Oficial
2302/UDP	**ArmA** multiplayer (default for game)	No Oficial
2302/UDP	**Halo: Combat Evolved** multiplayer	No Oficial
2303/UDP	**ArmA** multiplayer (default for server reporting) *(default port for game +1)*	No Oficial
2305/UDP	**ArmA** multiplayer (default for VoN) *(default port for game +3)*	No Oficial
2369/TCP	Default for **BMC Software CONTROL-M/Server**—Configuration Agent, though often changed during installation	Oficial
2370/TCP	Default for **BMC Software CONTROL-M/Server**—to allow the **CONTROL-M/Enterprise Manager** to connect to the **CONTROL-M/Server**, though often changed during installation	Oficial
2381/TCP	HP Insight Manager default for Web server	No Oficial

2401/TCP	**CVS** version control system	No Oficial
2404/TCP	**IEC 60870-5-104**, used to send **electric power telecontrol messages** between two systems via directly connected **data circuits**	Oficial
2420/UDP	Westell Remote Access	Oficial
2427/UDP	Cisco **MGCP**	Oficial
2447/TCP,UDP	ovwdb—**OpenView Network Node Manager** (NNM) daemon	Oficial
2483/TCP,UDP	**Oracle database** listening for unsecure client connections to the listener, replaces port 1521	Oficial
2484/TCP,UDP	**Oracle database** listening for **SSL** client connections to the listener	Oficial
2500/TCP	THEÒSMESSENGER listening for TheòsMessenger client connections	Oficial
2546/TCP,UDP	EVault—Data Protection Services	No Oficial
2593/TCP,UDP	RunUO—**Ultima Online** server	No Oficial
2598/TCP	new ICA—when Session Reliability is enabled, TCP port 2598 replaces port 1494	No Oficial
2610/TCP	**Dark Ages**	No Oficial
2612/TCP,UDP	QPasa from MQSoftware	Oficial
2638/TCP	Sybase database listener	No Oficial
2700–2800/TCP	KnowShowGo P2P	Oficial

2710/TCP	XBT Bittorrent Tracker	No Oficial
2710/UDP	XBT Bittorrent Tracker experimental UDP tracker extension	No Oficial
2710/TCP	Knuddels.de	No Oficial
2713/TCP,UDP	Raven Trinity Broker Service	Oficial
2714/TCP,UDP	Raven Trinity Data Mover	Oficial
2735/TCP,UDP	**NetIQ** Monitor Console	Oficial
2809/TCP	corbaloc:iiop URL, per the **CORBA** 3.0.3 specification	Oficial
2809/TCP	IBM **WebSphere Application Server** (WAS) **Bootstrap/rmi default**	No Oficial
2809/UDP	corbaloc:iiop URL, per the **CORBA** 3.0.3 specification.	Oficial
2868/TCP,UDP	Norman Proprietary Event Protocol NPEP	Oficial
2944/UDP	**Megaco** Text H.248	No Oficial
2945/UDP	**Megaco** Binary (ASN.1) H.248	No Oficial
2948/TCP,UDP	**WAP**-push **Multimedia Messaging Service** (MMS)	Oficial
2949/TCP,UDP	**WAP**-pushsecure **Multimedia Messaging Service** (MMS)	Oficial
2967/TCP	Symantec AntiVirus Corporate Edition	No Oficial
3000/TCP	Miralix License server	No Oficial

3000/UDP	**Distributed Interactive Simulation** (DIS), modifiable default	No Oficial
3001/TCP	Miralix Phone Monitor	No Oficial
3002/TCP	Miralix CSTA	No Oficial
3003/TCP	Miralix GreenBox API	No Oficial
3004/TCP	Miralix InfoLink	No Oficial
3005/TCP	Miralix TimeOut	No Oficial
3006/TCP	Miralix SMS Client Connector	No Oficial
3007/TCP	Miralix OM Server	No Oficial
3017/TCP	Miralix IVR and Voicemail	No Oficial
3025/TCP	netpd.org	No Oficial
3030/TCP,UDP	**NetPanzer**	No Oficial
3050/TCP,UDP	gds_db (Interbase/Firebird)	Oficial
3051/TCP,UDP	Galaxy Server (Gateway Ticketing Systems)	Oficial
3074/TCP,UDP	**Xbox LIVE** and/or **Games for Windows - LIVE**	Oficial
3100/TCP	**HTTP** used by Tatsoft as the default listen port	No Oficial
3101/TCP	**Blackberry Enterprise Server** communcation to cloud	No Oficial
3128/TCP	**HTTP** used by **Web caches** and the default for the **Squid cache**	No Oficial

3128/TCP	**HTTP** used by Tatsoft as the default client connection	No Oficial
3225/TCP,UDP	**FCIP** (Fiber Channel over Internet Protocol)	Oficial
3233/TCP,UDP	**WhiskerControl** research control protocol	Oficial
3235/TCP,UDP	Galaxy Network Service (Gateway Ticketing Systems)	Oficial
3260/TCP,UDP	**iSCSI** target	Oficial
3268/TCP,UDP	msft-gc, Microsoft Global Catalog (**LDAP** service which contains data from **Active Directory** forests)	Oficial
3269/TCP,UDP	msft-gc-ssl, Microsoft Global Catalog over **SSL** (similar to port 3268, **LDAP** over **SSL**)	Oficial
3283/TCP	**Apple Remote Desktop** reporting (Oficially *Net Assistant*, referring to an earlier product)	Oficial
3299/TCP	SAP-Router (routing application proxy for **SAP R/3**)	No Oficial
3300/TCP	**TripleA** game server	No Oficial
3300/TCP,UDP	Debate Gopher backend database system	No Oficial
3305/TCP,UDP	odette-ftp, **Odette File Transfer Protocol** (**OFTP**)	Oficial
3306/TCP,UDP	**MySQL** database system	Oficial
3333/TCP	Network Caller ID server	No Oficial
3386/TCP,UDP	**GTP' 3GPP GSM/UMTS CDR** logging protocol	Oficial
3389/TCP	Microsoft Terminal Server (**RDP**) Oficially registered as Windows	Oficial

	Based Terminal (WBT)	
3396/TCP,UDP	**Novell** NDPS Printer Agent	Oficial
3455/TCP,UDP	[RSVP] Reservation Protocol	Oficial
3423/TCP	**Xware** xTrm Communication Protocol	Oficial
3424/TCP	**Xware** xTrm Communication Protocol over SSL	Oficial
3478/TCP,UDP	**STUN**, a protocol for NAT traversal	Oficial
3483/UDP	**Slim Devices** discovery protocol	Oficial
3483/TCP	**Slim Devices** SlimProto protocol	Oficial
3516/TCP,UDP	Smartcard Port	Oficial
3532/TCP,UDP	Raven Remote Management Control	Oficial
3533/TCP,UDP	Raven Remote Management Data	Oficial
3537/TCP,UDP	ni-visa-remote	No Oficial
3544/UDP	**Teredo tunneling**	Oficial
3632/TCP	**distributed compiler**	Oficial
3689/TCP	**Digital Audio Access Protocol** (DAAP)—used by **Apple's iTunes** and **AirPort Express**	Oficial
3690/TCP,UDP	**Subversion** version control system	Oficial
3702/TCP,UDP	**Web Services Dynamic Discovery** (WS-Discovery), used by	Oficial

	various components of **Windows Vista**	
3723/TCP,UDP	Used by many Battle.net Blizzard games (**Diablo II**, **Warcraft II**, **Warcraft III**, **StarCraft**)	No Oficial
3724/TCP,UDP	**World of Warcraft** Online gaming MMORPG	No Oficial
3724/TCP	**Club Penguin** Disney online game for kids	No Oficial
3784/TCP,UDP	**Ventrilo** VoIP program used by **Ventrilo**	No Oficial
3785/UDP	**Ventrilo** VoIP program used by **Ventrilo**	No Oficial
3868/TCP,SCTP	**Diameter** base protocol (**RFC 3588**)	Oficial
3872/TCP	Oracle Management Remote Agent	No Oficial
3899/TCP	**Remote Administrator**	No Oficial
3900/TCP	udt_os, **IBM UniData** UDT OS[29]	Oficial
3945/TCP,UDP	EMCADS service, a Giritech product used by G/On	Oficial
3978/UDP	**OpenTTD** game serverlist masterserver	No Oficial
3979/TCP,UDP	**OpenTTD** game	No Oficial
3999/TCP,UDP	Norman distributed scanning service	Oficial
4000/TCP,UDP	**Diablo II** game	No Oficial
4001/TCP	**Microsoft Ants** game	No Oficial
4007/TCP	PrintBuzzer printer monitoring socket server	No Oficial

4018/TCP,UDP	protocol information and warnings	Oficial
4069/UDP	Minger Email Address Verification Protocol[30]	Oficial
4089/TCP,UDP	OpenCORE Remote Control Service	Oficial
4093/TCP,UDP	PxPlus Client server interface **ProvideX**	Oficial
4096/TCP,UDP	Bridge-Relay Element **ASCOM**	Oficial
4100	WatchGuard Authentication Applet—default	No Oficial
4111/TCP	**Xgrid**	Oficial
4116/TCP,UDP	Smartcard-TLS	Oficial
4125/TCP	**Microsoft Remote Web Workplace** administration	No Oficial
4201/TCP	**TinyMUD** and various derivatives	No Oficial
4226/TCP,UDP	**Aleph One (game)**	No Oficial
4224/TCP	Cisco Audio Session Tunneling	No Oficial
4321/TCP	**Referral Whois (RWhois) Protocol**[31]	Oficial
4500/UDP	**IPSec NAT Traversal** (**RFC 3947**)	Oficial
4534/UDP	**Armagetron Advanced** default server port	No Oficial
4569/UDP	**Inter-Asterisk eXchange**	No Oficial
4610–4640/TCP	**QualiSystems** TestShell Suite Services	No Oficial

4662/TCP,UDP	OrbitNet Message Service	Oficial
4662/TCP	often used by **eMule**	No Oficial
4664/TCP	**Google Desktop Search**	No Oficial
4664/TCP	Default for Unica's Campaign Listener, though often changed during installation	No Oficial
4672/UDP	**eMule**—often used	No Oficial
4747/TCP	**Apprentice**	No Oficial
4750/TCP	**BladeLogic** Agent	No Oficial
4840/TCP,UDP	OPC UA TCP Protocol for **OPC Unified Architecture** from **OPC Foundation**	Oficial
4843/TCP,UDP	OPC UA TCP Protocol over TLS/SSL for **OPC Unified Architecture** from **OPC Foundation**	Oficial
4847/TCP,UDP	Web Fresh Communication, **Quadrion Software** & **Odorless Entertainment**	Oficial
4993/TCP,UDP	Home FTP Server web Interface Default Port	
4894/TCP,UDP	**LysKOM** Protocol A	Oficial
4899/TCP,UDP	**Radmin** remote administration tool (program sometimes used by a **Trojan horse**)	Oficial
5000/TCP	commplex-main	Oficial
5000/TCP	**UPnP**—Windows network device interoperability	No Oficial

5000/TCP,UDP	**VTun**—**VPN** Software	No Oficial
5001/TCP	commplex-link	Oficial
5001/TCP,UDP	Iperf (Tool for measuring TCP and UDP bandwidth performance)	No Oficial
5001/TCP	**Slingbox** and Slingplayer	No Oficial
5003/TCP,UDP	**FileMaker**	Oficial
5004/TCP,UDP,DCCP	**RTP** (Real-time Transport Protocol) media data (**RFC 3551**, **RFC 4571**)	Oficial
5005/TCP,UDP,DCCP	**RTP** (Real-time Transport Protocol) control protocol (**RFC 3551**, **RFC 4571**)	Oficial
5031/TCP,UDP	AVM CAPI-over-TCP (**ISDN** over **Ethernet** tunneling)	No Oficial
5050/TCP	**Yahoo! Messenger**	No Oficial
5051/TCP	ita-agent **Symantec** Intruder Alert[32]	Oficial
5060/TCP,UDP	**Session Initiation Protocol** (SIP)	Oficial
5061/TCP	**Session Initiation Protocol** (SIP) over **TLS**	Oficial
5093/UDP	**SPSS** (Statistical Package for the Social Sciences) License Administrator	No Oficial
5104/TCP	**IBM Tivoli Framework** NetCOOL/Impact[33] **HTTP** Service	No Oficial
5106/TCP	A-Talk Common connection	No Oficial
5107/TCP	A-Talk Remote server connection	No Oficial

5110/TCP	ProRat Server	No Oficial
5121/TCP	**Neverwinter Nights**	No Oficial
5151/TCP	**ESRI** SDE Instance	Oficial
5151/UDP	**ESRI** SDE Remote Start	Oficial
5154/TCP,UDP	**BZFlag**	Oficial
5176/TCP	ConsoleWorks default UI interface	No Oficial
5190/TCP	**ICQ** and **AOL Instant Messenger**	Oficial
5222/TCP	**Extensible Messaging and Presence Protocol** (XMPP) client connection (**RFC 3920**)	Oficial
5223/TCP	**Extensible Messaging and Presence Protocol** (XMPP) client connection over **SSL**	No Oficial
5269/TCP	**Extensible Messaging and Presence Protocol** (XMPP) server connection (**RFC 3920**)	Oficial
5298/TCP,UDP	**Extensible Messaging and Presence Protocol** (XMPP) JEP-0174: Link-Local Messaging / **XEP-0174: Serverless Messaging**	Oficial
5351/TCP,UDP	**NAT Port Mapping Protocol**—client-requested configuration for inbound connections through **network address translators**	Oficial
5353/UDP	**Multicast DNS** (mDNS)	Oficial
5355/TCP,UDP	**LLMNR**—Link-Local Multicast Name Resolution, allows **hosts** to perform **name resolution** for hosts on the same **local link** (only provided by **Windows Vista** and **Server 2008**)	Oficial
5402/TCP,UDP	mftp, Stratacache **OmniCast content delivery** system **MFTP file**	Oficial

	sharing protocol	
5405/TCP,UDP	**NetSupport**	Oficial
5421/TCP,UDP	**Net Support 2**	Oficial
5432/TCP,UDP	**PostgreSQL** database system	Oficial
5433/TCP	Bouwsoft file/webserver (**http://www.bouwsoft.be**)	No Oficial
5445/UDP	**Cisco** Unified Video Advantage	No Oficial
5450/TCP	**OSIsoft** PI Server Client Access	No Oficial
5495/TCP	**Applix** TM1 Admin server	No Oficial
5498/TCP	**Hotline** tracker server connection	No Oficial
5499/UDP	**Hotline** tracker server discovery	No Oficial
5500/TCP	**VNC** remote desktop protocol—for incoming listening viewer, **Hotline** control connection	No Oficial
5501/TCP	**Hotline** file transfer connection	No Oficial
5517/TCP	**Setiqueue** Proxy server client for **SETI@Home** project	No Oficial
5550/TCP	**Hewlett-Packard** Data Protector	No Oficial
5555/TCP	**Freeciv** versions up to 2.0, **Hewlett-Packard** Data Protector, **SAP**	No Oficial
5556/TCP,UDP	**Freeciv**	Oficial
5631/TCP	pcANYWHEREdata, **Symantec pcAnywhere** (version 7.52 and	Oficial

	later[34])[35] data	
5632/UDP	pcANYWHEREstat, **Symantec pcAnywhere** (version 7.52 and later) status	Oficial
5666/TCP	NRPE (Nagios)	No Oficial
5667/TCP	NSCA (Nagios)	No Oficial
5723/TCP	Operations Manager	No Oficial
5800/TCP	**VNC** remote desktop protocol—for use over **HTTP**	No Oficial
5814/TCP,UDP	**Hewlett-Packard** Support Automation (HP OpenView Self-Healing Services)	Oficial
5850/TCP	COMIT SE (PCR)	No Oficial
5852/TCP	Adeona client: communications to OpenDHT	No Oficial
5900/TCP,UDP	**Virtual Network Computing** (VNC) remote desktop protocol (used by **Apple Remote Desktop** and others)	Oficial
5938/TCP,UDP	TeamViewer[36] remote desktop protocol	No Oficial
5984/TCP,UDP	**CouchDB** database server	Oficial
5999/TCP	**CVSup** [37] file update tool	Unknown
6000/TCP	**X11**—used between an X client and server over the network	Oficial
6001/UDP	**X11**—used between an X client and server over the network	Oficial
6005/TCP	Default for **BMC Software CONTROL-M/Server**—Socket used for communication between CONTROL-M processes—though often	Oficial

	changed during installation	
6005/TCP	Default for Camfrog Chat & Cam Client **http://www.camfrog.com**	No Oficial
6050/TCP	Brightstor Arcserve Backup	No Oficial
6050/TCP	Nortel Software	No Oficial
6051/TCP	Brightstor Arcserve Backup	No Oficial
6072/TCP	iOperator Protocol Signal Port	No Oficial
6086/TCP	**PDTP**—FTP like file server in a P2P network	Oficial
6100/TCP	Vizrt System	No Oficial
6101/TCP	Backup Exec Agent Browser	No Oficial
6110/TCP,UDP	softcm, **HP Softbench** CM	Oficial
6111/TCP,UDP	spc, **HP Softbench** Sub-Process Control	Oficial
6112/TCP,UDP	"dtspcd"—a network **daemon** that accepts requests from clients to execute commands and launch applications remotely	Oficial
6112/TCP	**Blizzard**'s **Battle.net** gaming service, **ArenaNet** gaming service	No Oficial
6112/TCP	**Club Penguin** Disney online game for kids	No Oficial
6113/TCP	**Club Penguin** Disney online game for kids	No Oficial
6129/TCP	**DameWare Remote Control**	Oficial
6257/UDP	**WinMX** (see also 6699)	No Oficial

6346/TCP,UDP	**gnutella-svc**, Gnutella (**FrostWire**, **Limewire**, **Shareaza**, etc.)	Oficial
6347/TCP,UDP	**gnutella-rtr**, Gnutella alternate	Oficial
6389/TCP	**EMC** Clariion	No Oficial
6444/TCP,UDP	**Sun Grid Engine**—Qmaster Service	Oficial
6445/TCP,UDP	**Sun Grid Engine**—Execution Service	Oficial
6502/TCP,UDP	Danware Data NetOp Remote Control	No Oficial
6522/TCP	**Gobby** (and other libobby-based software)	No Oficial
6523/TCP	**Gobby** 0.5 (and other libinfinity-based software)	No Oficial
6543/UDP	**Paradigm Research & Development** Jetnet[38] default	No Oficial
6566/TCP	**SANE** (Scanner Access Now Easy)—SANE network scanner daemon	No Oficial
6571	**Windows Live FolderShare** client	No Oficial
6600/TCP	**Music Playing Daemon (MPD)**	No Oficial
6619/TCP,UDP	odette-ftps, **Odette File Transfer Protocol** (**OFTP**) over **TLS**/**SSL**	Oficial
6646/UDP	**McAfee** Network Agent	No Oficial
6660–6664/TCP	**Internet Relay Chat**	No Oficial
6665–6669/TCP	**Internet Relay Chat**	Oficial

6679/TCP	**IRC SSL** (Secure Internet Relay Chat)—often used	No Oficial
6697/TCP	**IRC SSL** (Secure Internet Relay Chat)—often used	No Oficial
6699/TCP	**WinMX** (see also 6257)	No Oficial
6771/UDP	**Polycom** server broadcast	No Oficial
6789/TCP	**Datalogger Support Software** Campbell Scientific Loggernet Software	No Oficial
6881–6887/TCP,UDP	**BitTorrent** part of full range of ports used most often	No Oficial
6888/TCP,UDP	MUSE	Oficial
6888/TCP,UDP	**BitTorrent** part of full range of ports used most often	No Oficial
6889–6890/TCP,UDP	**BitTorrent** part of full range of ports used most often	No Oficial
6891–6900/TCP,UDP	**BitTorrent** part of full range of ports used most often	No Oficial
6891–6900/TCP,UDP	**Windows Live Messenger** (File transfer)	No Oficial
6901/TCP,UDP	**Windows Live Messenger** (Voice)	No Oficial
6901/TCP,UDP	**BitTorrent** part of full range of ports used most often	No Oficial
6902–6968/TCP,UDP	**BitTorrent** part of full range of ports used most often	No Oficial
6969/TCP,UDP	Acmsoda	Oficial

6969/TCP	**BitTorrent** tracker	No Oficial
6970–6999/TCP,UDP	**BitTorrent** part of full range of ports used most often	No Oficial
7000/TCP	Default for **Vuze**'s built in **HTTPS Bittorrent Tracker**	No Oficial
7001/TCP	Default for **BEA WebLogic Server**'s **HTTP** server, though often changed during installation	No Oficial
7002/TCP	Default for **BEA WebLogic Server**'s **HTTPS** server, though often changed during installation	No Oficial
7005/TCP	Default for **BMC Software CONTROL-M/Server** and CONTROL-M/Agent for Agent-to-Server, though often changed during installation	Oficial
7006/TCP	Default for **BMC Software CONTROL-M/Server** and CONTROL-M/Agent for Server-to-Agent, though often changed during installation	Oficial
7010/TCP	Default for Cisco AON AMC (AON Management Console) **[2]**	No Oficial
7025/TCP	Zimbra LMTP [mailbox]—local mail delivery	No Oficial
7047/TCP	Zimbra conversion server	No Oficial
7133/TCP	Enemy Territory: Quake Wars	No Oficial
7171/TCP	**Tibia**	No Oficial
7306/TCP	Zimbra mysql [mailbox]	No Oficial
7307/TCP	Zimbra mysql [logger]	No Oficial
7312/UDP	**Sibelius** License Server	No Oficial

7400/TCP,UDP	RTPS (Real Time Publish Subscribe) **DDS** Discovery	Oficial
7401/TCP,UDP	RTPS (Real Time Publish Subscribe) **DDS** User-Traffic	Oficial
7402/TCP,UDP	RTPS (Real Time Publish Subscribe) **DDS** Meta-Traffic	Oficial
7670/TCP	**BrettspielWelt** BSW Boardgame Portal	No Oficial
7676/TCP	Aqumin AlphaVision Remote Command Interface	No Oficial
7777/TCP	iChat server file transfer proxy	No Oficial
7777/TCP	Default used by Windows backdoor program tini.exe	No Oficial
7777-7788/TCP,udp	Unreal Tournament 2004 default server	No Oficial
7831/TCP	Default used by Smartlaunch Internet Cafe Administration[39] software	No Oficial
7915/TCP	Default for YSFlight server **[3]**	No Oficial
8000/TCP,UDP	iRDMI (Intel Remote **Desktop Management Interface**)[40]— sometimes erroneously used instead of port 8080	Oficial
8000–8001/TCP	Commonly used for internet radio streams such as those using **SHOUTcast**	No Oficial
8002/TCP	Cisco Systems Unified Call Manager Intercluster	No Oficial
8008/TCP	**HTTP** Alternate	Oficial
8008/TCP	**IBM HTTP Server** administration default	No Oficial

8009/TCP	**ajp13 – Apache JServ Protocol** AJP Connector	No Oficial
8010/TCP	**XMPP** File transfers	No Oficial
8074/TCP	**Gadu-Gadu**	No Oficial
8080/TCP	**HTTP** alternate (http_alt)—commonly used for **Web proxy** and **caching** server, or for running a Web server as a non-**root** user	Oficial
8080/TCP	**Apache Tomcat**	No Oficial
8080/UDP	**FilePhile** Master/Relay	No Oficial
8081/TCP	**HTTP** alternate, e.g. **McAfee ePolicy Orchestrator (ePO)**	No Oficial
8086/TCP	**HELM** Web Host Automation Windows Control Panel	No Oficial
8086/TCP	**Kaspersky** AV Control Center	No Oficial
8087/TCP	**Hosting Accelerator** Control Panel	No Oficial
8087/TCP	**Parallels Plesk** Control Panel	No Oficial
8087/UDP	**Kaspersky** AV Control Center	No Oficial
8090/TCP	**HTTP** Alternate (http_alt_alt)—used as an alternative to port 8080	No Oficial
8116/UDP	**Check Point** Cluster Control Protocol	No Oficial
8118/TCP	**Privoxy**—advertisement-filtering Web proxy	Oficial
8123/TCP	**Polipo** Web proxy	Oficial

8192/TCP	**Sophos** Remote Management System	No Oficial
8193/TCP	**Sophos** Remote Management System	No Oficial
8194/TCP	**Sophos** Remote Management System	No Oficial
8200/TCP	**GoToMyPC**	No Oficial
8222	**VMware** Server Management User Interface (insecure Web interface)[41]. See also port 8333	No Oficial
8243/TCP,UDP	**HTTPS** listener for **Apache Synapse** [42]	Oficial
8280/TCP,UDP	**HTTP** listener for **Apache Synapse** [42]	Oficial
8291/TCP	Winbox—Default on a MikroTik RouterOS for a Windows application used to administer MikroTik RouterOS	No Oficial
8333	**VMware** Server Management User Interface (secure Web interface)[41]. See also port 8222	No Oficial
8400/TCP,UDP	cvp, **Commvault** Unified Data Management	Oficial
8443/TCP	**SW Soft Plesk** Control Panel, **Apache Tomcat** SSL, **Promise** WebPAM SSL	No Oficial
8484/TCP,UDP	**MapleStory**	No Oficial
8500/TCP,IPX	**ColdFusion** Macromedia/Adobe ColdFusion default and **Duke Nukem 3D**—default	No Oficial
8501/TCP	**[4]** DukesterX —default	No Oficial
8691/TCP	**Ultra Fractal** default server port for distributing calculations over network computers	No Oficial

8701/UDP	**SoftPerfect Bandwidth Manager**	No Oficial
8702/UDP	**SoftPerfect Bandwidth Manager**	No Oficial
8767/UDP	**TeamSpeak**—default	No Oficial
8768/UDP	**TeamSpeak**—altérnate	No Oficial
8880/UDP	cddbp-alt, **CD DataBase** (**CDDB**) protocol (CDDBP) alternate	Oficial
8880/TCP	cddbp-alt, **CD DataBase** (**CDDB**) protocol (CDDBP) alternate	Oficial
8880/TCP	**WebSphere Application Server SOAP** connector **default**	No Oficial
8881/TCP	**Atlasz Informatics Research Ltd** Secure Application Server	No Oficial
8882/TCP	**Atlasz Informatics Research Ltd** Secure Application Server	No Oficial
8888/TCP,UDP	**NewsEDGE** server	Oficial
8888/TCP	**Sun Answerbook dwhttpd** server (deprecated by **docs.sun.com**)	No Oficial
8888/TCP	**GNUmp3d** HTTP music streaming and Web interface	No Oficial
8888/TCP	**LoLo Catcher** HTTP Web interface (www.optiform.com)	No Oficial
8888/TCP	**D2GS Admin Console** Telnet administration console for D2GS servers (Diablo 2)	No Oficial
8888/TCP	Earthland Relams 2 Server (AU1_2)	No Oficial
8889/TCP	Earthland Relams 2 Server (AU1_1)	No Oficial

9000/TCP	Buffalo LinkSystem Web access	No Oficial
9000/TCP	**DBGp**	No Oficial
9000/TCP	**SqueezeCenter** web server & streaming	No Oficial
9000/UDP	**UDPCast**	No Oficial
9001	Microsoft Sharepoint Authoring Environment	Oficial
9001	cisco-xremote router configuration	No Oficial
9001	**Tor** network default	No Oficial
9001/TCP	**DBGp** Proxy	No Oficial
9009/TCP,UDP	**Pichat Server**—Peer to peer chat software	Oficial
9030/TCP	**Tor** often used	No Oficial
9043/TCP	**WebSphere Application Server** Administration Console secure	No Oficial
9050/TCP	**Tor**	No Oficial
9051/TCP	**Tor**	No Oficial
9060/TCP	**WebSphere Application Server** Administration Console	No Oficial
9080/UDP	glrpc, **Groove Collaboration software** GLRPC	Oficial
9080/TCP	glrpc, **Groove Collaboration software** GLRPC	Oficial
9080/TCP	**WebSphere Application Server HTTP** Transport (port 1) **default**	No Oficial

9090/TCP	**Openfire** Administration Console	No Oficial
9090/TCP	**SqueezeCenter** control (CLI)	No Oficial
9091/TCP	**Openfire** Administration Console (SSL Secured)	No Oficial
9100/TCP	PDL Data Stream	Oficial
9101	**Bacula** Director	Oficial
9102	**Bacula** File Daemon	Oficial
9103	**Bacula** Storage Daemon	Oficial
9105/TCP,UDP	**Xadmin** Control Daemon	Oficial
9110/UDP	**SSMP** Message protocol	No Oficial
9119/TCP,UDP	**MXit** Instant Messenger	Oficial
9300/TCP	**IBM Cognos 8 SOAP** Business Intelligence and Performance Management	No Oficial
9418/TCP,UDP	git, **Git** pack transfer service	Oficial
9420/TCP	**MooseFS** distributed file system – master server to chunk servers	No Oficial
9421/TCP	**MooseFS** distributed file system – master server to clients	No Oficial
9422/TCP	**MooseFS** distributed file system – chunk servers to clients	No Oficial
9443/TCP	**WSO2 Web Services Application Server HTTPS** transport (Oficially *WSO2 Tungsten HTTPS*	Oficial

9443/TCP	**WebSphere Application Server HTTP** Transport (port 2) **default**	No Oficial
9535/TCP	mngsuite, **LANDesk** Management Suite Remote Control	Oficial
9535/TCP	BBOS001, **IBM Websphere Application Server** (WAS) High Avail Mgr Com	No Oficial
9535/UDP	mngsuite, **LANDesk** Management Suite Remote Control	Oficial
9800/TCP,UDP	**WebDAV** Source	Oficial
9800	**WebCT** e-learning portal	No Oficial
9875/TCP	**Club Penguin** Disney online game for kids	No Oficial
9898/TCP,UDP	MonkeyCom	Oficial
9898/TCP	Tripwire – File Integrity Monitoring Software	No Oficial
9996/TCP,UDP	**The Palace** "The Palace" Virtual Reality Chat software. – 5	Oficial
9999	**Hydranode**—edonkey2000 **TELNET** control	No Oficial
9999/TCP	**Lantronix** UDS-10/UDS100[43] **RS-485** to Ethernet Converter **TELNET** control	No Oficial
9999	Urchin Web Analytics	No Oficial
10000	**Webmin**—Web-based Linux admin tool	No Oficial
10000	**BackupExec**	No Oficial
10000	Ericsson Account Manager (avim)	No Oficial

10001/TCP	**Lantronix** UDS-10/UDS100[44] **RS-485** to Ethernet Converter **default**	No Oficial
10008/TCP,UDP	Octopus Multiplexer, primary port for the **CROMP protocol**, which provides a **platform-independent** means for communication of **objects** across a **network**	Oficial
10010/TCP	**Open Object Rexx (ooRexx)** rxapi daemon	Oficial
10017	AIX,NeXT, HPUX—rexd daemon control	No Oficial
10024/TCP	Zimbra smtp [mta]—to amavis from postfix	No Oficial
10025/TCP	Ximbra smtp [mta]—back to postfix from amavis	No Oficial
10050/TCP,UDP	**Zabbix**-Agent	Oficial
10051/TCP,UDP	**Zabbix**-Trapper	Oficial
10113/TCP,UDP	**NetIQ** Endpoint	Oficial
10114/TCP,UDP	**NetIQ** Qcheck	Oficial
10115/TCP,UDP	**NetIQ** Endpoint	Oficial
10116/TCP,UDP	**NetIQ** VoIP Assessor	Oficial
10200/TCP	**FRISK Software International**'s *fpscand* virus scanning daemon for Unix platforms **[5]**	No Oficial
10200–10204/TCP	**FRISK Software International**'s *f-protd* virus scanning daemon for Unix platforms **[6]**	No Oficial
10308	Lock-on: Modern Air Combat	No Oficial

10480	SWAT 4 Dedicated Server	No Oficial
11211	**memcached**	No Oficial
11235	Savage:Battle for Newerth Server Hosting	No Oficial
11294	Blood Quest Online Server	No Oficial
11371	**OpenPGP** HTTP **key server**	Oficial
11576	**IPStor** Server management communication	No Oficial
12012/TCP,UDP	**Audition Online Dance Battle**, Korea Server – Status/Version Check	No Oficial
12013/TCP,UDP	**Audition Online Dance Battle**, Korea Server	No Oficial
12035/UDP	**Linden Lab** viewer to sim	No Oficial
12345	**NetBus**—remote administration tool (often **Trojan horse**). Also used by **NetBuster**. Little Fighter 2 (TCP).	No Oficial
12975/TCP	LogMeIn **Hamachi** (VPN tunnel software; also port 32976)—used to connect to Mediation Server (bibi.hamachi.cc); will attempt to use **SSL** (TCP port 443) if both 12975 & 32976 fail to connect	No Oficial
12998–12999/UDP	**Takenaka RDI** Mirror World on SL	No Oficial
13000–13050/UDP	**Linden Lab** viewer to sim	No Oficial
13076/TCP	Default for **BMC Software CONTROL-M/Enterprise Manager** Corba communication, though often changed during installation	Oficial
13720/TCP,UDP	**Symantec NetBackup**—bprd (formerly **VERITAS**)	Oficial

13721/TCP,UDP	**Symantec NetBackup**—bpdbm (formerly **VERITAS**)	Oficial
13724/TCP,UDP	**Symantec** Network Utility—vnetd (formerly **VERITAS**)	Oficial
13782/TCP,UDP	**Symantec NetBackup**—bpcd (formerly **VERITAS**)	Oficial
13783/TCP,UDP	**Symantec** VOPIED protocol (formerly **VERITAS**)	Oficial
13785/TCP,UDP	**Symantec NetBackup** Database—nbdb (formerly **VERITAS**)	Oficial
13786/TCP,UDP	**Symantec** nomdb (formerly **VERITAS**)	Oficial
14439/TCP	**APRS UI-View Amateur Radio**[45] UI-WebServer	No Oficial
14552/TCP	**Lasso (programming language)** application service	No Oficial
14567/UDP	**Battlefield 1942** and mods	No Oficial
15000/TCP	**psyBNC**	No Oficial
15000/TCP	**Wesnoth**	No Oficial
15000/TCP	Kaspersky Network Agent	No Oficial
15000/TCP	hydap, Hypack **Hydrographic** Software Packages Data Acquisition	Oficial
15000/UDP	hydap, Hypack **Hydrographic** Software Packages Data Acquisition	Oficial
15567/UDP	**Battlefield Vietnam** and mods	No Oficial
15345/TCP,UDP	**XPilot** Contact	Oficial
16000/TCP	**shroudBNC**	No Oficial

16080/TCP	**Mac OS X Server** Web (HTTP) service with performance cache[46]	No Oficial
16384/UDP	Iron Mountain Digital online backup	No Oficial
16567/UDP	**Battlefield 2** and mods	No Oficial
18010/TCP	Super Dancer Online Extreme(SDO-X) – CiB Net Station Malaysia Server	No Oficial
18180/TCP	DART Reporting server	No Oficial
18200/TCP,UDP	**Audition Online Dance Battle**, AsiaSoft Thailand Server – Status/Version Check	No Oficial
18201/TCP,UDP	**Audition Online Dance Battle**, AsiaSoft Thailand Server	No Oficial
18206/TCP,UDP	**Audition Online Dance Battle**, AsiaSoft Thailand Server – FAM Database	No Oficial
18300/TCP,UDP	**Audition Online Dance Battle**, AsiaSoft SEA Server – Status/Version Check	No Oficial
18301/TCP,UDP	**Audition Online Dance Battle**, AsiaSoft SEA Server	No Oficial
18306/TCP,UDP	**Audition Online Dance Battle**, AsiaSoft SEA Server – FAM Database	No Oficial
18400/TCP,UDP	**Audition Online Dance Battle**, KAIZEN Brazil Server – Status/Version Check	No Oficial
18401/TCP,UDP	**Audition Online Dance Battle**, KAIZEN Brazil Server	No Oficial
18505/TCP,UDP	**Audition Online Dance Battle**, Nexon Server – Status/Version Check	No Oficial
18506/TCP,UDP	**Audition Online Dance Battle**, Nexon Server	No Oficial

18605/TCP,UDP	**X-BEAT** – Status/Version Check	No Oficial
18606/TCP,UDP	**X-BEAT**	No Oficial
19000/TCP,UDP	**Audition Online Dance Battle**, G10/alaplaya Server – Status/Version Check	No Oficial
19001/TCP,UDP	**Audition Online Dance Battle**, G10/alaplaya Server	No Oficial
19226/TCP	**Panda Software** AdminSecure Communication Agent	No Oficial
19283/TCP,UDP	K2 - KeyAuditor & KeyServer, **Sassafras Software Inc. Software Asset Management** tools	Oficial
19315/TCP,UDP	KeyShadow for K2 - KeyAuditor & KeyServer, **Sassafras Software Inc. Software Asset Management** tools	Oficial
19638/TCP	Ensim Control Panel	No Oficial
19771/TCP,UDP	**Softros LAN Messenger**	No Oficial
19813/TCP	4D database Client Server Communication	No Oficial
19880/TCP	**Softros LAN Messenger**	No Oficial
20000	**DNP** (Distributed Network Protocol), a protocol used in **SCADA** systems between communicating **RTU**'s and **IED**'s	Oficial
20000	**Usermin**, Web-based user tool	No Oficial
20014/TCP	DART Reporting server	No Oficial
20720/TCP	**Symantec i3** Web GUI server	No Oficial

22347/TCP,UDP	WibuKey, **WIBU-SYSTEMS AG Software protection** system	Oficial
22350/TCP,UDP	CodeMeter, **WIBU-SYSTEMS AG Software protection** system	Oficial
23073	Soldat Dedicated Server	No Oficial
23399	**Skype** Default Protocol	No Oficial
23513	**[7]** Duke Nukem Ports	No Oficial
24444	**NetBeans** integrated development environment	No Oficial
24465/TCP,UDP	Tonido Directory Server for **Tonido** which is a Personal Web app and peer-to-peer platform	Oficial
24554/TCP,UDP	**BINKP**, **Fidonet** mail transfers over **TCP/IP**	Oficial
24800	**Synergy**: keyboard/mouse sharing software	No Oficial
24842	**StepMania**: Online: ***Dance Dance Revolution*** Simulator	No Oficial
25888/UDP	**Xfire** (Firewall Report, UDP_IN) IP Address (206.220.40.146) resolves to gameservertracking.xfire.com. Use unknown.	No Oficial
25999/TCP	**Xfire**	No Oficial
26000/TCP,UDP	**id Software**'s ***Quake*** server	Oficial
26000/TCP	**CCP**'s **EVE Online** Online gaming MMORPG	No Oficial
26900/TCP	**CCP**'s **EVE Online** Online gaming MMORPG	No Oficial
26901/TCP	**CCP**'s **EVE Online** Online gaming MMORPG	No Oficial

27000/UDP	(through 27006) **id Software**'s ***QuakeWorld*** master server	No Oficial
27000/TCP	**FlexNet Publisher**'s License server (from the range of default ports)	No Oficial
27001/TCP	**FlexNet Publisher**'s License server (from the range of default ports)	No Oficial
27002/TCP	**FlexNet Publisher**'s License server (from the range of default ports)	No Oficial
27003/TCP	**FlexNet Publisher**'s License server (from the range of default ports)	No Oficial
27004/TCP	**FlexNet Publisher**'s License server (from the range of default ports)	No Oficial
27005/TCP	**FlexNet Publisher**'s License server (from the range of default ports)	No Oficial
27006/TCP	**FlexNet Publisher**'s License server (from the range of default ports)	No Oficial
27007/TCP	**FlexNet Publisher**'s License server (from the range of default ports)	No Oficial
27008/TCP	**FlexNet Publisher**'s License server (from the range of default ports)	No Oficial
27009/TCP	**FlexNet Publisher**'s License server (from the range of default ports)	No Oficial
27010	**Source engine** dedicated server port	No Oficial
27015	**GoldSrc** and **Source engine** dedicated server port	No Oficial
27374	**Sub7** default. Most **script kiddies** do not change from this.	No Oficial

27500/UDP	(through 27900) **id Software**'s ***QuakeWorld***	No Oficial
27888/UDP	**Kaillera** server	No Oficial
27900	(through 27901) **Nintendo Wi-Fi Connection**	No Oficial
27901/UDP	(through 27910) **id Software**'s ***Quake II*** master server	No Oficial
27960/UDP	(through 27969) **Activision**'s ***Enemy Territory*** and **id Software**'s ***Quake III Arena*** and *Quake III* and some ioquake3 derived games	No Oficial
28000	**Bitfighter** Common/default Bitfighter Server	No Oficial
28001	**Starsiege: Tribes** Common/default Tribes v.1 Server	No Oficial
28395/TCP	**www.SmartSystemsLLC.com** Used by Smart Sale 5.0	No Oficial
28910	**Nintendo Wi-Fi Connection**	No Oficial
28960/UDP	**Call of Duty** – **Call of Duty: United Offensive** – **Call of Duty 2** – **Call of Duty 4: Modern Warfare** – **Call of Duty: World at War** (PC Version)	No Oficial
29900	(through 29901) **Nintendo Wi-Fi Connection**	No Oficial
29920	**Nintendo Wi-Fi Connection**	No Oficial
30000	**Pokémon Netbattle**	No Oficial
30301	**BitTorrent**	No Oficial
30564/TCP	**Multiplicity**: keyboard/mouse/clipboard sharing software	No Oficial
31337/TCP	**Back Orifice**—remote administration tool (often **Trojan horse**)	No Oficial

31415	**ThoughtSignal**—Server Communication Service (often **Informational**)	No Oficial
31456/TCP	**TetriNET** IRC gateway on some servers	No Oficial
31457/TCP	**TetriNET**	Oficial
31458/TCP	**TetriNET** Used for game spectators	No Oficial
32245/TCP	**MMTSG-mutualed** over **MMT** (encrypted transmission)	No Oficial
32976/TCP	LogMeIn **Hamachi** (VPN tunnel software; also port 12975)—used to connect to Mediation Server (bibi.hamachi.cc); will attempt to use **SSL** (TCP port 443) if both 12975 & 32976 fail to connect	No Oficial
33434/TCP,UDP	**traceroute**	Oficial
34443	Linksys PSUS4 print server	No Oficial
37777/TCP	**Digital Video Recorder hardware**	No Oficial
36963	**Counter Strike 2D** multiplayer (2D clone of popular CounterStrike computer game)	No Oficial
40000/TCP,UDP	SafetyNET p **Real-time Industrial Ethernet** protocol	Oficial
43047/TCP	TheòsMessenger second port for service TheòsMessenger	Oficial
43594–43595/TCP	**RuneScape**	No Oficial
47808/TCP,UDP	**BACnet** Building Automation and Control Networks	Oficial
49151/TCP,UDP	Reserve	Oficial

ANEXO C

C. EVENTOS QUE SUCEDEN CUANDO SE PRESENTA UN ATAQUE

384: ICMP ping
Este evento se genera cuando un eco ICMP genérico es realizado. Un atacante puede intentar determinar que hosts están activos en una red antes de lanzar un ataque.

376: ICMP PING Microsoft Windows
Este evento se genera cuando un eco ICMP genérico es realizado desde un host Windows. De igual manera que en el evento 384, un atacante puede intentar determinar que hosts estan activos en una red antes de lanzar un ataque.

408: ICMP Echo Reply
Este evento se genera cuando un host de la red genera un eco de respuesta ICMP in respuesta al un mensaje petición del eco de ICMP. Un atacante remoto puede utilizar datagramas de la petición de eco ICMP para determinar los hosts activos n la red en preludio de otros ataques.

540: CHAT MSN message
Este evento se genera cuando una actividad referente a clientes chat de la red es detectada. Un atacante puede utilizar una vulnerabilidad en un cliente de mensajeria instantánea para acceder a un host, entonces cargar un programa Trojan Horse para ganar control sobre ese host.

1990: CHAT MSN user search
Este evento se genera cuando una actividad referente a clientes chat de la red es detectada. Al igual que en el evento 540, Un atacante puede utilizar una vulnerabilidad en un cliente de mensajeria instantánea para acceder a un host, entonces cargar un programa Trojan Horse para ganar control sobre ese host.

1411: SNMP public access UDP
Este evento se genera cuando una conexión del SNMP sobre UDP usando la comunidad “pública” por defecto es hecha. El SNMP (Simple Network Management Protocol) v1 utiliza comunidades y direcciones del IP para autenticar la comunicación entre el cliente SNMP y el administrador SNMP. Muchas puestas en práctica del SNMP vienen preconfiguradas con las comunidades “público” y “private”. Si éstos no son deshabilitados, el atacante puede recopilar información sobre los dispositivo que esta usando el administrador SNMP.

2003: MS-SQL Worm propagation attempt
Este evento se genera cuando una tentativa es hecha por el gusano “Slammer” que compromete a un servidor de Microsoft SQL. El gusano intenta explotar un desbordamiento del buffer en esta petición de la versión. Si el gusano envía demasiados bytes, una condición de desbordamiento del buffer se acciona dando por resultado una avenencia potencial con el servidor SQL.

1420: SNMP trap tcp
Este evento ocurre cuando se hace una conexión SNMP sobre TCP hacia un administrador SNMP. Un atacante puede intentar enviar esta petición para determinar si un dispositivo está utilizando SNMP.

1201: ATTACK-RESPONSES 403 Forbidden
Este evento se genera cuando un código de respuesta de error 403 es devuelto a un cliente por el Web Server.

Esto puede indicar una intención de acceso no autorizado a un Web Server o una aplicación corriendo en el mismo. Un atacante puede tener acceso al mecanismo de autentificación del sistema y proveer sus propias contraseñas para acceder.

1781: Sorry, no such sid-gen
Esta regla indica que una pagina que incluía temas de ”didlo” fue visitada.

1794: Sorry, no such sid-gen
Esta regla indica que una pagina que incluía temas de ”masturbación” fue visitada.

1841: WEB-CLIENT Javascript URL host spoofing attempt
Este evento se genera cuando un cliente dentro de la red probablemente ha visitado paginas que contienen código javascript malicioso. Sistemas afectados: versiones anteriores a Mozilla a 1.0.1 y versiones anteriores a Netscape 6.2.1

ANEXO D

D. GLOSARIO DE SIGLAS

ASN: Autonomous System Number
BSD: Berkeley Software Distribution
CPU: Central Processing Uni
DLL: Dynamic Link Library
FTP: File transfer protocol
FPU: Floating Point Unit
FAT32: File Allocation Table 32
GNU: General Public License
HPFS: High Performance File System
IAB: Internet Architecture Board
IP: Internet Protocol
ISO: International Organization for Standardization
LSB: Linux Standard Base
Minix: Unix Clone
NAT: Network Address Translation
NTFS: NT File System
POSIX: Portable Operating System Interface para UNIX
RFC: Request For Comments
SCO: Unix system intellectual property
SVR: Advanced Compatibility Package
STD: Security Tool Distro
TCP: Transmission Control Protocol

ANEXO E

E. DOCUMENTO DE APROBACIÓN DEL AUSPICIANTE