UNIVERSIDAD AMAZÓNICA DE PANDO
AREA CIENCIAS Y TECNOLOGÍA
CARRERA DE INGENIERÍA INFORMÁTICA

PROYECTO DE GRADO

“IMPLETACIÓN DE UN SERVIDOR PROXY PARA LA ADMINISTRACIÓN DE LA RED DE DATOS E INTERNET EN CONSULADO DEL BRASIL EN COBIJA”

INFORME FINAL DE PROYECTO DE GRADO PARA OPTAR AL TÍTULO DE LICENCIADO EN INGENIERÍA DE SISTEMAS INFORMÁTICOS

Postulante	**:**	**Univ. Néstor Méndez Apinayé**.
Tutor	**:**	**Lic. Milton Ramírez L.**
Asesor	**:**	**Ing. Alex Argandoña**

Cobija Pando Bolivia
2011

AGRADECIMIENTOS

A Dios

Por darme salud, vida y estar siempre presente en mis plegarias, en los momentos de Alegría, desesperación, agobio, logros, fracasos y cuando lo necesito, y nunca

A mi familia

Mi madrecita que siempre me brindo su apoyo cariño y comprensión, incondicionalmente
Mis hermanos por los buenos o malos momentos de mi vida, y que siempre están a mi lado.
A Yanira por brindarme todo su apoyo, amor y entendimiento.
Mi bebe por impulsarme de gran manera en mi vida y por ser el regalo más preciado que Dios me dio.

A mis docentes

Por los conocimientos e ideales impartidos durante todo el proceso de formación universitaria, además de compartir sus vivencias y brindar su amistad incondicional, a largo de esta etapa universitaria.
Al Lic. Milton Ramírez, Director del Área, Ing. Alex Argandoña, Lic. Juan C. Huanca, Ing. Tito Pons, por la enseñanza y colaboración brindada a mi persona desinteresadamente.
Al señor Eclair Soares de Frias Vice-Cónsul, por confiar y darme la oportunidad de realizar este proyecto de grado en la institución que ahora dirige.

A mis compañeros y amigos

A Rudy, Efraín, Pedro, compañeros de la MIC, por brindarme su amistad sincera y su colaboración desinteresada durante el trayecto de vida universitaria, y en el desarrollo del proyecto final
A todas las personas que de alguna manera contribuyeron e hicieron posible la realización de este proyecto de grado

DEDICATORIA

A mi madre Narcisa Apinayé, por el cariño que siempre me da, por impulsarme y apoyarme incondicionalmente en el proceso de mi formación profesional.

A mi bebe, que se ha convertido en la fuente de inspiración y motivación, durante esta etapa de mi vida y el desarrollo de este proyecto.

A mi abuelita Eufemia Trujillo, por haber contribuido en mi formación estudiantil y haberme inculcado siempre los grandes valores humanos, que aprendí a reconocer y valorar en el transcurso de mi vida universitaria y laboral.

RESUMEN

Durante el proceso de desarrollo del informe final del proyecto de grado, se emprendió la investigación sobre el tema de la administración de la Red de Datos e Internet, y la aplicabilidad en nuestro medio, para la implementación de un Servidor Proxy, de acuerdo al análisis que se realizo a los problemas presentados dentro del consulado determina que el problema principal es el *deficiente administración de la re de datos e internet en el consulado del Brasil en Cobija*, paro lo cual se plantea el objetivo principal que es la de Implementar un Servidor proxy, para la Administración de la Red de Datos e Internet del Consulado General del Brasil en Cobija, mediante la metodología del modelo funcional, permitiendo gestionar todo el ciclo de la administración desde su análisis, gestión, monitorización y la optimización para un crecimiento futuro, además de relacionar las actividades con los objetivos y la herramientas utilizadas.

En el desarrollo de la implementación, se hizo la reutilización de todos los recursos que cuenta la institución, garantizando de esta forma el buen funcionamiento de los sistemas de información existentes que trabajan directamente en línea con el (Itamaraty)[1].

Como resultado de la implementación del servidor, se obtiene mejoras en las atención al usuario requerente de un servicio, buena conexión a los sistemas existentes, ofreciendo diversos servicios de emitidos por esta institución de gran importancia en los que refleja lazos de hermandad buenas relaciones bilaterales con nuestro, quedando abierta la posibilidad de cambios o mejoras en el futuro.

[1] (Itamaraty: Nombre del palacio del Ministerio de Relaciones Exteriores del Brasil)

ÍNDICE

CAPITULO I

INTRODUCCIÓN

Pag.

CAPÍTULO II

MARCO TEÓRICO

CAPÍTULO III

EJECUCIÓN DEL PROYECTO

1.1. ANTECEDENTES Y MOTIVACIÓN

Con el avance tecnológico de la comunicación, también creció la inseguridad en navegación a sitios web, en la actualidad el Internet es muy utilizado por las grandes empresas, gobiernos, tomando en cuenta en el mundo actualmente funciona entrono a internet, para lo cual se hace presente la administración de redes que es definido como la suma total de todas las políticas y procedimientos que intervienen en la planeación, configuración, control, monitoreo de los elementos que conforman a una red con el fin de asegurar el eficiente y efectivo empleo de sus recursos. Lo cual se verá reflejado en la calidad de los servicios ofrecidos. Incrementando la eficiencia y productividad de las personas.

Para una administración de Redes de Datos (LAN)[1] e Internet en la actualidad todas las empresas y gobiernos en general han buscado mecanismos seguros ya que la gran mayoría de sus sistemas trabajan en línea, usando entre estos mecanismos los servidores proxy que tienen firewalls que nos brindan seguridad y han jugado un papel muy importante y trascendental en todo el mundo, brindando muchas ventajas y funcionalidades para la Administración de la Red de Datos e Internet.

El Consulado General del Brasil en Cobija, inicialmente no contaba con una red de datos ya que todos los tramites y documentos se hacían de forma manual, luego con los convenios internacionales respecto a la emisión de pasaportes biométricos, el Brasil comenzó a trabajar en sus propios sistemas de emisión de documentos, de tal forma luego de la implantación de estos servidores que trabajan directamente on-line, para autorizaciones por la autoridad consular, y por ese motivo se ve la necesidad de la implementación de una red, para la cual no existe la administración de una red de datos de control y monitoreo de la misma y para el Servicio de Internet, produciendo así constantemente saturaciones perdidas de información congestionamiento del ancho de banda del Servicio de Internet, a esto se suma las constantes fallas físicas de la red, y la falta de políticas de uso de la red.

[1] (Red de Datos Local)

Tomando en cuenta los aspectos y ventajas que nos da la administración de redes e Internet y por los problemas expuestos, en este proyecto de grado se plantea la implementación de un Servidor de administración y seguridad de datos para el Consulado General del Brasil en Cobija, el cual permitirá regularizar el tráfico de ancho de banda y restringirá el acceso a sitios web prohibidos, tomando en cuenta el control a cada equipo de manera individual, con el fin de tener una red de datos más optima y con una mejor administración de todos los recursos que interactúan entre usuarios haciendo uso de la metodología funcional.

Como impacto se considera un eficiente servicio de los usuarios administrativos como a la población usuaria tanto a sus nacionales como a extranjeros de los servicios de este Consulado considerando además la eficiente comunicación entre el (Itamaraty)[2] con esta Repartición Consular con otras, ancho de banda descongestionado y controlado.

1.2. PLANTEAMIENTO DEL PROBLEMA

Las causas del problema principal en la Red de Datos e Internet del consulado brasilero son: el crecimiento de la población estudiantil brasilera que migra a nuestra ciudad para poder estudiar, que debido a ello ha crecido los tramites de documentación en esta institución, cambio de categoría del Consulado desde el punto de vista estructural de la red por la inadecuada planificación, diseño e implementación de la red de datos actual, mal manejo del Internet por el personal de la institución ay que hacen un uso desmesurado del ancho de banda de la red, descarga desde un gestor p2p, como videos, músicas, imágenes y otros, falta de políticas de control, ya que se cuentan con los diferentes servicios que presta a los ciudadanos brasileños y extranjeros en general además que pasa hacer de un vice-Consulado a un Consulado General.

Por lo antes expuesto se identifica el siguiente problema principal:

"Deficiente Administración de la Red de Datos e Internet en el Consulado General del Brasil en Cobija."

Los efectos del problema nos llevan a distracción en el trabajo por parte del personal, saturación del ancho de banda, molestias de las autoridades por la lentitud del Internet,

[2] (Itamaraty: Nombre del palacio del Ministerio de Relaciones Exteriores del Brasil)

conflicto de IP, inseguridad en el acceso a la información requerida en el tiempo deseado, lo que genera en algunos momentos demora en: atención al solicitante de un servicio, informes retrasados, reportes de sistemas, y pérdidas económicas en el mantenimiento de la red.

1.3. SOLUCIÓN PROPUESTA

Es de implementar el servidor proxy para la administración de Red de Datos e Internet, para tener mejor funcionamiento de la red, en la que todos los usuarios estarán gestionados por el administrador, de acuerdo a su registro y prioridad asignada, evitando así disconformidad en la velocidad y seguridad de la red, también se contará con un monitoreo continuo de todos los sitios visitados por los usuarios registrados.

1.4. OBJETIVOS

1.4.1. Objetivo General

Implementar un Servidor Proxy, para la Administración de la Red de Datos e Internet del Consulado General del Brasil en Cobija, mediante la metodología del modelo funcional, para mejorar la administración de datos e Internet garantizando el buen funcionamiento de los sistemas de información.

1.4.2. Objetivos Específicos

- Realizar un diagnostico de todo el funcionamiento de la red de datos actual
- Elaborar el rediseño de estructura de la red de datos actual
- Implementar el servidor Proxy para la administración de la red de datos.
- Realizar las pruebas de funcionamiento de acuerdo al servidor
- Administrar las posibles fallas para corrección oportuna de las mismas.
- Elaborar políticas y normativas del uso y acceso a la red de datos y el servicio de Internet.

1.5. ALCANCES

El presente trabajo contempla la implementación de un servidor proxy, para la administración de la red de datos del Consulado General del Brasil en Cobija, se controlara el buen uso del ancho de banda, el monitoreo del tráfico entrante y saliente por usuario, bloqueo de categorías de la web como por ejemplo P2P (videos, música), Orkut, facebook, chat, youtube, etc., ya que congestionan el nacho de banda, con la reconfiguración del sistema de intercomunicación de las computadoras que comprende: la fácil ampliación de la red, para garantizar la conectividad a los sistemas de información como es el SCI y el SCEDV, de esta repartición, mantenimiento del sistema de red, con la finalidad brindar seguridad, integridad en la de las prestaciones en la red de datos de comunicación que permita reutilizar los recursos (Hardware y software) existentes, prestaciones como la conectividad constante en el sistema de comunicación entre el Itamaraty y este consulado, priorizar el acceso de usuarios a internet con la implementación un servidor Proxy, además de que se puntualiza considerables mejoras en la conectividad a la información más eficiente y eficaz en del servidor central del sistema integrado SCI en áreas donde se manejas de los siguientes módulos y sub módulos del sistema SCI y SCEDV, mejorando así el desempeño de todas esta áreas consulares del Consulado como ser:

- El manejo la renda Consular (reportes de todos los servicios emitidos y sus diferentes precios): mejorando el desempeño de las diferentes funcionalidades con rapidez, y exactitud tratándose del dinero recaudado envió luego al Banco del Brasil en Nueva York
- Servicios: Mejorando el control sobre los diversos servicios que a continuación se describen algunos de ellos

  - ✓ Legalizaciones de documentos
  - ✓ Reconocimientos de firmas
  - ✓ Autenticación de documentos
  - ✓ Registros de nacimientos
  - ✓ Procuraciones
  - ✓ Pasaportes

- ✓ Visas
- ✓ Lizzer Pazer
- ✓ Padip

Y muchos otros servicios que nos describen estos dos Sistemas.

Control de Stop: optimizando con rápidez y eficiencia los procesos en pedidos de materiales de stop, como pasaportes, etiquetas M1, adhesivas S1, PADIP, PASOF, etc. Siendo esta la única forma de hacer solicitudes para los diversos servicios prestados.

1.6. METODOLOGÍA Y HERRAMIENTAS UTILIZADAS

En la etapa de diagnostico de la red se utilizara los métodos cualitativos y cuantitativos, e instrumentos como ser: las encuestas, entrevistas, observación, y otros. (VER ANEXO 2)

Aunque existen tres dimensiones para una administración de red, que son modos eficientes para administrar una red es claro que cada una difiere de otra, por ejemplo la dimensión temporal tomaría más tiempo de lo estimado para el desarrollo de este proyecto, la temporal nos amplia a otras áreas en donde además se requerirá de mucho más tiempo para abarcar las áreas a las que hace mención respecto a la administración como los sistemas de información, aplicaciones y otros. Siendo de este modo por lo puntual y especifico la dimensión funcional porque sus procesos se puntualizan específicamente a la administración de una red de datos.

Se adopta la metodología del modelo Funcional para la Administración de Redes, basada en funciones, ya que divide la administración de red en áreas de procesos funcionales (configuración, rendimiento, fallas, contabilidad y seguridad), tomando en cuenta tres de los primeros cinco procesos, para dar solución a las necesidades inmediatas de mayor importancia abordadas en el presente proyectos, ya que el cuarto proceso se refiere a un proceso lucrativo por cada punto de acceso se cobra una determinada cantidad de dinero, y la institución en este sentido no hará ningún cobro a sus funcionarios por el uso de la red, ya sea por la adición o retiro de terminales a la red, y el quinto es un proceso de estudio ampliado, pero que de alguna forma se toma en cuenta con la elaboración de políticas de

uso de la red, definiendo de esta forma una estructura organizacional con funciones bien definidas nos ayuda cumplir estos procesos en base a la realización de actividades relacionadas con los objetivos y las herramientas utilizadas en el desarrollo del proyecto.

A continuación de describe el desarrollo de la metodología con los tres procesos a ser desarrollados en este proyecto.

1.6.1. Administración de la Configuración

Estas actividades son la planeación y diseño de la red; la instalación y administración del software; administración de hardware, y el aprovisionamiento. Por último se mencionan los procedimientos y políticas que pueden ser de ayuda para el desarrollo de esta área, limitando cada a tarea según se describe a continuación.

1.6.2. Administración del rendimiento

Tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo. Esto permitirá tomar las decisiones pertinentes de acuerdo al comportamiento encontrado. La administración del rendimiento se divide en 2 etapas: monitoreo y análisis

1.6.3. Administración de Fallas

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para restablecer la situación o minimizar el impacto de la falla.

El proceso de la administración de fallas consiste de distintas fases.

- Monitoreo de alarmas. Se realiza la notificación de la existencia de una falla y del lugar donde se ha generado. Esto se puede realizar con el auxilio de las herramientas basadas en el protocolo (SNMP)[3].
- Localización de fallas. Determinar el origen de una falla.
- Pruebas de diagnóstico. Diseñar y realizar pruebas que apoyen la localización de una falla.
- Corrección de fallas. Tomar las medidas necesarias para corregir el problema, una vez que el origen de la misma ha sido identificado.
- Administración de reportes. Registrar y dar seguimiento a todos los reportes generados por los usuarios o por el mismo administrador de la red. Una falla puede ser notificada por el sistema de alarmas o por un usuario que reporta algún problema.

[3] (Protocolo Simple de Administración de Red)

1.7. ORGANIZACIÓN DEL DOCUMENTO

Capítulo I: Es la etapa donde se establece la parte introductoria del proyecto de grado donde se describe la introducción, el problema, la solución propuesta, objetivos planteados, y la metodología utilizada y alcances

Capítulo II: Hace referencia a los fundamentos teóricos y conceptuales del tema, la metodología, herramientas y técnicas aplicadas en el desarrollo del presente Proyecto de Grado.

Capítulo III: En este capítulo se realiza la ejecución del proyecto en base a la metodología, sus etapas y actividades como ser el análisis previo, planeación del diseño de implementación, instalación y configuración, monitoreo y puesta en marcha del servicio.

Capítulo IV: Este capítulo refleja las conclusiones obtenidas del proyecto de grado, en base a los objetivos planteados en el primer capítulo manifestando el grado de alcance y las recomendaciones para mejorar o ampliar este servicio, dentro de la institución.

2.1. MARCO INSTITUCIONAL

Las reparticiones consulares del Brasil como Consulado General y Vice-Consulados, son destinadas primordialmente para brindar todas las asistencias consulares a los brasileros residentes en el exterior e a los turistas que tengan dificultades durante sus viajes a países extranjeros. Diferenciándose de la embajada, cuya naturaleza es típicamente diplomática que implica representar al Estado brasilero ante el Estado boliviano, promover relaciones de amistad e desenvolver relaciones políticas, económicas y comerciales, culturales y científicas entre los dos Estados.

El Consulado General del Brasil, fue creado en este departamento en épocas, coloniales épocas donde el oro negro cerrándolo años mas tardes, para la reapertura de sus puertas en junio de 1985 como Vice-Consulado del Brasil en Cobija y ocho meses más tarde comienza a brindar sus servicios tanto a sus compatriotas como a extranjeros, y luego de casi 25 años de funcionamiento ininterrumpidos y por decreto Supremo del gobierno del Brasil es elevado a la categoría es elevado de Consulado General, actualmente se encuentra ubicado en la Av. Tcnl. Enrique Fernández Cornejo Nº 096 – Centro.

En el consulado existen dos sistemas: uno es el SCI (Sistema Consular Integrado), mismo que interactúa con las distintas áreas de donde depende todos los servicios ofrecidos a la población en usuaria de los mismos, conectado a un total de 18 terminales en áreas como ser:

Área Consular (donde se emiten todos los actos notariales), Recepción de solicitudes (Web de solicitud para el público), y el SCEDV (Sistema de Control de Emisión de Documentos de Viajes), Comunicación de total confidencia pero por donde llegan todas las instrucciones y comunicaciones a este consulado, Contabilidad donde maneja los sistemas de (compras, descargos), además de contar con varios sistema On-line del Itamaraty, excepto por el sistema contable los demás hacen uso del servicio de internet ADSL, proveído por la empresa de telecomunicaciones (COTECO)[1], sufriendo constantes cortes por parte de la proveedora, y congestionamiento del ancho de banda por el uso inadecuado por los usuarios

[1] (Cooperativa de Teléfonos Cobija Ltda.)

administrativos de esta institución ocasionando problemas con el servicio del sistema de comunicación exclusivamente de confidencia total..

2.2. ADMINISTRACIÓN DE REDES

Según (Stoner-Wankel, 1989), la definición etimológica de la palabra Administración viene del latín “A4D” que significa Dirección - Tendencia y “MINISTERES” que significa subordinación u obediencia. Con la definición etimológica clara se puede deducir que la administración es el proceso de planear, organizar, dirigir, controlar los esfuerzos de los miembros de la organización y de aplicar los demás recursos de ella para alcanzar las metas establecidas.

Una vez conocida la definición de la administración se puede deducir que la administración de red de datos es el proceso de planificar, organizar, dirigir y controlar los recursos de tecnológicos de hardware (físicos) y software (lógicos) de una red de datos.

2.2.1. Tres dimensiones de la administración de redes

a) **Dimensión Funcional.** Se refiere a la asignación de tareas de administración por medio de áreas funcionales.

b) **Dimensión Temporal.** Se refiere a dividir el proceso de administración en diferentes fases cíclicas, incluyendo las fases de planeación, implementación y operación.

c) **Dimensión del escenario.** Se refiere al resto de los escenarios adicionales al de administración de redes, como son administración de sistemas, administración de aplicaciones, etc.

2.2.2. Dimensión Funcional

Existen diversas modelos sobre arquitecturas de administración de redes. Tanto el modelo TMN de la ITU como el modelo OSI-NM (Network Management) son modelos funcionales que dividen la administración de una red en áreas funcionales (configuración, fallas, desempeño, contabilidad y seguridad), definiendo de ésta forma una estructura organizacional con funciones bien definidas. De esto se deriva el nombre de modelos funcionales.

El presente trabajo se basa únicamente a lo que proponen los modelos funcionales mencionados.

2.2.3. Objetivos de una administración de Red

Según (Stoner-Wankel, 1989), a continuación se presenta un listado de los objetivos de una administración de red:

- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.
- Hacer uso eficiente de la red y utilizar mejor los recursos, como por ejemplo, el ancho de banda.
- Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan entender la información que circula en ella.
- Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios.

2.2.4. Funciones de un Administrador de Red

Según (Stoner-Wankel, 1989) define las cinco funciones de administración básica que son:

- **Configuración:** La configuración comprende las funciones de monitoreo y mantenimiento del estado de la red.
- **Fallas:** La función de fallas incluye la detección, el aislamiento y la corrección de fallas en la red.
- **Contabilidad:** La función de contabilidad permite el establecimiento de cargos a usuarios por uso de los recursos de la red.
- **Comportamiento:** La función de comportamiento mantiene el comportamiento de la red en niveles aceptables.
- **Seguridad:** La función de seguridad provee mecanismos para autorización, control de acceso, confidencialidad y manejo de claves.

2.3. REDES

Una red es un conjunto de dispositivos (a menudo denominados nodos) conectados por enlaces de un medio físico. Un nodo puede ser una computadora, una impresora, o

cualquier otro dispositivo capaz de enviar y/o recibir datos generados por otros nodos de la red. (Forouzan, 2006).

2.3.1. Redes de computadoras

Las redes de computadoras son un conjunto de equipos informáticos (computadoras) autónomos, interconectados entre sí, con la finalidad de compartir sus recursos de información así como los recursos de hardware, (Chapman, 2002).

2.3.2. Redes LAN

Las redes LAN suelen ser una red de propiedad privada, y conectar enlaces de una única oficina, edificio o campus, alcanza hasta unos cuantos kilómetros de extensión. Se usan para conectar computadoras personales o estaciones de trabajo, con objeto de compartir recursos e intercambiar información. (Forouzan, 2006).

Están restringidas en tamaño, lo cual significa que el tiempo de transmisión, en el peor de los casos, se conoce, lo que permite cierto tipo de diseños (deterministas) que de otro modo podrían resultar ineficientes. Además, simplifica la administración de la red, además que suelen emplear tecnología de difusión mediante un cable sencillo al que están conectadas todas las máquinas. Operan a velocidades entre 10 y 100 Mbps.

2.3.3. Cableado estructurado

Es el sistema colectivo de cables, canalizaciones, conectores, etiquetas, espacios y demás dispositivos que deben ser instalados para establecer una infraestructura de telecomunicaciones genérica en un edificio o campus. Las características e instalación de estos elementos se deben hacer en cumplimiento de estándares para que califiquen como cableado estructurado. El apego de las instalaciones de cableado estructurado a estándares trae consigo los beneficios de independencia de proveedor y protocolo (infraestructura genérica), flexibilidad de instalación, capacidad de crecimiento y facilidad de administración.

El **cableado estructurado** consiste en el tendido de cables en el interior de un edificio con el propósito de implantar una red de área local. Suele tratarse de cable de par trenzado de

cobre, para redes de tipo IEEE 802.3. No obstante, también puede tratarse de fibra óptica o cable coaxial.

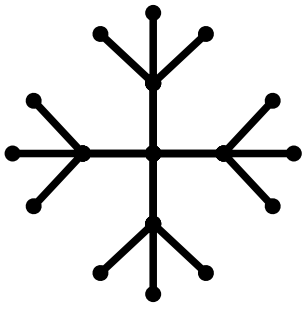
2.3.4. Topología física de red

El termino topología física se refiere a la forma en que está diseñada la red físicamente. La topología es la representación geométrica de la relación entre todos los enlaces y los dispositivos que se enlazan entre sí (habitualmente llamados nodos), hay cuatro posibles topologías básicas: Malla, estrella, bus y anillo. (Forouzan, 2006).

Para el presente proyecto de grado se opto por tomar la topología estrella la cual es explicada en el acápite 2.3.3.1.

2.3.3.1 Estrella extendida

Una topología en estrella extendida tiene una topología en estrella central, con cada uno de los nodos extremos de la topología en estrella, como se muestra en la figura 2.2 La ventaja es que hace que el cableado sea más corto y limita el número de dispositivos necesarios para interconectar cualquier nodo central. Una topología en estrella extendida es muy jerárquica y se puede configurar (con el equipo apropiado) para "animar" a que el trafico permanezca local. (Chapman, 2002),



Fuente: (Chapman, 2002)
Figura 2.1: Topología de red estrella extendida

2.3.5. Estándar TIA/EIA de cableado de red

De todas las organizaciones que existen en estándares, la TIA/EIA tiene el mayor impacto en las normas relacionadas con los medios de red. Específicamente, los estándares TIA/EIA-568-A y TIA/EIA-568-B han sido y continúan siendo las más ampliamente utilizadas para la actuación técnica de los medios de red, (Chapman, 2002).

Los estándares TIA/EIA especifican los requisitos mínimos para entornos de múltiples productos y de múltiples fabricantes. Permiten la planificación y la instalación de sistemas LAN sin dictar el uso de equipos específicos, de modo que dan a los diseñadores de LAN la libertad de crear opciones de mejora expansión.

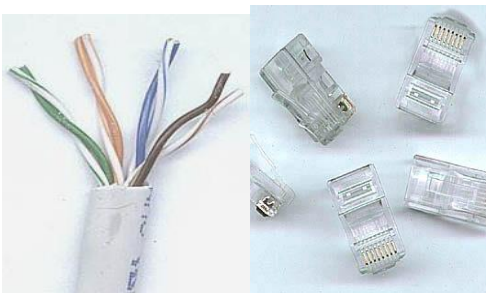
2.3.5.1. *TIA/EIA-568 A*

El Estándar TIA/EIA-568-A trata de seis elementos del proceso de cableado para una red LAN, Son los Siguientes:

- Cableado horizontal.
- Recintos de telecomunicaciones.
- Cableado del Backbone.
- Salas de equipamiento.
- Áreas de trabajo.
- Facilidades de entradas.

Al tomar en cuenta para este proyecto la reestructuración de la red en este proyecto eligiendo así el cableado horizontal definiendo el mismo como el cableado que se extiende desde una toma de telecomunicaciones hasta un conector transversal horizontal. Incluye los medios de red que recorren una ruta horizontal, la toma de telecomunicaciones o conector, las terminaciones mecánicas en el armario para el cableado y los cables de conmutación o jumper en el armario para el cableado. En resumen, el cableado horizontal incluye el medio de red que se utiliza en el área que va desde el armario para el cableado a una estación de trabajo.

El estándar TIA/EIA-568-A contiene especificaciones que rigen el rendimiento del cable. Requiere dos cables, uno para voz y otro para datos, por cada toma. De los dos cables, el de voz debe ser UTP de cuatro pares. El estándar TIA/EIA-568-A especifica cinco categorías de estas categorías la que se utilizo para la reestructuración es la categoría (CAT 5e), cable par trenzado sin apantallar UTP). Esta categoría fue la más recomendable para la aplicación de la instalación porque es la que se puede encontrar en el medio.



Fuente: (Martínez, 1997)
Figura 2.2: Cable UTP de categoría 5 y su conector RJ-45.

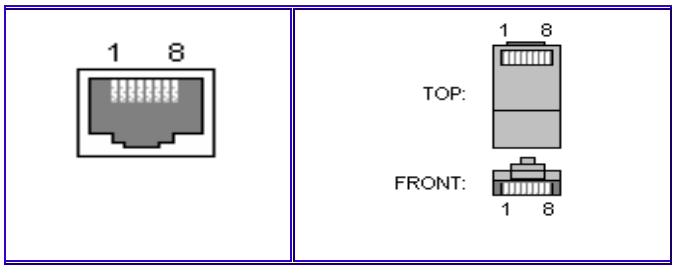
2.3.5.2. *Cable de Par trenzado sin apantallar*

Como muestra la figura 2.3, el cable de par trenzado sin apantallar (UTP) es un cable regular de cuatro pares de cables que se utiliza en un gran número de redes. En el cable UTP, el material aislante cubre cada uno de los ocho cables de cobre individuales. Además, los pares de cables están trenzados entre si. Este tipo de cable depende únicamente del efecto de cancelación, producido por los pares de cables trenzados, para limitar la degradación de la señal provocada por las EMI y las RFI. Para reducir más la diafonía entre los pares de cable UTP, el número de trenzas en los pares de cable varia. Cuando se utiliza una red media, el cable UTP tiene cuatro pares de hilo de cobre de calibre 22 o 24. El UTP tiene una impedancia de 100 Ohms. Como el UTP tiene un diámetro exterior de 0.43 cm. aproximadamente, su pequeño tamaño es una ventaja para las instalaciones. Debido a que el UTP se puede utilizar con la mayoría de las principales estructuras de red, sigue siendo el medio dominante para las LAN. (Chapman, 2002).

2.3.5.3. *Conectores RJ-45*

Los conectores que se usan más frecuentemente para UTP son los RJ-45 (RJ es por conector registrado), el conector es un conector de posición única los que significa que el conector se puede insertar de una sola forma, En la figura 2.4 se observa los tipos de conectores RJ-45, (Forouzan, 2006).

Hembra	Macho
Visto de frente	Conector visto de frente y desde arriba



Fuente: Fuente: (Martínez, 1997)
Figura 2.3: Conector RJ-45 hembra y macho.

2.3.6. Protocolos de comunicación

En las redes de computadoras, la comunicación se lleva a cabo entre distintas entidades de diferentes sistemas. Una entidad es cualquier cosa capaz de recibir y enviar información. Para que exista comunicación las entidades deben estar de acuerdo en un protocolo. Un protocolo es un conjunto de reglas que gobiernan la comunicación de datos. Un protocolo define que se comunica, como se comunica y cuando se comunica. Los elementos claves de un protocolo son su sintaxis, su semántica y su temporización, (Forouzan, 2006).

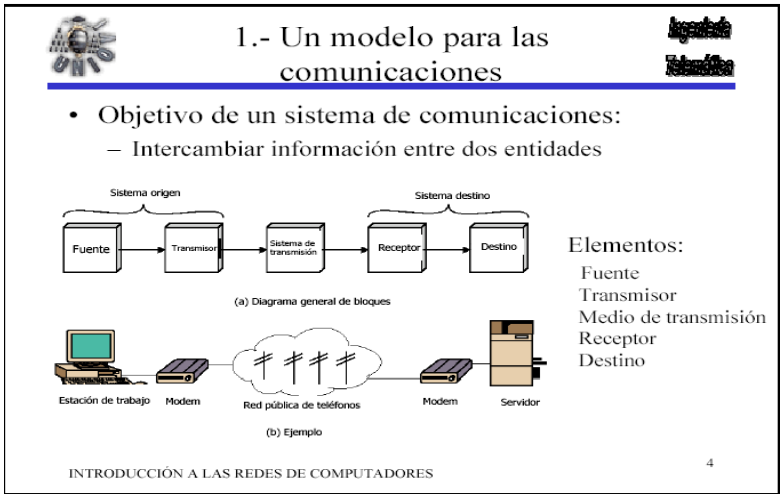


Figura 2.4: Modelo de Protocolo de Comunicación
Fuente: Fuente: (Martínez, 1997)

2.3.6.1. *Protocolo TCP/IP*

El nombre TCP/IP, proviene de dos protocolos importantes de la familia, el Protocolo de Control de Transmisión (TCP) y el Protocolo de Internet (IP). El TCP / IP es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos,

incluyendo PC, mini computadoras y computadoras centrales sobre redes de área local y área extensa, (Chávez, 2003).

2.3.6.1.1. *Capas del protocolo TCP/IP de internet*

El protocolo TCP/IP está organizado en cuatro capas conceptuales que se construyen sobre una quinta capa física o hardware. El siguiente esquema muestra las capas conceptuales así como la forma en que los datos pasan entre ellas, (Chávez, 2003).

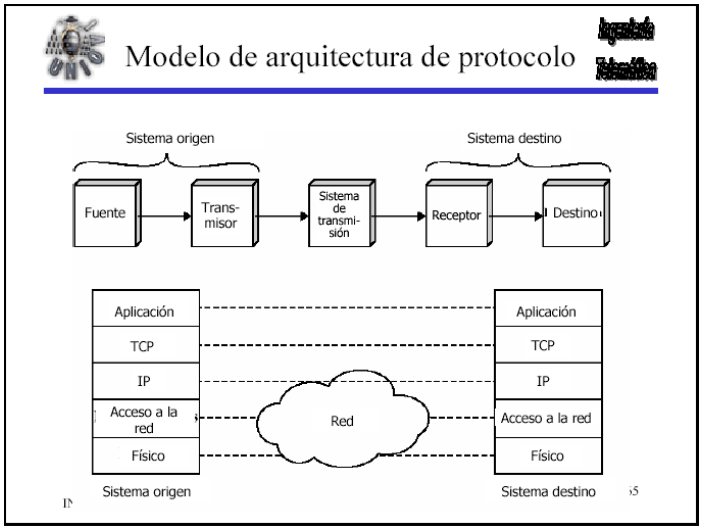


Figura 2.5: Modelo de Arquitectura del Protocolo TCP/IP
Fuente: Fuente: (Martínez, 1997)

2.3.6.1.2. *Ancho de banda de internet*

En conexiones a Internet el **ancho de banda** es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bits por segundo (bps), kilobits por segundo (Kbps), o megabits por segundo (Mbps).[1]

Para señales analógicas, el **ancho de banda** es la longitud, medida en Hz, del rango de frecuencias en el que se concentra la mayor parte de la potencia de la señal. Puede ser calculado a partir de una señal temporal mediante el análisis de Fourier. También son llamadas frecuencias efectivas las pertenecientes a este rango.

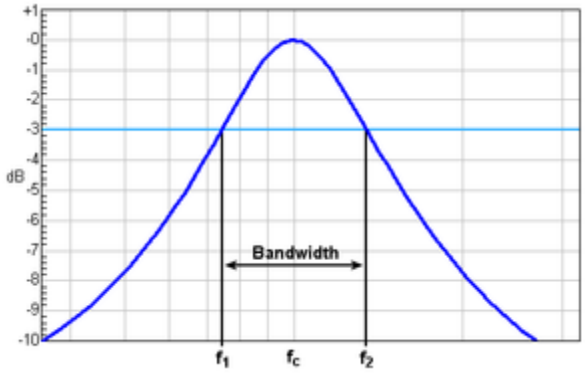


Figura 1.- El ancho de banda viene determinado por las frecuencias comprendidas entre f_1 y f_2.

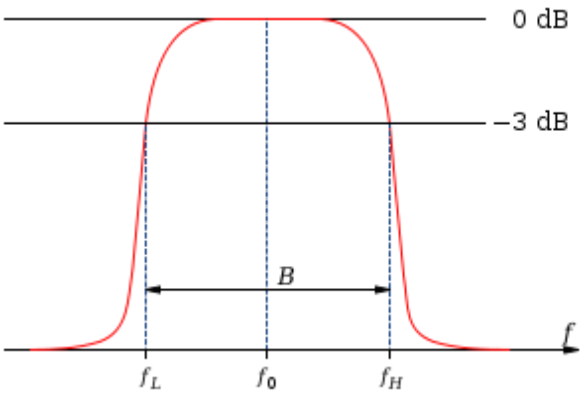
Así, el ancho de banda de un filtro es la diferencia entre las frecuencias en las que su atenuación al pasar a través de filtro se mantiene igual o inferior a 3 dB comparada con la frecuencia central de pico ($\mathbf{f_c}$) en la Figura 1.

La frecuencia es la magnitud física que mide las veces por unidad de tiempo en que se repite un ciclo de una señal periódica. Una señal periódica de una sola frecuencia tiene un ancho de banda mínimo. En general, si la señal periódica tiene componentes en varias frecuencias, su ancho de banda es mayor, y su variación temporal depende de sus componentes frecuenciales.

Normalmente las señales generadas en los sistemas electrónicos, ya sean datos informáticos, voz, señales de televisión, etc. son señales que varían en el tiempo y no son periódicas, pero se pueden caracterizar como la suma de muchas señales periódicas de diferentes frecuencias.

Uso común

Es común denominar *ancho de banda digital* a la cantidad de datos que se pueden transmitir en una unidad de tiempo. Por ejemplo, una línea ADSL de 256 kbps puede, teóricamente, enviar 256000 bits (no bytes) por segundo. Esto es en realidad la tasa de transferencia máxima permitida por el sistema, que depende del ancho de banda analógico, de la potencia de la señal, de la potencia de ruido y de la codificación de canal.



Un gráfico de la magnitud de ganancia de banda de un filtro, ilustrando el concepto de un ancho de banda de -3 dB a una ganancia de 0,707. Los ejes de frecuencia en el diagrama pueden ser a escala linear o logarítmica.

Un ejemplo de banda estrecha es la realizada a través de una conexión telefónica, y un ejemplo de banda ancha es la que se realiza por medio de una conexión DSL, microondas, cablemódem o T1. Cada tipo de conexión tiene su propio ancho de banda analógico y su tasa de transferencia máxima. El ancho de banda y la *saturación redil* son dos factores que influyen directamente sobre la calidad de los enlaces.

El rango de frecuencia que deja a un canal pasar satisfactoriamente se expresa en Hz.

Bw=Δf=fcs (frecuencia de corte superior) – fci (frecuencia de corte inferior)

También suele usarse el término ancho de banda de un bus de ordenador para referirse a la velocidad a la que se transfieren los datos por ese bus (véase Front-side bus), suele expresarse en bytes por segundo (B/s), Megabytes por segundo (MB/s) o Gigabytes por segundo (GB/s).

Se calcula multiplicando la frecuencia de trabajo del bus, en ciclos por segundo por el número de bytes que se transfieren en cada ciclo.

Por ejemplo, un bus que transmite 64 bits de datos a 266 MHz tendrá un ancho de banda de 2,1 GB/s.

Algunas veces se transmite más de un bit en cada ciclo de reloj, en este caso se multiplicará el número de bits por la cantidad de transferencias que se realizan en cada ciclo (MT/s).

Comúnmente, el ancho de banda que no es otra cosa que un conjunto de frecuencias consecutivas, es confundido al ser utilizado en líneas de transmisión digitales, donde es utilizado para indicar régimen binario o caudal que es capaz de soportar la línea.

2.3.7. Norma Ethernet 802.3u

Según la norma IEEE 802.3 (Ethernet), define un protocolo de comunicación conceptualmente dividido en dos partes. La primera de ellas es la capa MAC (Media Access Control) o de control de acceso al medio, que se ocupa de formatear la información para su transmisión y de arbitrar la forma en que los participantes de la red obtienen acceso a la misma. La segunda parte del protocolo Ethernet es la capa física que se ocupa de la comunicación entre la capa MAC y el cableado. En el caso de Ethernet hay diferentes implementaciones de la capa física, dadas las diferentes posibilidades de cableado (10Base5, 10Base2, 10Broad36, 10Base-F, 10Base-T y 1Base5), pero en todos los casos se emplea el mismo MAC CSMA/CD, (Chapman, 2002).

Es la norma que permite La norma Ethernet 802.3u tiene características propias las cuales son mostradas en la tabla 2.1

	Tipo de cable	**Conexión**	**Longitud máxima**	**º max. de estaciones**	**Observaciones**
10 base 2	Coaxial fino,50 ohmios RG58	BNC	185 m	30	conexión por "T" [Problema: hay que abrir la red] Líneas libres acabadas en tapones para evitar los rebotes
10 base T	Par trenzado	RJ-45 (ISO 8877).	100 m		Hub: Bus lógico en una caja y todas las estaciones colgando
100 base T	UTP cat. 5				

Fuente: Fuente: (Martínez, 1997)
Tabla 2.1: Norma Ethernet 802.3u

2.3.8. Direcciones IP, mascaras de red y clases de red

El protocolo de red IP utiliza direcciones formadas por números de 32 bits. Se le debe asignar un número único a cada máquina del entorno de red. Si está haciendo funcionar una red local que no tiene tráfico TCP/IP con otras redes, puede asignar estos números de acuerdo con sus preferencias personales. Hay algunos rangos de direcciones IP que han sido reservadas para redes privadas. De cualquier modo, los números para los sitios en Internet los asigna una autoridad central, el Network Information Center (NIC), (Dawson, 2000).

Para facilitar la lectura, las direcciones IP se separan en cuatro números de ocho bits llamados octetos. Por ejemplo, quark.physics.groucho.edu tiene una dirección IP 0x954C0C04, que se escribe como 149.76.12.4. Este formato se denomina normalmente notación de puntos divisorios.

Otra razón para usar esta notación es que las direcciones IP se dividen en un número de red, que es contenido en el octeto principal, y un número de puesto, que es contenido en el resto. Cuando se solicita al NIC una dirección IP, no se le asignará una dirección para cada puesto individual que pretenda usar. En cambio, se le otorgará un número de red y se le permitirá asignar todas las direcciones IP válidas dentro de ese rango para albergar puestos en su red de acuerdo con sus preferencias.

El tamaño de la parte dedicada al puesto depende del tamaño de la red. Para complacer diferentes necesidades, se han definido varias clases de redes, fijando diferentes sitios donde dividir la dirección IP. Las clases de redes se definen en lo siguiente:

2.3.8.1. Clases de Red

Las clases de red se dividen en 6, de las cuales 3 de ellas son las más utilizadas tal como se observa en la tabla 2.2, (Dawson, 2000):

- **La clase A:** comprende redes desde 1.0.0.0 hasta 127.0.0.0. El número de red está contenido en el primer octeto. Esta clase ofrece una parte para el puesto de 24 bits, permitiendo aproximadamente 1,6 millones de puestos por red.

- **La clase B:** comprende las redes desde 128.0.0.0 hasta 191.255.0.0; el número de red está en los dos primeros octetos. Esta clase permite 16.320 redes con 65.024 puestos cada una.
- **La clase C:** van desde 192.0.0.0 hasta 223.255.255.0, con el número de red contenido en los tres primeros octetos. Esta clase permite cerca de 2 millones de redes con más de 254 puestos.
- **Clases D, E, y F:** Las direcciones que están en el rango de 224.0.0.0 hasta 254.0.0.0 son experimentales o están reservadas para uso con propósitos especiales y no especifican ninguna red. La IP Multicast, un servicio que permite trasmitir material a muchos puntos en un internet a la vez, se le ha asignado direcciones dentro de este rango.

Clase	Redes
A	10.0.0.0 hasta 10.255.255.255
B	172.16.0.0 hasta 173.31.0.0
C	192.168.0.0 hasta 192.168.255.0

Fuente: Fuente: (Martínez, 1997)

Tabla 2.2: Clases y Rangos de Direcciones IP reservado para uso privado.

2.3.9. Equipos de red

2.3.9.1. *Routers*

El router es el principal dispositivo con el que se trabaja cuando se esta en la capa de red OSI, permite al router tomar decisiones basándose en las direcciones de red. Los routers también pueden conectar diferentes tecnologías, sin embargo, debido a su capacidad de **enrutar paquetes**, los routers se han convertido en el **backbone** de Internet, ejecutando el protocolo IP, (Chapman, 2002).

Fuente: (Chapman, 2002)

Figura 2.6: Símbolo del Router (Se observa flechas entrantes y salientes)

El propósito de un router es examinar los paquetes entrantes, elegir la mejor ruta para ellos a través de la red y después conmutarlos al mejor puerto de salida. Los routers son el dispositivo regulador de tráfico más importante en las redes grandes. Permiten que cualquier tipo de computadora se comunique con otra en cualquier parte del mundo.

Fuente: (mercado libre, 2005)
Figura 2.7: Router Cisco 1760 – 1600

2.3.9.2. *Hub*

En general, el termino hub se emplea en lugar de repetidor cuando se refiere al dispositivo que sirve como centro de la red, como se puede observar en la figura 2.9. Aunque un hub opera en una topología física en estrella, crea el mismo entorno de contención que un bus. Esto se debe a que cuando un dispositivo transmite, el resto de dispositivos le escuchan y la contención crea un bus lógico, (Chapman, 2002).

El propósito de un hub es regenerar y reenviar señales de red. Esto se hace a nivel de bits con gran número de host. Esta acción se conoce como concentración. Estas son las propiedades más importantes de un hub:

- Regenerar y repetir las señales.
- Propagar las señales por la red.
- No pueden filtrar el tráfico de la red.
- No pueden determinar la mejor ruta.
- Se utilizan como puntos de concentración de la red.

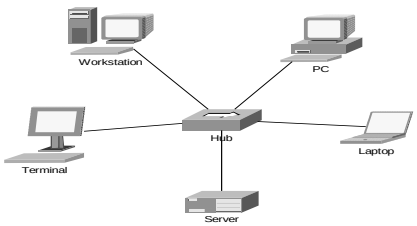
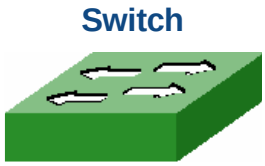


Figura 2.8: Símbolo del Hub (Se encuentra en el centro)
Fuente: electrónica

2.3.9.3. *Switch*

La diferencia entre un hub y un switch reside en lo que sucede en el interior del dispositivo el cual es que recibe y emite la información en el mismo instante. La figura 2.10 muestra el símbolo de un switch. Las flechas de la parte superior presentan los datos de rutas separadas que pueda haber en un switch, a diferencia del hub, donde los datos fluyen en todas las rutas, (Chapman, 2002),



Fuente: (Chapman, 2002)

Figura 2.9: Símbolo del Switch (Se observa flechas salientes)

2.3.9.4. *Patch Panels*

Los patch panels son agrupaciones de jacks RJ-45. Los hay de 12 y 48 puertos y normalmente están montados en racks (vease figura 11). Los lados anteriores son jacks RJ-45; los lados posteriores son bloques de empuje que proporcionan rutas de conectividad o de conexión. Se clasifican como componentes de la Capa 1.

Fuente: (mercado libre, 2005)
Figura 2.10: Patch Panels

2.4. SERVIDOR

2.4.1. Definición de un Servidor Proxy

Un **proxy**, en una red informática, es un programa o dispositivo que realiza una acción en representación de otro, esto es, si una hipotética máquina ***a*** solicita un recurso a una ***c***, lo

hará mediante una petición a ***b***; ***C*** entonces no sabrá que la petición procedió originalmente de ***a***. Su finalidad más habitual es la de **servidor proxy**, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

Un firewall o cortafuegos es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar o descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios (reglas).

2.4.2. Brevemente

- En Internet, un servidor es un ordenador remoto que provee los datos solicitados por parte de los navegadores de otras computadoras.
- En redes locales se entiende como el software que configura un PC como servidor para facilitar el acceso a la red y sus recursos.
- Los Servidores almacenan información en forma de páginas web y a través del protocolo HTTP lo entregan a petición de los clientes (navegadores web) en formato HTML.

2.4.3. Ventajas de las redes basadas en servidor

Aunque resulta más compleja de instalar, gestionar y configurar, una red basada en servidor tiene muchas ventajas sobre una red simple Trabajo en Grupo.

• Compartir recursos: Un servidor está diseñado para ofrecer acceso a muchos archivos e impresoras manteniendo el rendimiento y la seguridad de cara al usuario.

• La compartición de datos basada en servidor puede ser administrada y controlada de forma centralizada. Como estos recursos compartidos están localizados de forma central, son más fáciles de localizar y mantener que los recursos situados en equipos individuales.

• Seguridad: La seguridad es a menudo la razón primaria para seleccionar un enfoque basado en servidor en las redes. En un entorno basado en servidor, hay un administrador que define la política y la aplica a todos los usuarios de la red, pudiendo gestionar la seguridad.

• Copia de seguridad: Las copias de seguridad pueden ser programadas varias veces al día o una vez a la semana, dependiendo de la importancia y el valor de los datos. Las copias de seguridad del servidor pueden programarse para que se produzcan automáticamente, de acuerdo con una programación determinada, incluso si los servidores están localizados en sitios distintos de la red.

• Redundancia: Mediante el uso de métodos de copia de seguridad llamados sistemas de redundancia, los datos de cualquier servidor pueden ser duplicados y mantenidos en línea. Aun en el caso de que ocurran daños en el área primaria de almacenamiento de datos, se puede usar una copia de seguridad de los datos para restaurarlos.

• Número de usuarios: Una red basada en servidor puede soportar miles de usuarios. Este tipo de red sería, imposible de gestionar como red Trabajo en Grupo, pero las utilidades actuales de monitorización y gestión de la red hacen posible disponer de una red basada en servidor para grandes cifras de usuarios.

• Hardware: El hardware de los equipos cliente puede estar limitado a las necesidades del usuario, ya que los clientes no necesitan la memoria adicional (RAM) y el almacenamiento en disco necesarios para los servicios de servidor.

2.4.4. FIREWALL

Un firewall o cortafuegos son una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar o descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios (reglas).

2.5. MODELO FUNIONAL PARA ADMINISTRACION DE REDES DE DATOS.

Se sugiere la creación de las siguientes áreas funcionales para ser aplicadas en la administración de redes.

2.5.1. Administración de la configuración

A continuación se describen las actividades ubicadas dentro del proceso de la administración de la configuración. Estas actividades son la planeación y diseño de la red; la instalación y administración del software; administración de hardware, y el aprovisionamiento. Por último se mencionan los procedimientos y políticas que pueden ser de ayuda para el desarrollo de esta área.

2.5.1.1. Planeación y diseño de la red

La meta de esta actividad es satisfacer los requerimientos inmediatos y futuros de la red, reflejarlos en su diseño hasta llegar a su implementación.

El proceso de planeación y diseño de una red contempla varias etapas, algunas son:

a) Reunir las necesidades de la red. Las cuales pueden ser específicas o generales, tecnológicas, cuantitativas, etc. Algunas de las necesidades específicas y de índole tecnológico de una red pueden ser

- Multicast,
- Voz sobre IP (VoIP),
- Calidad de servicio (QoS), etc.

Algunas necesidades cuantitativas pueden ser

- Cantidad de nodos en un edificio
- Cantidad de switches necesarios para cubrir la demanda de nodos.

Este tipo de requerimientos solamente involucran una adecuación en el diseño de la red, no requiere de un rediseño completo, en el caso de alguna necesidad más general puede requerir de un cambio total en la red ya que en estos casos los cambios afectan a gran parte del diseño. Una necesidad general, por ejemplo, se presenta cuando se desea la

implementación de nuevas tecnologías de red como el cambiar de ATM a GigabitEthernet, o cambiar los protocolos de ruteo interno.

b) Diseñar la topología de la red
c) Determinar y seleccionar la infraestructura de red basada en los requerimientos técnicos y en la topología propuesta.
d) Diseñar, en el caso de redes grandes, la distribución del tráfico mediante algún mecanismo de ruteo, estático o dinámico.

e) Si el diseño y equipo propuesto satisfacen la necesidades, se debe proceder a planear la implementación, en caso contrario, repetir los pasos anteriores hasta conseguir el resultado esperado.

2.5.1.2. Selección de la infraestructura de red

Esta selección se debe realizar de acuerdo a las necesidades y la topología propuesta. Si se propuso un diseño jerárquico, se deben seleccionar los equipos adecuados para las capas de acceso, distribución y núcleo (core). Además, la infraestructura debe cumplir con la mayoría de las necesidades técnicas de la red. Lo más recomendable es hacer un plan de pruebas previo al cual deben ser sujetos todos los equipos que pretendan ser adquiridos.

2.5.1.3. Instalaciones y administración del hardware

Las tareas de instalación de hardware contemplan, tanto la agregación como la sustitución de equipamiento, y abarcan un dispositivo completo, como un switch o un ruteador; o solo una parte de los mismos, como una tarjeta de red, tarjeta procesadora, un módulo, etc. El proceso de instalación consiste de las siguientes etapas:

- Realizar un estudio previo para asegurar que la parte que será instalada es compatible con los componentes ya existentes.
- Definir la fecha de ejecución y hacer un estimado sobre el tiempo de duración de cada paso de la instalación.
- Notificar anticipadamente a los usuarios sobre algún cambio en la red.

- Generalmente, a toda instalación de hardware corresponde una instalación o configuración en la parte de software, entonces es necesario coordinar esta configuración.
- Generar un plan alterno por si la instalación provoca problemas de funcionalidad a la red.
- Realizar la instalación procurando cumplir con los límites temporales previamente establecidos.
- Documentar el cambio para futuras referencias.

2.5.1.4. Instalación del software

Es la actividad responsable de la instalación, desinstalación y actualización de una aplicación, sistema operativo o funcionalidad en los dispositivos de la red. Además, de mantener un control sobre los programas que son creados para obtener información específica en los dispositivos.

Antes de realizar una instalación, se debe tomar en cuenta lo siguiente.

Que las cantidades de memoria y almacenamiento sean suficientes para la nueva entidad de software.

Asegurar que no exista conflicto alguno, entre las versiones actuales y las que se pretenden instalar.

Otra actividad importante es el respaldo frecuente de las configuraciones de los equipos de red ya que son un elemento importante que requiere especial cuidado. Estos respaldos son de mucha utilidad cuando un equipo se daña y tiene que ser reemplazado ya que no es necesario realizar la configuración nuevamente, lo que se hace es cargar las configuraciones al dispositivo mediante un servidor de tftp.

2.5.1.5. Aprovisionamiento

Esta tarea tiene la función de asegurar la redundancia de los elementos de software y hardware más importantes de la red. Puede llevarse a cabo en diferentes niveles, a nivel de la red global o de un elemento particular de la red. Es la responsable de abastecer los recursos necesarios para que la red funcione, elementos físicos como conectores, cables, multiplexores, tarjetas, módulos, elementos de software como versiones de sistema

operativo, parches y aplicaciones. Además de hacer recomendaciones para asegurar que los recursos, tanto de hardware como de software, siempre se encuentren disponibles ante cualquier eventualidad.

Algunos elementos de hardware más importantes como son: tarjetas procesadoras, fuentes de poder, módulos de repuesto, equipos para sustitución y un respaldo de cada uno de ellos.

2.5.1.6. Políticas y procedimientos relacionados

En este apartado se recomienda realizar, entre otros, los siguientes procedimientos y políticas.

Procedimiento de instalación de aplicaciones más utilizadas.
Políticas de respaldo de configuraciones.
Procedimiento de instalación de una nueva versión de sistema operativo.

2.5.2. Administración del rendimiento

Tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo. Esto permitirá tomar las decisiones pertinentes de acuerdo al comportamiento encontrado.

La administración del rendimiento se divide en 2 etapas: monitoreo y análisis.

2.5.2.1. Monitoreo

El monitoreo consiste en observar y recolectar la información referente al comportamiento de la red en aspectos como los siguientes:

a) Utilización de enlaces

Se refiere a las cantidades ancho de banda utilizada por cada uno de los enlaces de área local (Ethernet, Fastethernet, GigabitEthernet, etc), ya sea por elemento o de la red en su conjunto.

b) Caracterización de tráfico.

Es la tarea de detectar los diferentes tipos de tráfico que circulan por la red, con el fin de obtener datos sobre los servicios de red, como http, ftp, que son más utilizados. Además, esto también permite establecer un patrón en cuanto al uso de la red.

c) Porcentaje de transmisión y recepción de información.

Encontrar los elementos de la red que más solicitudes hacen y atienden, como servidores, estaciones de trabajo, dispositivos de interconexión, puertos y servicios.

d) Utilización de procesamiento

Es importante conocer la cantidad de procesador que un servidor esta consumiendo para atender una aplicación.

Esta propuesta considera importante un sistema de recolección de datos en un lugar estratégico dentro de la red, el cual puede ser desde una solución comercial como Spectrum o la solución propia de la infraestructura de red, hasta una solución integrada con productos de software libre.

2.5.2.2. Análisis

Una vez recolectada la información mediante la actividad de monitoreo, es necesario interpretarla para determinar el comportamiento de la red y tomar decisiones adecuadas que ayuden a mejorar su desempeño.

En el proceso de análisis se pueden detectar comportamientos relacionados a lo siguiente:

a) Utilización elevada.

Si se detecta que la utilización de un enlace es muy alta, se puede tomar la decisión de incrementar su ancho de banda o de agregar otro enlace para balancear las cargas de tráfico. También, el incremento en la utilización, puede ser el resultado de la saturación por tráfico generado maliciosamente, en este caso de debe contar con un plan de respuesta a incidentes de seguridad.

b) Tráfico inusual.

El haber encontrado, mediante el monitoreo, el patrón de aplicaciones que circulan por la red, ayudará a poder detectar tráfico inusual o fuera del patrón, aportando elementos importantes en la resolución de problemas que afecten el rendimiento de la red.

c) Elementos principales de la red.

Un aspecto importante de conocer cuáles son los elementos que más reciben y transmiten, es el hecho de poder identificar los elementos a los cuales establecer un monitoreo más constante, debido a que seguramente son de importancia. Además, si se detecta un elemento que generalmente no se encuentra dentro del patrón de los equipos con más actividad, puede ayudar a la detección de posibles ataques a la seguridad de dicho equipo.

d) Calidad de servicio.

Otro aspecto, es la Calidad de servicio o QoS, es decir, garantizar, mediante ciertos mecanismos, las condiciones necesarias, como ancho de banda, retardo, a aplicaciones que requieren de un trato especial, como lo son la voz sobre IP (VoIP), el video sobre IP mediante H.323, etc.

e) Control de tráfico.

El tráfico puede ser reenviado o ruteado por otro lado, cuando se detecte saturación por un enlace, o al detectar que se encuentra fuera de servicio, esto se puede hacer de manera automática si es que se cuenta con enlaces redundantes.

Si las acciones tomadas no son suficientes, éstas se deben reforzar para que lo sean, es decir, se debe estar revisando y actualizando constantemente.

2.5.2.3. Interacción con otras áreas

La administración del rendimiento se relaciona con la administración de fallas cuando se detectan anomalías en el patrón de tráfico dentro de la red y cuando se detecta saturación en los enlaces. Con la administración de la seguridad, cuando se detecta tráfico que es generado hacia un solo elemento de la red con más frecuencia que la común. Y con la administración de la configuración, cuando ante una falla o situación que atente contra el

rendimiento de la red, se debe realizar alguna modificación en la configuración de algún elemento de la red para solucionarlo.

2.5.3. Administración de fallas

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para restablecer la situación o minimizar el impacto de la falla.

El proceso de la administración de fallas consiste de distintas fases.

- *Monitoreo de alarmas.* Se realiza la notificación de la existencia de una falla y del lugar donde se ha generado. Esto se puede realizar con el auxilio de las herramientas basadas en el protocolo SNMP.
- *Localización de fallas.* Determinar el origen de una falla.
- *Pruebas de diagnóstico.* Diseñar y realizar pruebas que apoyen la localización de una falla.
- *Corrección de fallas.* Tomar las medidas necesarias para corregir el problema, una vez que el origen de la misma ha sido identificado.
- *Administración de reportes.* Registrar y dar seguimiento a todos los reportes generados por los usuarios o por el mismo administrador de la red.

Una falla puede ser notificada por el sistema de alarmas o por un usuario que reporta algún problema.

2.5.3.1. Monitoreo de alarmas

Las alarmas son un elemento importante para la detección de problemas en la red. Es por eso que se propone contar con un sistema de alarmas, el cual es una herramienta con la que el administrador se auxilia para conocer que existe un problema en la red. También conocido como sistema de monitoreo, se trata de un mecanismo que permite notificar que

ha ocurrido un problema en la red. Esta propuesta se basa en la utilización de herramientas basadas en el protocolo estándar de monitoreo, (SNMP)[2], ya que este protocolo es utilizado por todos los fabricantes de equipos de red.

Cuando una alarma ha sido generada, ésta debe ser detectada casi en el instante de haber sido emitida para poder atender el problema de una forma inmediata, incluso antes de que el usuario del servicio pueda percibirla.

Las alarmas pueden ser caracterizadas desde al menos dos perspectivas, su tipo y su severidad.

2.5.3.2. Tipos de las alarmas

- Alarmas en las comunicaciones. Son las asociadas con el transporte de la información, como las pérdidas de señal.
- Alarmas de procesos. Son las asociadas con las fallas en el software o los procesos, como cuando el procesador de un equipo excede su porcentaje normal.
- Alarmas de equipos. Como su nombre lo indica, son las asociadas con los equipos. Una falla de una fuente de poder, un puerto, son algunos ejemplos.
- Alarmas ambientales. Son las asociadas con las condiciones ambientales en las que un equipo opera. Por ejemplo, alarmas de altas temperaturas.
- Alarmas en el servicio. Relacionadas con la degradación del servicio en cuanto a límites predeterminados, como excesos en la utilización del ancho de banda, peticiones abundantes de icmp.

2.5.3.3. Severidad de las alarmas

- Crítica. Indican que un evento severo ha ocurrido, el cual requiere de atención inmediata. Se les relaciona con fallas que afectan el funcionamiento global de la red. Por ejemplo, cuando un enlace importante está fuera de servicio, su inmediato restablecimiento es requerido.

[2] (Protocolo Simple de Administración de Red)

- Mayor. Indica que un servicio ha sido afectado y se requiere su inmediato restablecimiento. No es tan severo como el crítico, ya que el servicio se sigue ofreciendo aunque su calidad no sea la óptima.
- Menor. Indica la existencia de una condición que no afecta el servicio pero que deben ser tomadas las acciones pertinentes para prevenir una situación mayor. Por ejemplo, cuando se alcanza cierto límite en la utilización del enlace, no indica que el servicio sea afectado, pero lo será si se permite que siga avanzando.

2.5.3.4. Localización de fallas

Este segundo elemento de la administración de fallas es importante para identificar las causas que han originado una falla. La alarma indica el lugar del problema, pero las pruebas de diagnóstico adicionales son las que ayudan a determinar el origen de la misma. Una vez identificado el origen, se tienen que tomar las acciones suficientes para reparar el daño.

2.5.3.5. Pruebas de diagnósticos

Las pruebas de diagnóstico son medios importantes para determinar el origen de una falla. Algunas de estas pruebas de diagnóstico que se pueden realizar son:

- Pruebas de conectividad física.

Son pruebas que se realizan para verificar que los medios de transmisión se encuentran en servicio, si se detecta lo contrario, tal vez el problema es el mismo medio.

- Pruebas de conectividad lógica.

Son pruebas que ofrecen una gran variedad, ya que pueden ser punto a punto, o salto por salto. Las pruebas punto a punto se realizan entre entidades finales, y las salto por salto se realizan entre la entidad origen y cada elemento intermedio en la comunicación. Los comandos usualmente utilizados son “ping” y “traceroute”.

2.5.3.6. Corrección de fallas

Es la etapa donde se recuperan las fallas, las cuales pueden depender de la tecnología de red. En esta propuesta solo se mencionan las prácticas referentes a las fallas al nivel de la red.

Entre los mecanismos más recurridos, y que en una red basada en interruptores son aplicables, se encuentran los siguientes.

- Reemplazo de recursos dañados. Hay equipos de red que permiten cambiar módulos en lugar de cambiarlo totalmente.
- Aislamiento del problema. Aislar el recurso que se encuentra dañado y que, además, afecta a otros recursos es factible cuando se puede asegurar que el resto de los elementos de la red pueden seguir funcionando.
- Redundancia. Si se cuenta con un recurso redundante, el servicio se cambia hacia este elemento.
- Recarga del sistema. Muchos sistemas se estabilizan si son reiniciados.
- Instalación de software. Sea una nueva versión de sistema operativo, una actualización, un parche que solucione un problema específico, etc.
- Cambios en la configuración. También es algo muy usual cambiar algún parámetro en la configuración del elemento de la red.

2.5.3.7. Administración de reportes

Es la etapa de documentación de las fallas. Cuando un problema es detectado o reportado, se le debe asignar un número de reporte para su debido seguimiento, desde ese momento un reporte queda abierto hasta que es corregido.

El ciclo de vida de la administración de reportes se divide en cuatro áreas, de acuerdo a la recomendación X.790 de la ITU-T

2.5.3.8. Creación de reportes

Un reporte es creado después de haber recibido una notificación sobre la existencia de un problema un problema en la red, ya sea por una alarma, una llamada telefónica de un

usuario, por correo electrónico o por otros medios. Cuando se crea un reporte de be contener al menos la siguiente información:

- El nombre de la persona que reportó el problema
- El nombre de la persona que atendió el problema o que creó el reporte del mismo.
- Información técnica para ubicar el área del problema
- Comentarios acerca de la problemática.
- Fecha y hora del reporte.

2.5.3.9. Seguimientos de reportes

La administración de reportes debe permitir al administrador dar seguimiento de cada acción tomada para solucionar el problema, y conocer el estado histórico y actual del reporte. Para cada reporte debe mantenerse un registro de toda la información relacionada al mismo: pruebas de diagnóstico, como fue solucionado el problema, tiempo que llevó la solución, etc, y este debe poder ser consultada en cualquier momento por el administrador.

2.5.3.10. Manejo de reportes

El administrador debe ser capaz de tomar ciertas acciones cuando un reporte está en curso, como escalar el reporte, solicitar que sea cancelado un reporte que no ha sido cerrado aún, poder hacer cambios en los atributos del reporte, como lo es el teléfono de algún contacto, poder solicitar hora y fecha de la creación o finalización de un reporte, etc.

2.5.3.11. Finalización de reportes

Una vez que el problema reportado ha sido solucionado, el administrador o la gente responsable del sistema de reportes, debe dar por cerrado el reporte. Una práctica importante, es que antes de cerrar un reporte el administrador debe asegurarse que efectivamente el problema reportado ha sido debidamente corregido.

Para llevar a cabo la implementación del servidor proxy para la administración de redes de datos, y la realización del esquema estructural de todo el cableado de la red del Consulado General del Brasil en Cobija, se está haciendo seguimiento a la metodología funcional para la administración de redes, el cual se describió de manera detallada en el capítulo anterior, para el análisis implementaciones utilizo las herramientas como encuestas, observación y el diseño lógico de la red.

3.1. FASE DE ANÁLISIS Y DIAGNÓSTICO

En esta fase se realizara el análisis y diagnóstico, ya que por el aumento de equipos y peticiones de conexiones a internet, también creció la dificulta para esquematizar la red LAN, en la que se optó, realizar el diseño del esquema de la red, utilizando la metodología funcional para la administración de redes, también las encuestas, para así hacer el estudio del uso de Red de datos e internet, con los datos adquiridos describir el funcionamiento debido de la red y la descripción de cada usuario que este en la red LAN.

3.1.1. Diagnóstico de la Red de datos y uso de Internet actual

Se realizó el levantamiento de datos vía encuesta para diagnosticar el uso actual de la Red de datos e internet, fueron encuestados los funcionarios que tienen acceso a la red, para así poner tener un diagnostico actual de las problemáticas e inquietudes de cada usuario que gozan de este servicio.

a) Evaluación previa de la situación actual de la red de datos

Para realizar esta actividad es necesario hacer una descripción de la situación actual de la red de datos y sus prestaciones que hacen uso de la misma, situación que explicamos a continuación observando el siguiente plano físico sobre la red en las figuras 3.1 y 3.2.

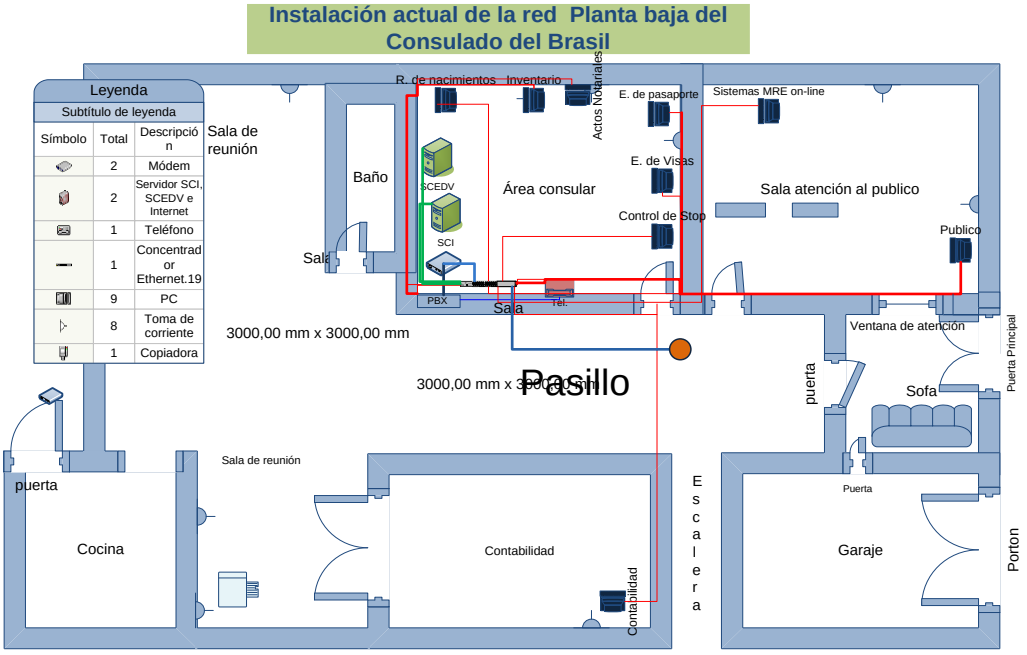


Figura 3.1: Croquis físico de la instalación actual de la red (planta baja)
Fuente: Elaboración propia

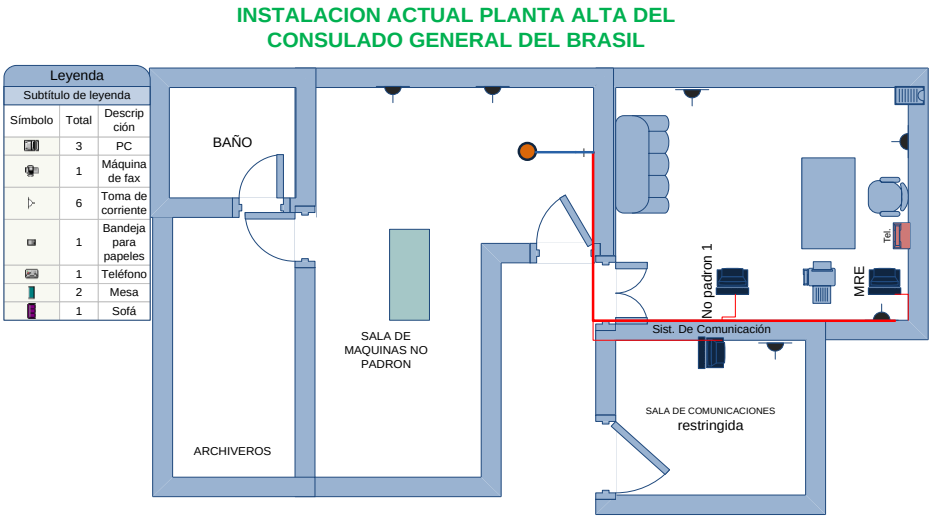


Figura 3.2: Croquis físico de la instalación actual de la red (planta alta)
Fuente: Elaboración propia

Antes de la implementación del los servidores y los diferentes servicios en el consulado existía una conexión a internet Dual-up, por medio de dos líneas telefónicas la cual servía para intercomunicar la terminal de comunicaciones por la cual llegan todas los telegramas

circulares, despachos telegráficos y otros. Además de dos máquina para el acceso de sistemas Web de dominios mre.gov.br.

En la planta baja figura 3.1, del consulado observamos los dos servidores y un total de 9 terminales, un router marca Broadband que establece la conexión a internet adsl, un Switch encoré D-Link, modelo DES-1016D, por el cual se conectan a la red todas las terminales, las cuales tienen IP con acceso a internet las mismas que son asignadas por medio de la configuración DHCP del mismo router, a la vez estas terminales se distribuyen en tres áreas: Consular, que es donde se procesa toda la infamación requerida de los solicitantes, las distintas terminales hacen uso de los servidores para solicitar y llenar los distintos servicios como ser, pasaportes (comunes, oficiales, diplomáticos, y de emergencias), visas, actos notariales, registro de nacimientos, de matrimonios, y otros. Los servidores tanto del SCI y el SCEDV, trabajan vía internet con los servidores centrales SERPRO en Brasilia, empresa encargada del desarrollo de los sistemas, la misma da acceso a estos servidores por medio de una IP fija, siendo un modo seguro de conexión según sus políticas de interfaz con las distintas reparticiones diplomáticas en todo el mundo, haciendo una copia de todos los servicios realizados almacenándolos en sus bases de datos en los servidores locales, una maquina pública con todas las restricciones debidas ya que por medio de una página Web por la cual el solicitante hace su respectiva solicitud de un servicio de los antes mencionados.

Para la planta alta figura 3.2, solo observamos tres terminales. la no padrón mediante la cual la autoridad consular autoriza previa revisión de un servicio requerido autorizaciones que se dan en coordinación con el (Itamaraty)[1], una terminal para los sistemas gubernamentales, y la máquina de comunicaciones, las cuales también están conectadas a la red por el mismo switch de 16 puertos de la planta baja.

Además de compartir los dispositivos de hardware que se encuentran instalados y configurados en los dos servidores mencionados que imprimen y escanean los diferentes documentos necesarios para cada proceso, dichos dispositivos son los siguientes:

[1] (Itamaraty: Nombre del palacio del Ministerio de Relaciones Exteriores del Brasil)

Dispositivos	Marca	cantidad
Impresora	Hp color LaserJet 3600n	1
Scanner	ICE 9600*4800, 48 bit color	1

Tabla 3.1. Dispositivos compartidos en red
Fuente: Elaboración propia

Por estas razones se da la implementación de una pequeña red LAN sin previa planificación y sin una estructurara adecuada, jalando los cables de la red por los pisos pegados a la pared mediante cinta Scott, y grampas de 3´´ y ½,, pasando por los cables de instalaciones eléctricas y telefónicos, lo que causaba interferencias magnéticas, también se dan algunas malas configuraciones de los cables con el conector RJ-45, lo que no permitía establecer una conexión a la red, malos contactos entre la tarjeta de red y el conector malos contactos, conflictos entre la tarjeta de red incorporada de la placa madre y la colocada requerida para la red, ocasionando por estos motivos un sin fin de problemas que dificultaban de gran manera la conexión con los servidores del consulado y con la conexión de los servidores con la central Serpro, haciendo de esta manera ineficiente las funciones administrativas de los funcionarios.

Además de contar con el servicio de internet ADSL proveído por la empresa de telecomunicaciones Coteco Ltda. Con un mínimo de ancho de banda de 128 kbps de bajada y 64 kbps de subida, se suman los constantes cortes ya sea por problemas de mantenimiento en Coteco o por parte de la empresa brasilera que provee el servicio a Coteco, ocasionando de igual forma retrasos de información requerida, perdidas de información, demora en la emisión de los diferentes servicios y otros.

La configuración de software con la que cuentan todas estas maquinas es la siguiente:

Descripción de software	Cantidad de computadoras
Sistema operativo Window xp SP 2.	11
Office 2007	8
Office 2003	3
Sistema operativo 2000	1
Office 2000	1

Tabla 3.2.
Fuente: Elaboración propia

b) Diagnostico total de la Red de Datos e Internet

El diagnostico de la red de datos e internet sirvió para apreciar la situación en la que se encontraba la red de datos e internet, todo el relevamiento de la información que se obtuvo fue concerniente a la estructura física y lógica de la red de datos, así como la consulta a los usuarios del predio del consulado de cada uno de los requerimientos y/o reclamos que tenían cada uno de ellos con respecto a la red de datos y el servicio de internet. Para tal efecto se planifico las actividades que son reflejadas en el (ANEXO 3A).

El diagnostico total de la red de datos e internet ayudo a detectar un conjunto de problemas los cuales surgen como una necesidad por parte de los usuarios. Para obtener información fiable se decidió dividir a los usuarios en tres grupos: autoridades consulares, agentes de atendimiento, atención al público, de los cuales se entrevisto de forma aleatoria a una muestra representativa de cada grupo. Del primer grupo de personas se entrevistaron a 2, del segundo grupo de personas se entrevistaron a 3 usuarios y del tercer grupo de personas se entrevistaron a 3, haciendo un total de 8 personas entrevistadas.

Para el planteamiento de las preguntas se decidió subdividirlas en tres aspectos: el primer aspecto concerniente a la Red de Datos, el segundo aspecto concerniente al servicio de Internet y el tercer aspecto al conocimiento del personal y otros. Las preguntas realizadas concernientes al primer aspecto fueron 7, del segundo aspecto fueron 6 y respecto al tercer aspecto fueron 6 haciendo un total de 21 preguntas cerradas.

A continuación se muestra una descripción de las variables más representativas respecto a la red, el servicio de internet, personal y otros, para resumir el diagnostico de la red de datos y el servicio de internet.

En el aspecto de estabilidad en la conexión a la red de datos y según las escuetas, 50% establece que la conexión a la red de datos es inestable, mala, un 40% regular, un 10% establece que es estable como se muestra en la siguiente grafica.

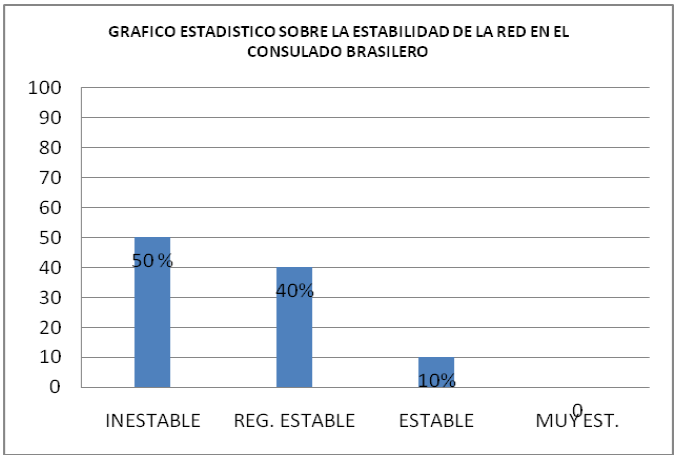


Grafico 3.1
Fuente: Elaboración propia

Respecto a la seguridad de la información obtenida de internet, el 60% determino inseguridad, el 30% que es regularmente fiable y solo un 10% que es bueno totalizando un 100%

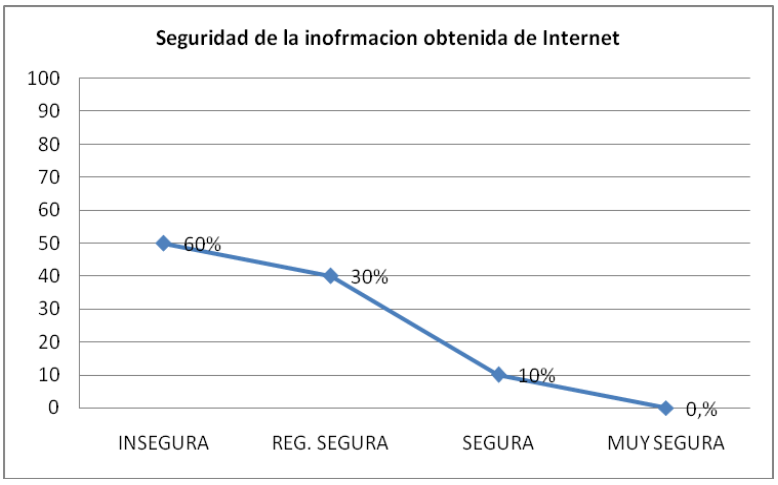


Grafico 3.2: Seguridad de la información de internet
Fuente: Elaboración propia

En cuanto al servicio técnico, el 37% menciono que cuentan con el servicio técnico con problemas relacionados con el cableado de la red o desperfectos que hubiera en ella y el 63% no cuenta con este elemental servicio.

En cuanto al aspecto de contaminación y limpieza de virus informáticos, el 25% saben como el virus informáticos pueden atacar o infectar a sus equipos, también tienen conocimientos de por qué medios pueden ser infectados y el 75% no tienen ningún conocimiento al respecto.

También se consulto a los funcionarios el tiempo que les toma en procesar un servicio con el objetivo de determinar la velocidad del internet en función al tiempo, de donde un 30% demora entre 10-20 minutos, promedio no aceptable pero mucho mejor a un 40% que demora entre 20-30 minutos, ya muy preocupante, y un 10% demasiado demora entre 10-20 minutos, situación preocupante respecto a la velocidad y estabilidad del internet, como se ve en el grafico siguiente:

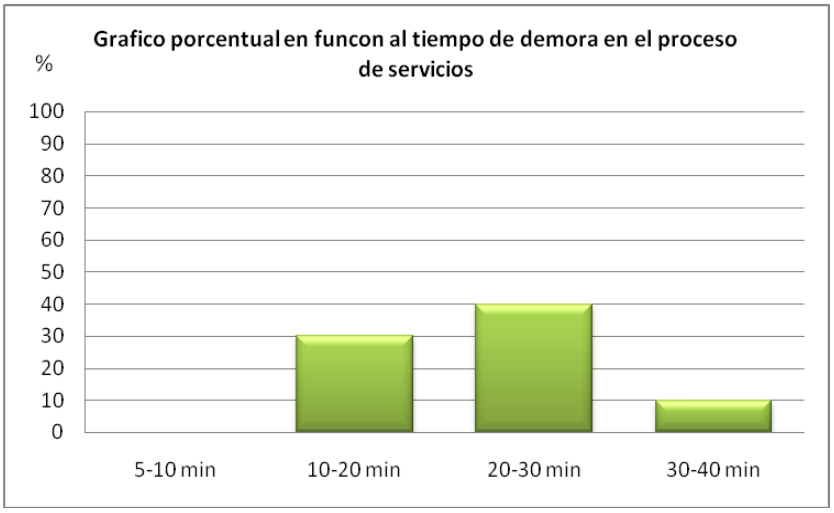


Grafico 3.3: Proceso de servicios en función al tiempo
Fuente: Elaboración propia

Dentro de este proceso del diagnostico de la red de datos y el Internet mediante la observación se tabularon datos respectos al consumo de ancho de banda real testeados desde las siguientes paginas.

1. http://www.adslzone.net/
2. http://www.testdevelocidad.es/

A continuación se observa datos obtenidos de forma aleatoria (fecha y hora) de cada uno de los monitoreo realizados.

Mes	Fecha	Hora	Ancho de Banda
Agosto	27/09/2010	11:00 a.m.	86,4 Kbps.
Agosto	27/09/2010	11:30 a.m.	65,1 Kbps.
Agosto	27/09/2010	12:00 p.m.	80,3 Kbps.
Agosto	29/09/2010	12:30 p.m.	70,7 Kbps.
Agosto	29/09/2010	12:45 p.m.	84,4 Kbps.

	Promedio Parcial		**77,38 Kbps.**
Septiembre	14/09/2010	01:00 p.m.	92,22 Kbps.
Septiembre	16/09/2010	16:00 p.m.	81,06 kbps.
Septiembre	17/09/2010	09:30 a.m.	79,71 Kbps.
Septiembre	19/09/2010	16:30 p.m.	83,04 Kbps.
	Promedio Parcial		**84,00 Kbps.**

Tabla 3.3: Testeo de ancho de banda real
Fuente: Elaboración Propia.

De donde se determina que durante este proceso de observación para el diagnostico de estos dos meses el promedio del ancho de banda fue de un 80,69 Kbps. Un rango regular para el desarrollo de los diferentes servicios

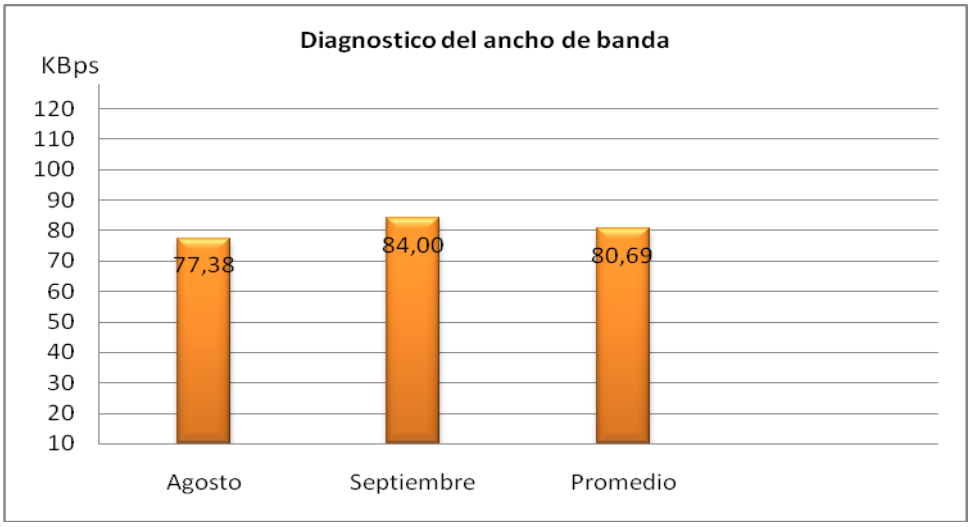


Grafico 3.4: Diagnóstico del ancho de banda
Fuente: Elaboración propia

Respecto a la existencia de reglamentos internos para el uso adecuado tanto de la red como de internet, el 100% del personal menciono que no existen políticas que reglen el uso adecuado tanto de la red como de internet.

Para observar con más detalle el diagnostico realizado, ver (ANEXO 4).

c) Conclusiones del diagnóstico

Tomando en cuenta que el uso del Internet es necesario en el ámbito laboral de la institución y que Internet no es constante debido al mal uso, cortes por parte de Coteco, es

necesario la implementación del servidor proxy, ya que los usuarios hacen las visitas a páginas informativas y de sistemas en líneas, es por eso que se debe evitar las descargaras de diferentes tipos como por ejemplo de los P2P, facebook, orkut, y otros.

Reestructurar parcialmente la red de datos para optimizar el funcionamiento de las prestaciones que por ella pasa, corrigiendo las malas conexiones físicas de la red de datos mediante la reorganización y adición de terminales necesarias.

Diseñar e implementar políticas de uso de la Red de Datos y el Servicio de internet, con la finalidad de reglamentar el uso adecuado de la red y el servicio de internet, además de contra restar los virus informáticos mediante la limpieza periódica y capacitación a los usuarios para esta actividad

Brindar la asistencia técnica necesaria a los usuarios de forma rápida e inmediata para la resolución de problemas de conexión en la red o de otros percances que se puedan presentar, Controlando y monitoreando del servicio de internet a fin de priorizar el eficiente funcionamiento de las prestaciones de la red.

3.2 FASE DE ADMINISTRACIÓN DE LA CONFIGURACIÓN

A continuación se describen las actividades ubicadas dentro del proceso de la administración de la configuración. Estas actividades son la planeación y diseño de la red; la instalación y administración del software; administración de hardware, y el aprovisionamiento. Por último se mencionan los procedimientos y políticas que pueden ser de ayuda para el desarrollo de esta área.

3.2.1. Planeación y diseño de la red

El objetivo de esta fase para implementación del servidor de administración de red de datos, es de tener los requerimientos para su ejecución, tales como el diseño estructural de la red tanto lógica como física, la ubicación de los dispositivos de conectividad que interactúan con el servidor y así tener las necesidades para la red.

Durante el diagnostico obtenido por medio de la observación, en la red anterior se percibieron muchas falencias, como repetidas conexiones entre vecinos a pocas distancia, ya que el objetivo es de tener una red de datos compactas y sin coaliciones ni perdidas de datos, así teniendo un diagnóstico del presente estudio se realizó un diagrama de red en base a los switch que interactúan en el entorno del cableado estructurado.

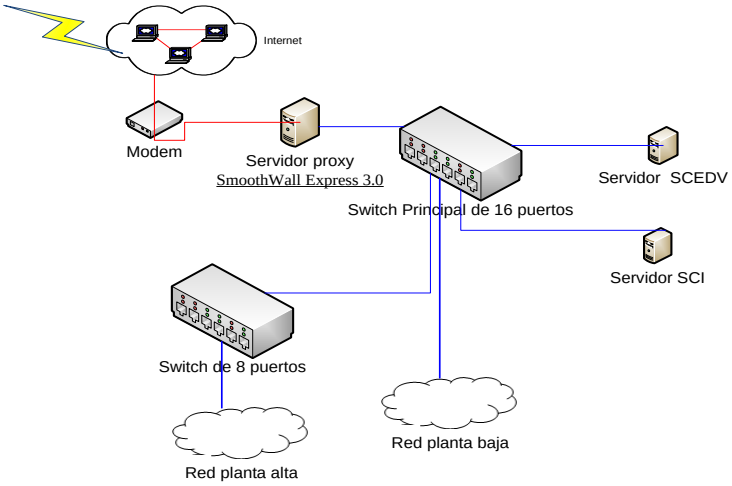


Figura 3.3: Diagrama estructural de la red
Fuente: Elaboración Propia

Es así en la que se plantea la realización del esquema estructural, de toda la red de datos del Consulado Brasilero en Pando, en este caso relacionando los equipos de forma espontánea y descriptiva, para así tener un idea de la red organizada global, las líneas segmentadas es la descripción de una conexión entre dos dispositivos y las llenas es de un dispositivo a un ordenador.

Tomando en cuenta que un esquema estructural de toda la red de datos, es de gran ayuda ya que se tiene la ventaja, a la hora de reparar un cable dañado o una soltura de un conector Rj45. así se puede tener una idea de donde se tiene en corte, estas descripciones son de gran ayuda, ya que sin un esquema estructural sería muy difícil saber dónde se tiene un corte se tendría que testear los Switch.

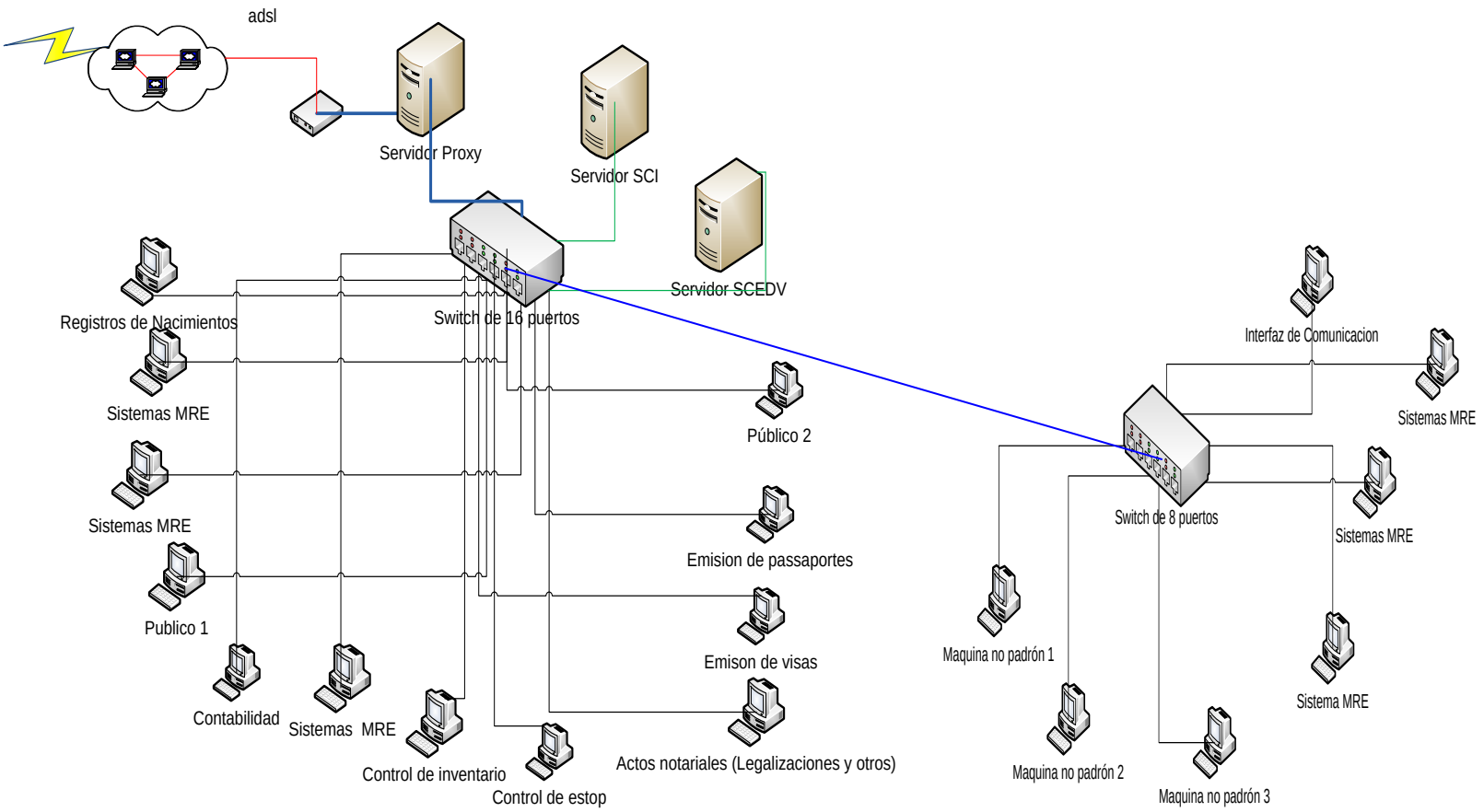


Figura 3.4: Diagrama de la red estructural descriptiva del consulado
Fuente: Elaboración Propia

En la figura anterior se describe la forma lógica de cómo fue instalado nuestro firewall, con la finalidad de administrar, controlar y monitorear el internet y su ancho de banda, y así resolver los posible problemas que se den dentro del trafico de información de la red de datos, así como optimizar el uso adecuado del ancho de banda del servicio de internet por parte de los usuario mediante la políticas relacionadas a este servicio y según la prioridad de usuario.

El siguiente paso del diseño fue la implantación del croquis de la institución, relacionado con las conexiones del cableado estructurado de la red de datos, de esta forma se obtuvo los datos mediante la observación, ya que es la esquematización más importante para el entendimiento y ubicaciones de los dispositivos de comunicación, como del medio de trasmisión o cable UTP, de esta manera se tiene una descripción exacta del diseño final del cableado.

El cual se trabajó con un cableado ya existente, en la que reestructuro gran parte, de manera más óptima para así tener un aproximamiento a las normas OSI, el centro donde se encuentra implantado el servidor de administración de redes de datos, está en la sala del área consular (planta baja) se encuentran dos Servidores SCI, SCEDV, para garantizar el funcionamiento de estos servidores se vio por conveniente reorganizar el cableado. Como se ve más adelante en la figura 3.5 y 3.6.

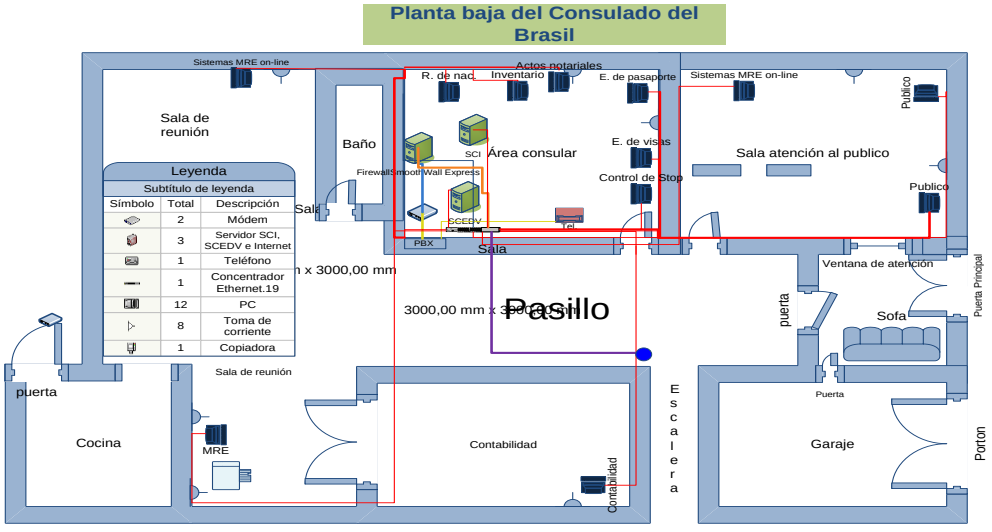


Figura 3.5: Reestructuración parcial de la red de datos.
Fuente: Elaboración Propia

En la figura 3.5. se instalo y habilito el segundo Switch de ocho puertos y la adición de 4 nodos también hechos a pedido de la autoridad consular, dos para la utilización de las Web gubernamentales y dos para la autorización de los servicios procesados, por los agentes consulares.

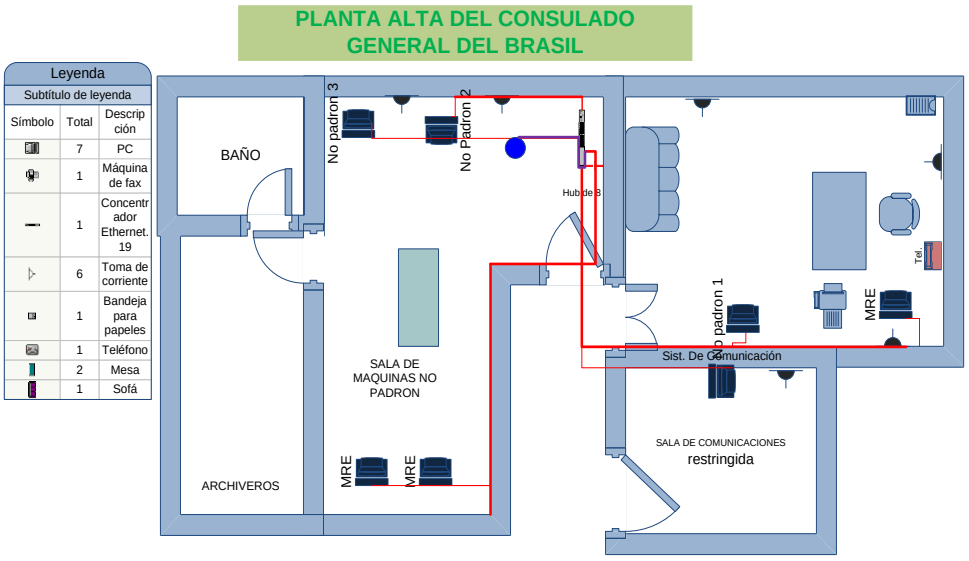


Figura 3.6: Reestructuración parcial de la red de datos.
Fuente: elaboración propia

3.2.2. Instalaciones y administración del software

En esta etapa se divide en dos partes la administración del hardware y el software en la que se describirá de manera resumida los dispositivos a usar de acuerdo a sus instalaciones:

A) ***Instalación del Hardware.-*** Para la implementación del **Servidor Proxy SmoothWall Express 3.0, para la administración** de la red de datos y restructuración de la red, los dispositivos que se instalan son de acuerdos a las necesidades requeridas, como conexiones de equipos nuevos en la que se tiene que agregar una tarjeta de red en caso que no tenga una integrada o incorporación de un Switch si no hay puertos disponibles estas son algunas de las instalaciones de hardware.

El servidor de administración de redes de datos fue armado de acuerdo a las funciones que realizara y estas son sus principales características de hardware características:

Unidad	Dispositivos	Descripción
2	Tarjetas de Red.	PCI con puerto RJ45-10/100.

1	Placa Madre.	Intel Gateguay.
1	Procesador.	Intel Pentium IV 3,06Ghz.
2	Memoria RAM.	Capacidad 1 Gb.
1	Disco Duro.	Capacidad de 160 Gb.
1	Lector de CD.	Marca LG.
1	Case Compag.	Color Blanca 40 x 40cm.

Tabla 3.4: Características del equipo para el servidor
Fuente: Elaboración Propia

De acuerdo a las características mencionadas el servidor de administración de redes, está en un estado bueno de acuerdo a sus dispositivos integrados, ya que teniendo los hardware idóneos sería mejor tomando en cuenta que subiría el nivel de rendimiento tanto del flujo de la red como el filtrado y monitoreo interno que realiza el servidor. Los hardware más importantes para la implementación del servidor fueron, los concentradores o switch ya que sin ellos no se pudiera interconectar los grupos de equipos que se tiene en el consulado a continuación se mencionaran los dispositivos que interactúan en la red de datos**.**

d) Instalación y administración Software

Para la instalación de los aspectos técnicos para la distribución de GNU Linux **"**SmoothWall Express 3.0**",** de nuestro Firewall,

Descargaremos el fichero ISO desde:
http://www.smoothwall.org/get

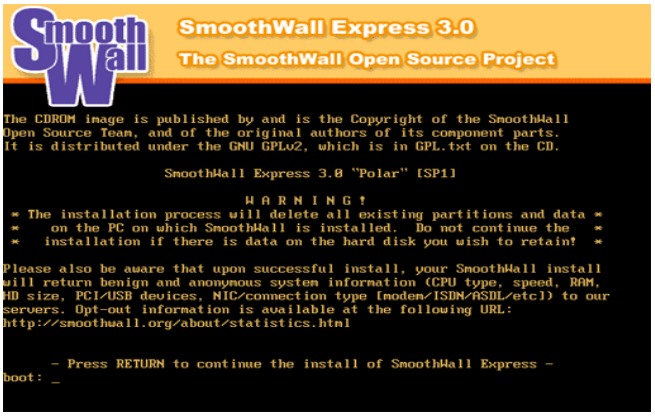


Figura 3.7: instalación del Smoothwall 3.0.
Fuente: SmoothWall Express 3.0

Una vez instalado y funcionando el proxy SmoothWall Express 3.0, ver detalles de la instalación en (ANEXO 6.), traslada a nuestras máquinas todas las peticiones de servicios de Internet.

Luego desde un equipo remoto y como interfaces graficas utilizaremos herramientas como el Putty para conectarnos mediante el protocolo SSH, que nos sirve como interfaz de modo consola para la ejecución de comandos, y Winscp, que facilita lo necesario para copiar editar archivos al igual que el FTP, como se muestra las siguientes imágenes.

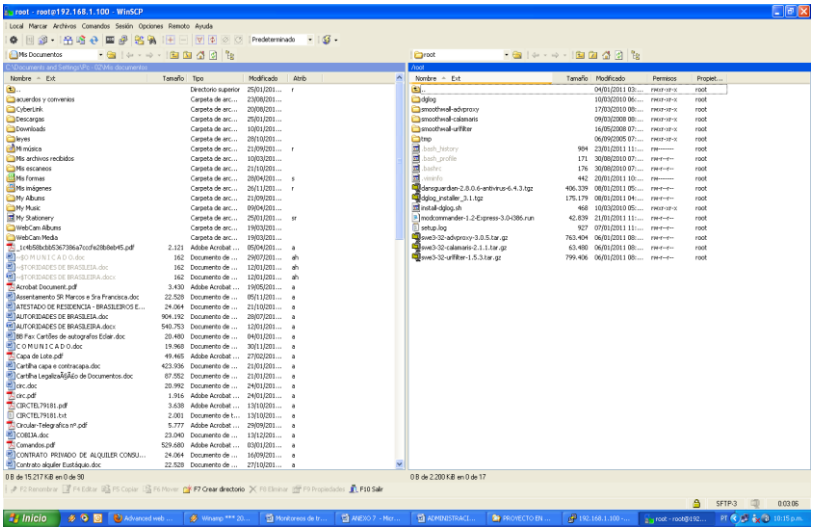


Figura 3.8: entorno grafico para manipulación de archivos.
Fuente: WinSCP

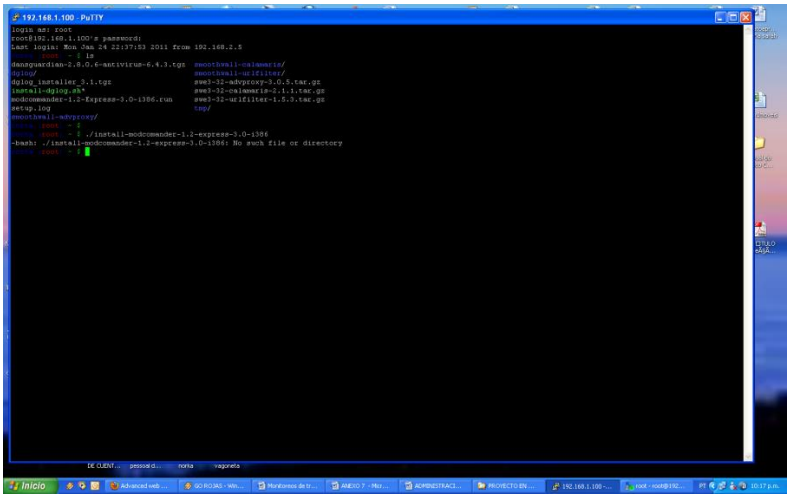


Figura 3.9: modo consola para manipulación de archivos conexión ssh.
Fuente: Putyy

Luego ingresamos desde un equipo remoto para la administración vía HTTP, ingresando a nuestra dirección https://192.168.1.100:441/cgi-bin/index.cgi y tenemos como página inicial..

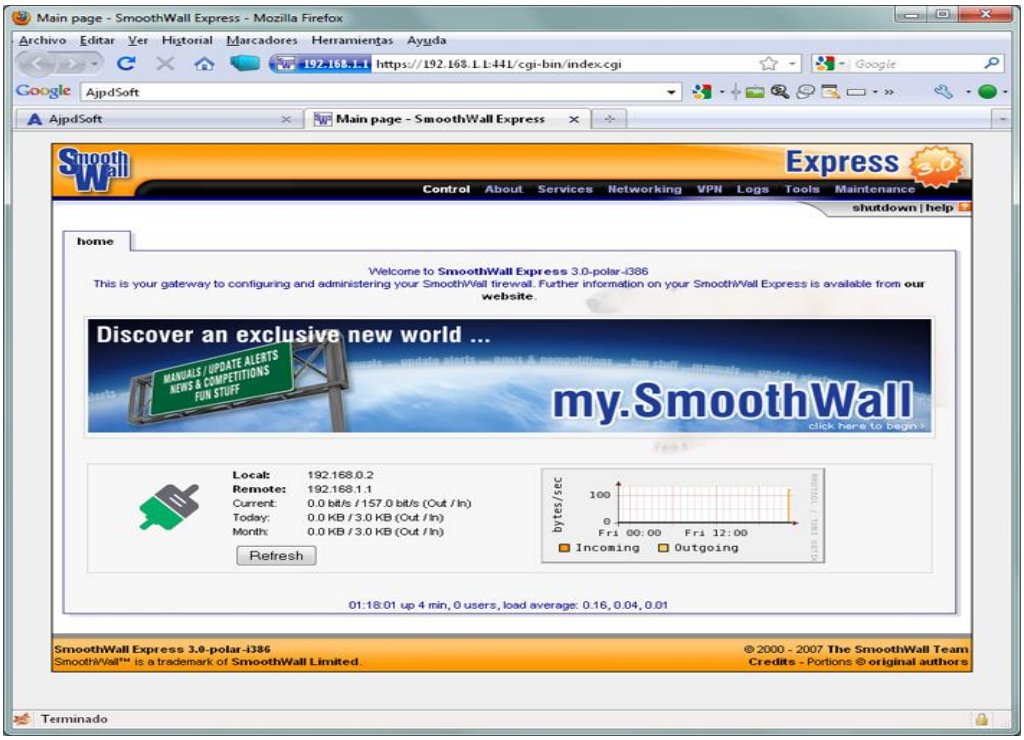


Figura 3.10: interfaz grafica del servidor.
Fuente: SmoothWall Express 3.0

Luego descargamos, descomprimimos e instalamos en modo consola los módulos advproxy, urlfilter, paquetes que nos dan una mejor administración, y filtraciones de páginas prohibidas, control de usuarios, control del ancho de banda, control de tráficos entrantes y salientes, etc.

De aquí en adelante describimos la configuración realizada en nuestro proxy:

ADVANCED- PROXY: Este es un complemento que extiende el interfaz proporcionándonos más opciones y ventajas para la administración de nuestro firewall con las siguientes opciones:

En el área de **Common Settings:**
Enable on Green: Activo
Transparent on Green: Activo
Visible Hostname: nombre-de-tu-server.local
Cache Administrator e-mail: tu-correo
Error messages languaje: Spanish
Error messages design: Standard

Log settings:
Log Enable: Activo
Log query terms: Activo
Loug user agents: Activo

Cache Management:

Enable offline mode: Activo

En Cache size: 22000

Con este valor indicamos la cantidad en megas que va a utilizar para cache de todas las peticiones de Internet de nuestros usuarios, vamos a definir que asigne 22mb para el cache.

Max object size (KB): 40960

Con esto indicamos que los archivos, fotos, videos y cualquier tipo de archivo que baje de Internet, que no exceda este tamaño (en megas) se guarde en el cache del proxy. (Con los archivos de actualización este tamaño es más que suficiente)

Transparent: [x]

Lo vamos a activar. Esto indica que nuestros usuarios no tendrán que efectuar configuración en sus exploradores web para utilizar el proxy.

Luego la opción Enabled: [x], corresponde a activar todo lo que hemos indicado en estas opciones.

im proxy (Sub-opción Services): Esta opción permite registrar todos los eventos en messenger. Activa los considerables.

Luego guardamos estas configuraciones, SAVE.

POP3 proxy: Chequea en los correos recibidos en POP3 la existencia de virus.
Presiona SAVE

SIP proxy: Activarlo para aplicaciones VOIP y similares como Skype.
y guardamos SAVE.

Remote Access:

Activamos Remote access a través de ssh y Allow admin access only from valid referral URLs. Esto es muy importante que lo activarlos para continuar con la administración via SSH

y guardamos SAVE

Networking (Opción principal):

Qos (Sub-opción Networking): Establecemos la administración para una mejor velocidad que la red es capaz de lograr respecto al ancho de banda.

Enable traffic shaping: [x]: aquí activamos la configuración de acuerdo a nuestro ancho de banda, pero funciona para enlace de 128, 256 con lo siguiente:

External upload speed: 512kbit
Headroom: 10%
Internal upload & download: 1gbit
Download speed: 512kbit
Traffic that does not match below gets treated as: normal

Rule selection:
Instant Messaging: low
File Transfer Protocol: high
Electronic Mail: high
Voice Over IP: high
Gaming: slow
VPN: slow
Domain Name Service: high
Web: high
Secure Shell: high
Peer to Peer: low
Multimedia: high
VNC: high

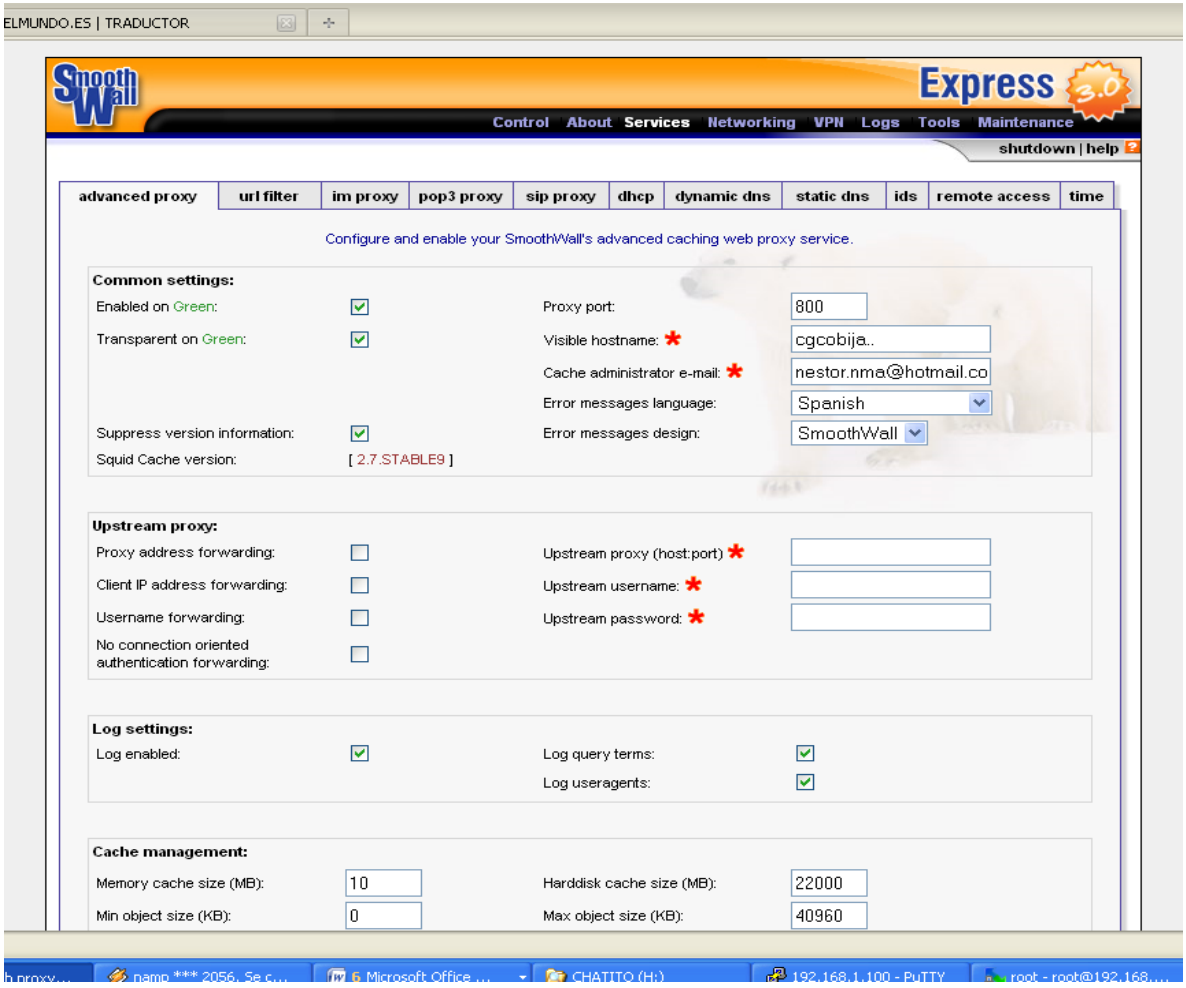


Figura 3.11: Configuración del proxy.
Fuente: SmoothWall Express 3.0

Siguiendo con la configuración del proxy, seguimos con el urlfilter - The URL filter add-on, que es una potente herramienta que permite bloquear sitios de internet que usen los usuarios y nos congestionen nuestro ancho de banda, utilizando catalogados como.

URL FILTER (Sub-opción Services)

Block categories: Selecciono las categorias deseadas a bloquear en Internet.

Custom Blacklist:
Enable custom blacklist: Activo

Custom Whitelist:
Enable custom whitelist: Activo

Custom expression list:
Enable custom expression list:

Block page settings:
Redirect to this URL: Puedemos colocar la dirección de una página o una de tu intranet.

Advanced settings:

Enable SafeSearch: Activo

Enable log: Activo

Log username: Activo

Split log by categories: Activo

Automatic Blacklist update:
Enable automatic: Activo
Automatic update schedule: Dialy
Select download: Selecciona MESD

Guardamos y actualizamos las configuraciones Save Update Settings...

Shalla Secure Services y luego Update Now
Esperas unos cuantos minutos porque tarda

MESD y luego Update Now
Sigues esperando...

Univ. Toulouse y luego Update Now.

Esta configuración tiene por objetivo activar una serie de categorías que nos permitirán o bloquearla o darles pasos.

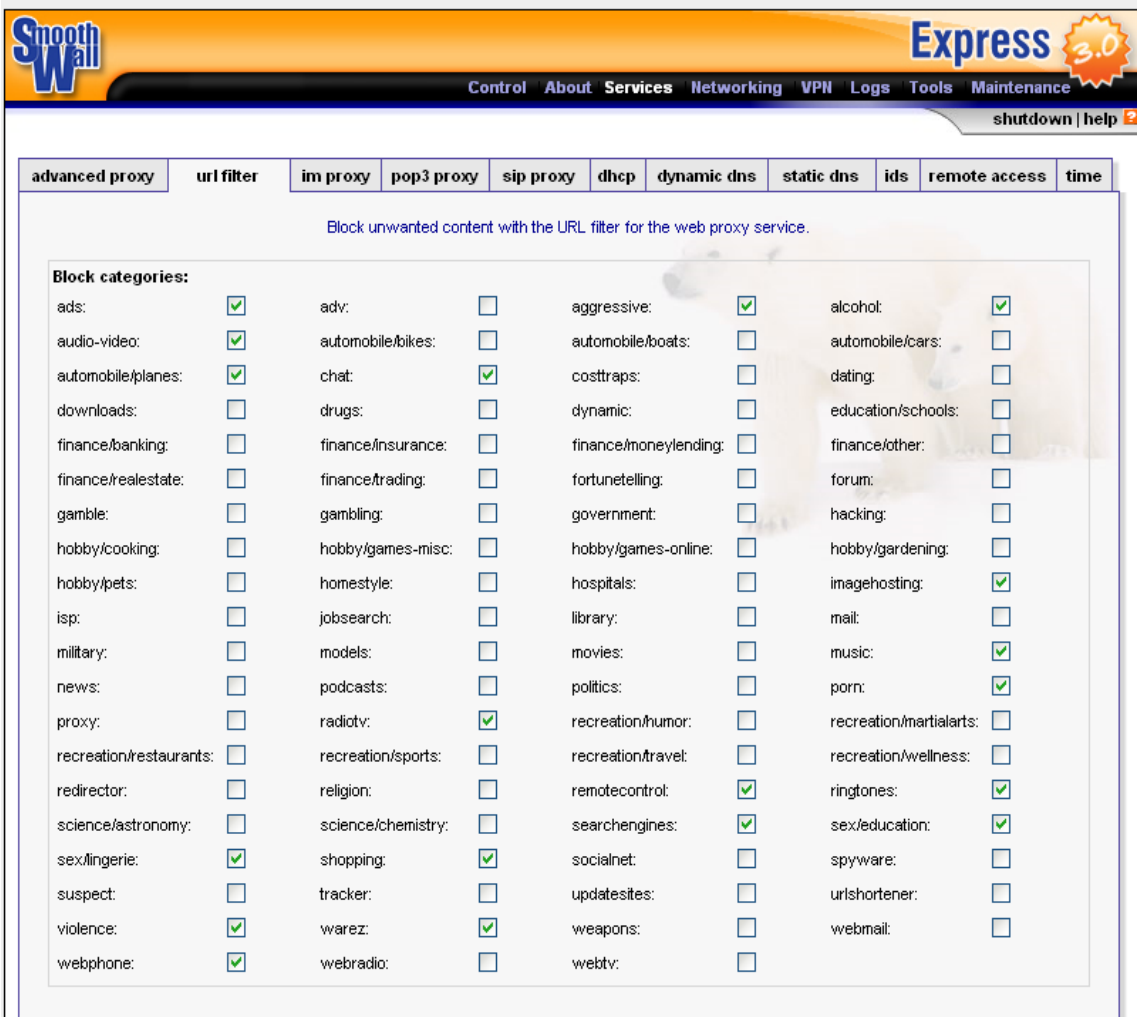


Figura 3.14: bloqueo de categorías peligrosas y/o de congestión del ancho de banda.
Fuente: SmoothWall Express 3.0.

Hasta este punto se ha activado los filtros requeridos.

Ahora activamos algunos puertos y protocolos mínimos, para nuestra administración

Networking (Opción principal)
outgoing (Sub-opción Networking)
Interface defaults:
Traffic originating on GREEN is:
Blocked with exceptions
Luego en Add Exception:
Applications on service(s): HTTPS
Luego presiona ADD
Agregamos estas excepciones, para nuestra administración.
MSN Messenger (1863)

Yahoo (5050)
POP3 (110)
SMTP (25)
HTTPS (443)
POP3 over SSL (995)
SMTP over SSL (465)
AMAROCK 8000:8200
WEBMAIL 2095

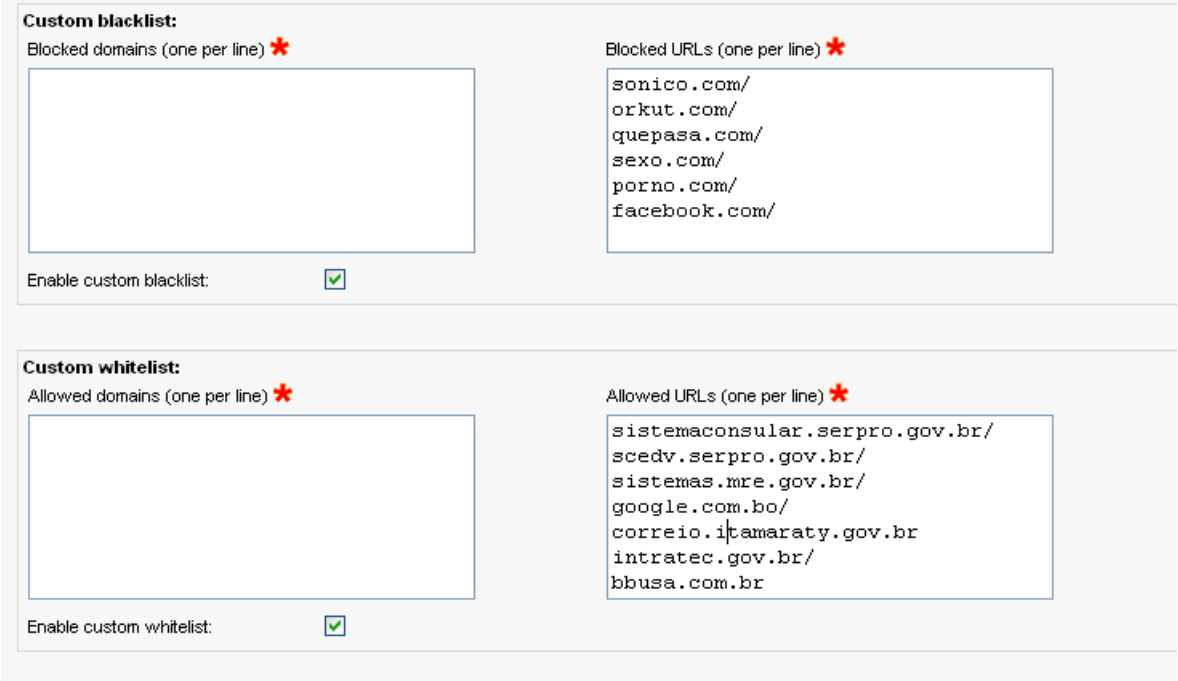


Figura 3.12: Configuracion de URLFilter.
Fuente: SmoothWall Express 3.0

3.3. ADMINISTRACIÓN DEL RENDIMIENTO

La administración de red de datos e internet se la realizo en las dos fases porque vio la necesidad de recolectar y analizar el tráfico que circula por la red de datos en un momento en particular (tiempo real) o en un intervalo de tiempo, esto permitió tomar decisiones pertinentes de acuerdo al comportamiento encontrado. La administración del rendimiento se la dividió en dos etapas: monitoreo y análisis las cuales explican a continuación:

3.3.1 Monitoreo

Para el monitoreo luego de la implementación del servidor de internet desde nuestro firewall se observa claramente tanto el trafico como las filtraciones de sitio que congestionen el ancho de banda

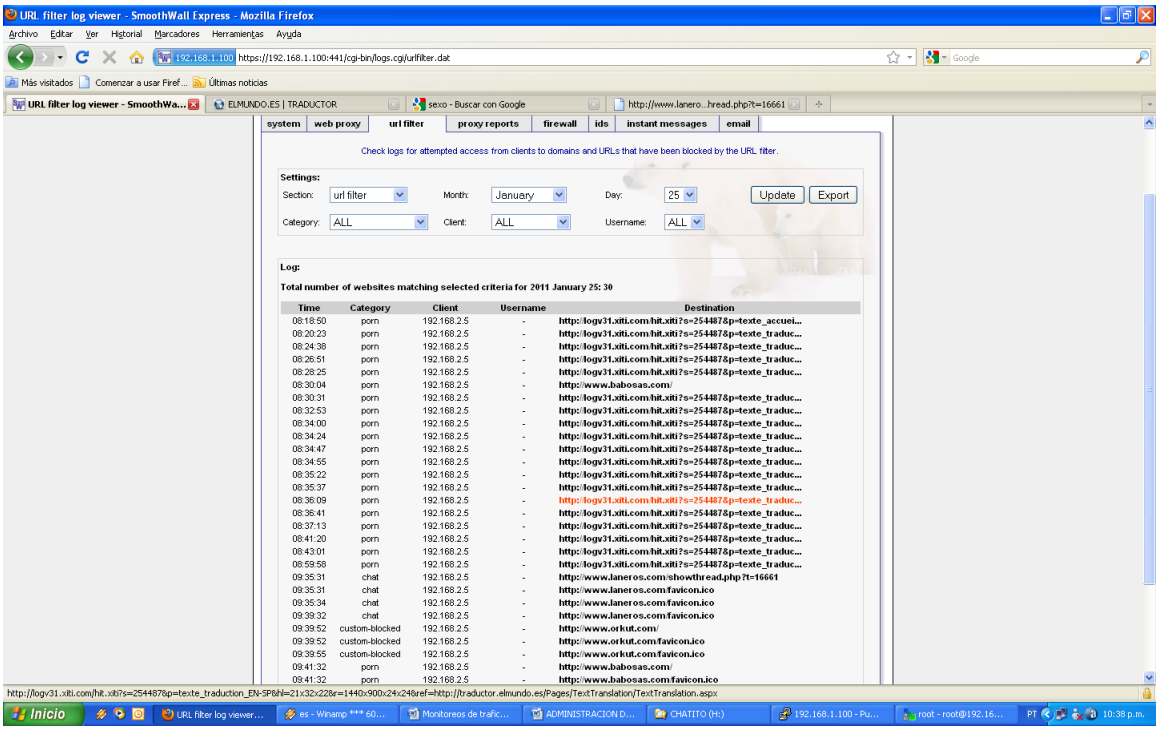


Figura 3.13: control de usuarios de URLFilter..
Fuente: SmoothWall Express 3.0

A continuación se muestra un listado desde el menú About de la administración del firewall o cortafuegos SmoothWall, del control de las opciones más destacadas como ser:

- **Status**: muestra el estado de los servicios de SmoothWall: Logging server, DNS proxy server, Kernel logging server, CRON server, Web server, DHCP server, SIP server, Quality of Service traffic shapping, UPNP, Clam Anti-Virus server, Web proxy, Secure shell server, Intrusion Detection System, IM proxy server, Network time server, POP3 proxy server, VPN:
- **Advanced**: muestra información general del sistema operativo y de las interfaces de red: memoria usada y libre, disco usado y libre, tabla de rutas, paquetes enviados y recibidos por cada interfaz de red, módulos cargados, versión del kernel, etc.:

- **Traffic grahs**: genera información del tráfico por cada interfaz de red y por cada equipo de la red (tráfico en tiempo real, tráfico acumulado por hora, por día, por semana y por mes).
- **Traffic monitor**: muestra un gráfico con el tráfico saliente y entrante por cada equipo de la red y por cada interfaz del cortafuegos

Desde la opción **"firewall"** podremos ver todos los paquetes enviados y recibidos entre nuestra red e Internet:

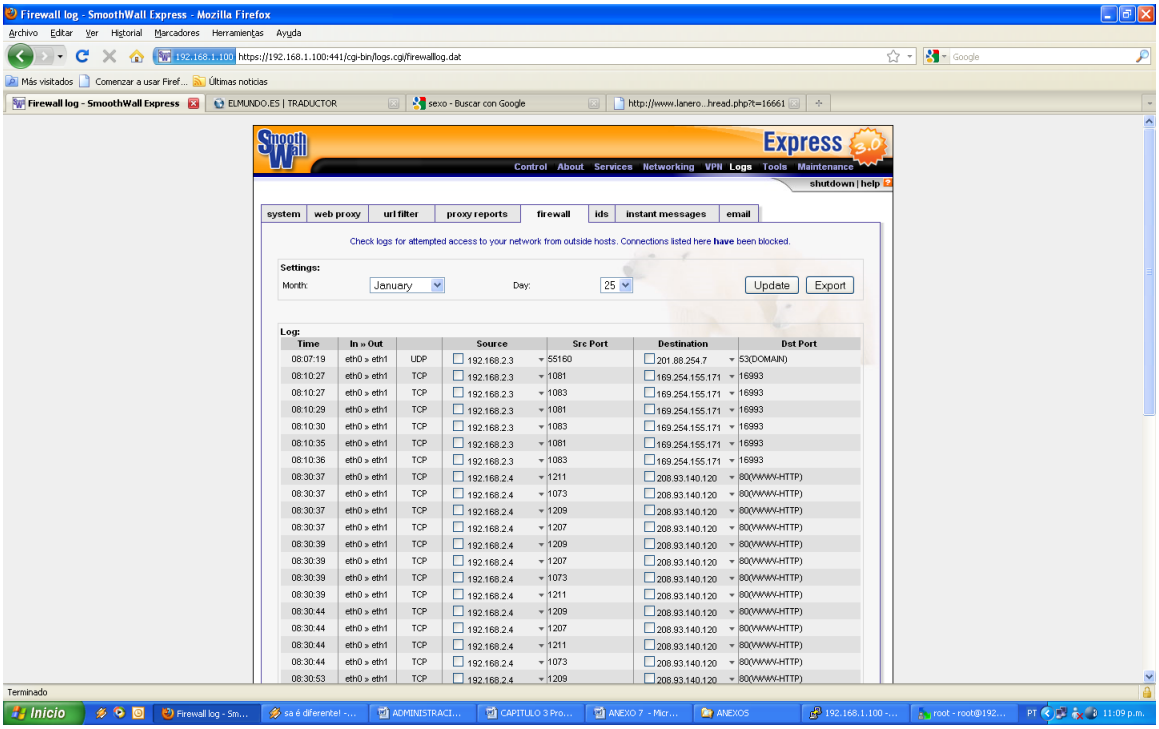


Figura 3.14: control del tráfico entrante y saliente de URLFilter..
Fuente: SmoothWall Express 3.0

Fueron las principales opciones que permitieron tomar decisiones respecto al filtrado de páginas como ser: orkut, msn, xxx, y dar así seguridad de la red, a cada usuario de acuerdo a la necesidad y requerimiento priorizando usuarios de la siguiente manera:

Usuarios con prioridad: Vice-Cónsules, Asistentes de Cancillería, Administrador de los sistemas.

Usuarios sin prioridad: Auxiliares administrativos, agentes consulares, estoquistas y auxiliares de apoyo.

Con la implementación de nuestro servidor Proxy se mejoro en un gran 95% la velocidad del ancho de banda debido a las filtraciones dadas del firewall, además de la adición de tres nodos de acuerdo a requerimiento de la autoridad consular, dos en la sala de reuniones de uso exclusivo para los sistemas web on-line gubernamentales, una terminal para la atención al público mediante la cual se hacen el llenado de formulario para las solicitaciones de los respectivos servicios.

3.3.1.1. Monitoreo del servicio de internet externo

- Se denomino monitoreo del servicio de internet externo al constante monitoreo del servicio de internet que nos brinda la Empresa (COTECO Ltda)[2].

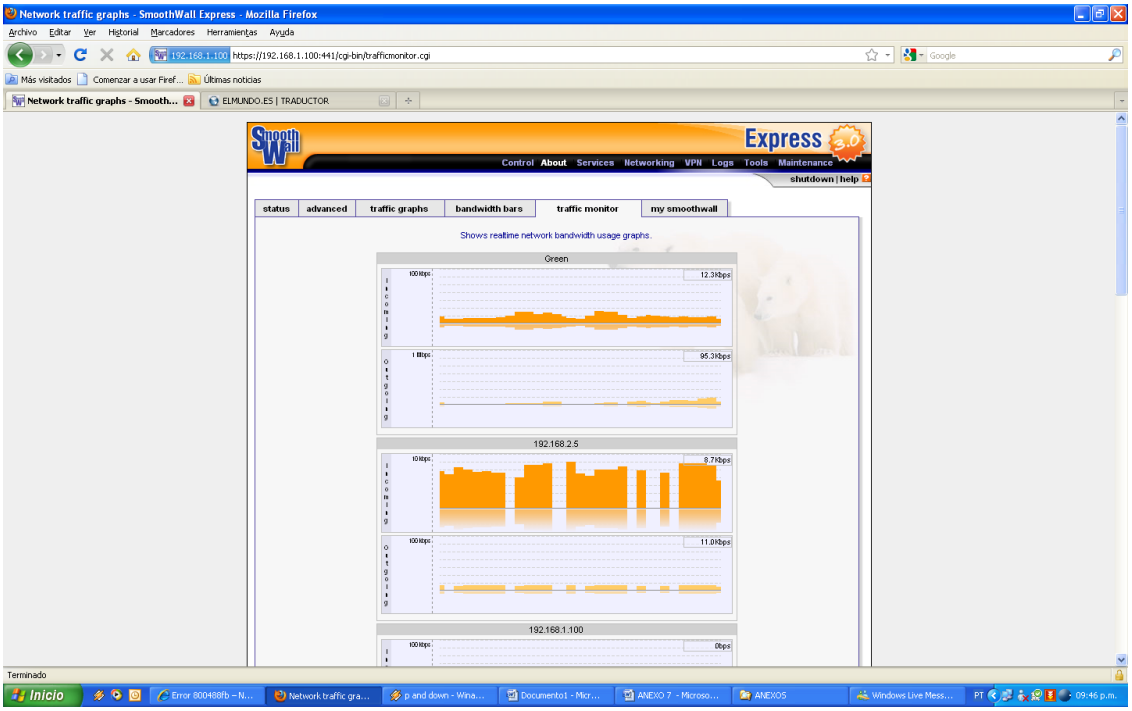


Figura 3.15: monitoreo del tráfico en la red.
Fuente: SmoothWall Express 3.0

[2] (Cooperativa De Telecomunicaciones Cobija)

3.3.1.2. Monitoreo del ancho de banda real.

- Monitoreo controlado por el **Bandwidth bars**: Controla el tráfico entrante y saliente en tiempo real por cada IP (equipo) de la red. Interesante utilidad para ver posibles equipos realizando subidas o bajadas que consuman tráfico en exceso.

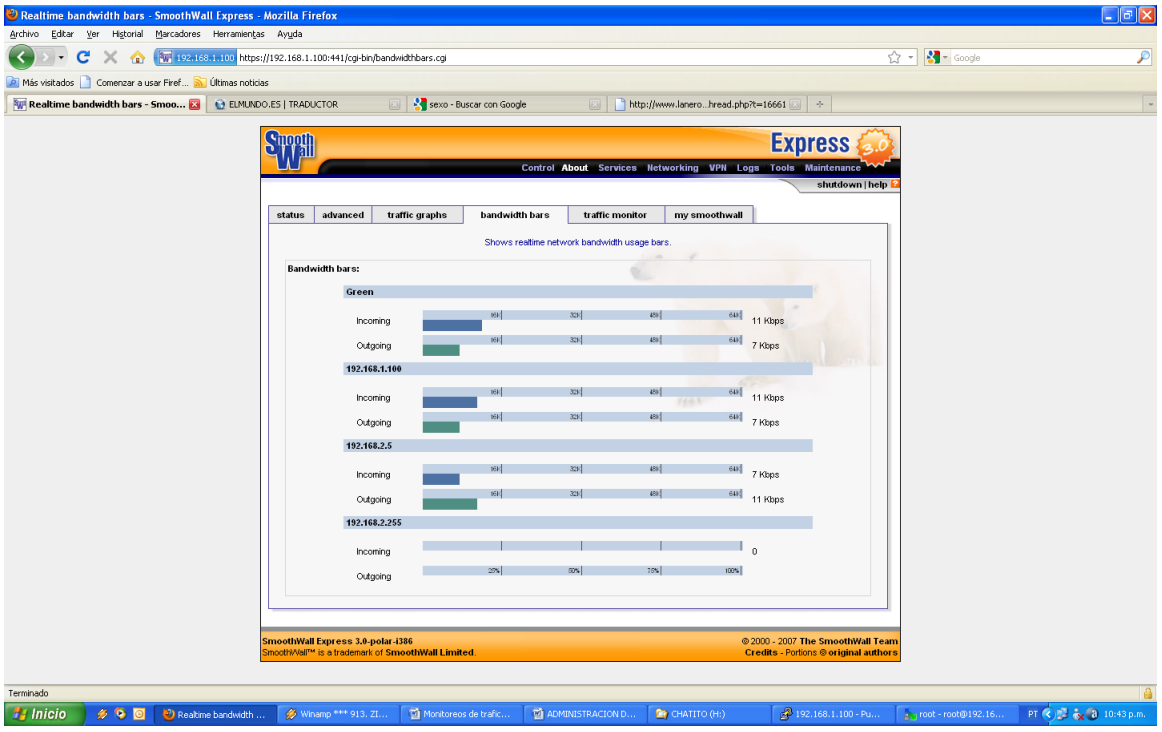


Figura 3.12: monitoreo del ancho de banda en tiempo real por usuario.
Fuente: SmoothWall Express 3.0

3.3.1.3. Monitoreo del servicio de internet interno

Se denomino control y monitoreo del servicio de internet interno al constante control y monitoreo del servicio de internet que se brinda a los usuarios del predio consulado. Para realizar este control se utilizo como herramienta el archivo access.log que genera el Servidor Proxy SmoothWall Express 3.0. El access.log genera un conjunto de datos los cuales son reflejados en la siguiente grafica.

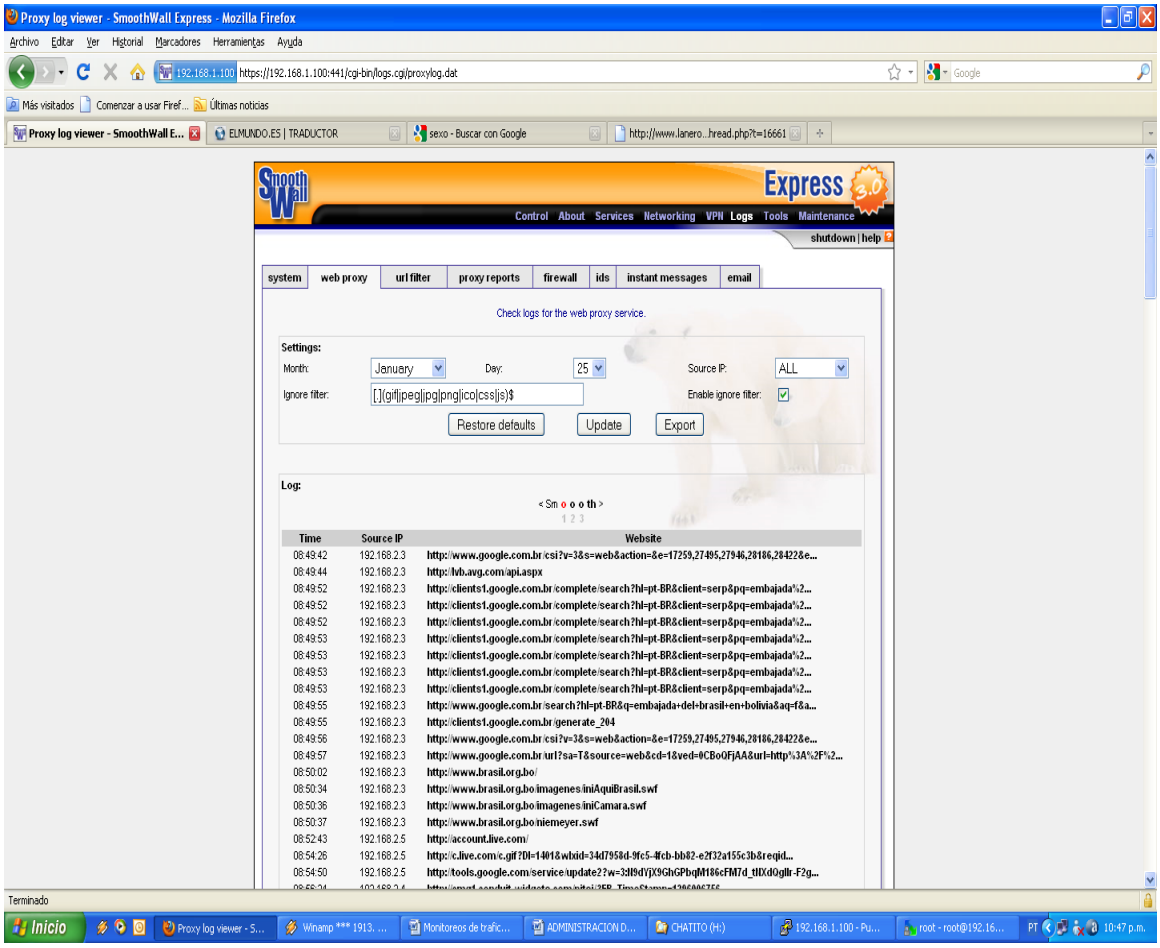


Figura 3.16: monitoreo de URLs accedida.
Fuente: SmoothWall Express 3.0

3.3.1.4. Análisis

Para un análisis se observo desde el menú "Logs" de la administración de SmoothWall, donde podremos analizar el tráfico y los distintos servicios activados de SmoothWall (web proxy, firewall, Snort IDS (detección de intrusiones), instant messages (chat), email, etc.

Una vez recolectada la información mediante la actividad de monitoreo, es necesario interpretarla para determinar el comportamiento de la red y tomar decisiones adecuadas que ayuden a mejorar su desempeño. En el proceso de análisis se pueden detectar comportamientos relacionados a lo siguiente:

- *Utilización elevada.*

- *Tráfico inusual.*
- *Elementos principales de la red.*
- *Calidad de servicio.*
- *Control de tráfico*

Todos estos los puntos se centran en base al monitoreo de acuerdo a los resultados obtenidos se hace el análisis para llegar a un deducción y así tomar decisiones.

3.3.1.5. Análisis del servicio de internet externo

Respecto a este análisis del servicio de internet externo se la realizo la misma consulta respecto a los datos (información) que los usuarios obtenían en el procesamiento de sus servicios consulta hecha en el diagnostico sobre la fiabilidad de la información obtenida de internet, donde se constato que el 75% determino seguridad, el 15% que la seguridad es regular y solo un 10% que le parece que es muy seguro, totalizando un 100%

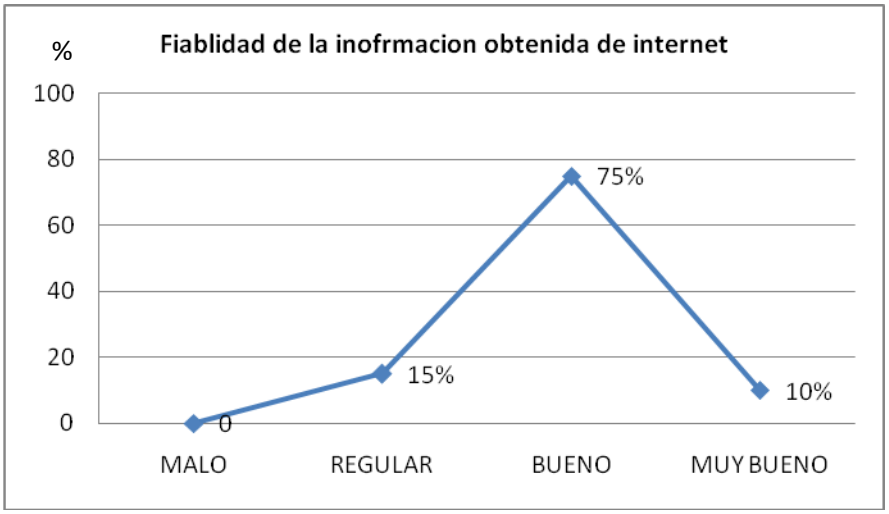


Grafico 3.5: fiabilidad de la información
Fuente: elaboración propia

- **Análisis del ancho de banda real.**

El análisis del ancho de banda real se realizo sacando un promedio de cada uno de los meses tal como se muestra en la tabla 3.5

Mes	ancho de banda
Octubre	99,53 Kbps.
Noviembre	114,29 Kbps.
Diciembre	109,96 Kbps.

Tabla 3.5: Ancho de banda en función al tiempo
Fuente: Elaboración Propia

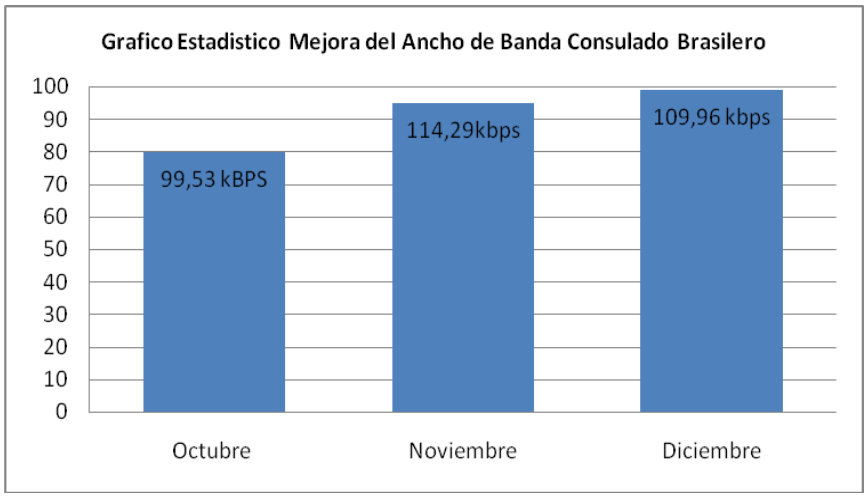


Grafico 3.6: Ancho de banda en función al tiempo
Fuente: Elaboración Propia.

De acuerdo a la figura 3.4, donde se realizo el análisis del ancho banda real y se llego a las siguientes conclusiones:

Antes de la implementación del proxy en el diagnostico se obtuvo un promedio respectos a la velocidad de 80,69 kbps, y luego de la implementación del proxy y monitoreo de firewall y respectos a los meses descritos arriba se puede decir que en octubre, noviembre y diciembre, el ancho de banda del servicio de internet promedio en un 107,92 kbps, haciendo la diferencia respecto al diagnostico inicial de 27,23 kbps, lo que significa que hubo una mejora respecto a la velocidad.

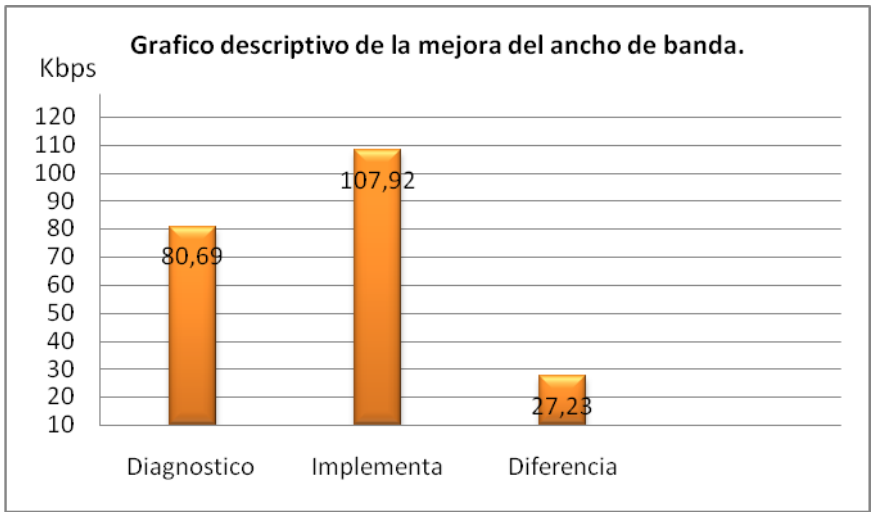


Grafico 3.7: Ancho de banda en función al tiempo
Fuente: Elaboración Propia.

Mejorando de esta manera el acceso a la información desde internet respecto al tiempo en la demora de un servicio procesado realizado por los usuarios del consulado, diferenciándose de la misma consulta hecha en el diagnostico inicial obteniendo como resultado que un 65% demora menos tiempo en realizar sus procesos, un 35% debido a su falta de práctica demora un poco más, como se muestra en la grafica 3.6.

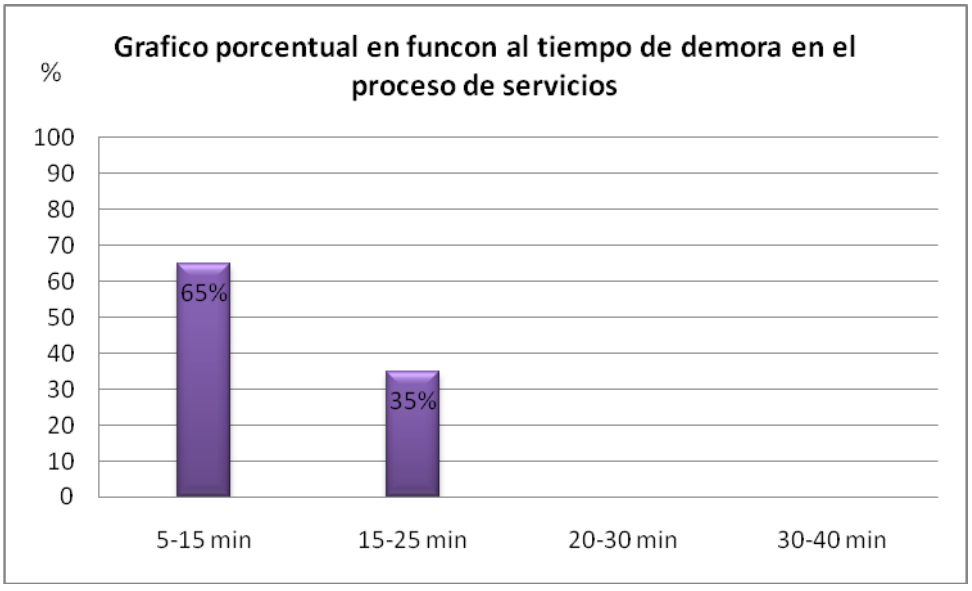


Grafico 3.8: Ancho de banda en función al tiempo
Fuente: Elaboración Propia.

3.4. ADMINISTRACIÓN DE FALLAS

Tiene como objetivo la detección y resolución oportuna de situaciones a normales en la red. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para restablecer la situación o minimizar el impacto de la falla.

La administración de fallas también llamada asistencia técnica para el presente proyecto de grado (Administración de Red de Datos y el Servicio de Internet) fue una actividad constante en toda la ejecución tal como se mostró en la primera parte del presente capitulo. Esta actividad se la clasifico en tres partes las cuales son: Asistencia técnica con relación a la red de datos, asistencia técnica con relación al servicio de internet y asistencia técnica con relación con otros aspectos.

3.4.1. Asistencia técnica por fallas de red.

Existen un sin fin de problemas causados por la falla de conexión de la computadora con la red de datos de los cuales a continuación mencionamos los más frecuentes ocurridos en el transcurso del desarrollo de este trabajo son detallados en los acápites siguientes.

3.4.1.1. Configuración de la dirección IP

Este trabajo se realizo cada vez que el usuario lo requería y simplemente se configuraba su protocolo TCP/IP asignándole una dirección IP para poder identificar a cada uno de los equipos informáticos (computadoras) de los usuarios.

3.4.1.2. Asistencia técnica de conexión a la red

Las causas para este tipo de fallas se las clasifico en dos:

- Tarjeta de red mal acomodada

Este es un problema típico cuando se mueve la unidad central de procesamiento (Case) de posición y además el Case sufre algún golpe. De alguna forma el movimiento y el golpe hacen que la tarjeta de red sufra movimientos, cuando la tarjeta de red sufre el más mínimo

movimiento hace que pierda la conexión entre sócalo de la placa madre y la peineta de la tarjeta de red y no haya la conexión física suficiente motivo por el cual pierda la conexión con la red de datos.

Una forma de comprobar que existe una conexión física es observando el led que viene incorporada en la tarjeta de red, este led tiene que estar encendida con eso nos garantiza que hay la respectiva conexión. En caso que este apagado el led ya se encontró el problema buscado.

- Adición de puntos de red

La adición de nuevos puntos fue una actividad muy importante debido a que mediante esta se ampliaba la red de datos del consulado General del Brasil, adicionando así 6 nuevas terminales necesarias en un eficiente desempeño de las diferentes funciones de esta repartición consular dividas de la siguiente manera:

3.4.2. Asistencia técnica por fallas de Internet.

Existen un sin fin de problemas causados por la falla del servicio de internet las cuales son detallados en los acápites siguientes.

- Creación de cuenta de correo electrónico

En esta actividad fue muy importante puesto que mediante esta se promovió el uso de las nuevas tecnologías implementadas por el Brasil respecto a la emisión de documentos, trabajo hecho a usuarios locales para recibir instrucciones de la secretaria de estado, para la comunicación en línea de los usuarios de la red de datos y el servicio de internet.

- Asistencia técnica del servicio de Internet

Dirección web mal escrita o digitada: Este tipo de error es común cuando digitan en forma herrada una página web. A (error de dedo). Por ejemplo: se digito la dirección www.googli.com.bo que está mal digitada, la dirección web correcta es www.google.com.bo.

3.4.3. Fallas con relación a otros aspectos

Aparte de las fallas ocurridas por la red de datos y el servicio de internet también existen otros más los cuales son detallados en mas adelantes.

A continuación se muestra la tabla 3.6 y la grafico 3.9, detallando el servicio técnico de fallas realizado en cada uno de los meses siguiendo la ejecución. Es decir está en función al mes y la cantidad de casos atendidos.

Mes	Actividad	Nº
Agosto	Asistencia técnica por fallas de la red de datos	6
	Asistencia técnica por fallas del servicio de internet	8
	Fallas con relación a otros aspectos	5
Casos atendidos el mes de agosto		**19**
Septiembre	Asistencia técnica por fallas de la red de datos	2
	Asistencia técnica por fallas del servicio de internet	5
	Fallas con relación a otros aspectos	3
Casos atendidos el mes de septiembre		**10**
Octubre	Asistencia técnica por fallas de la red de datos	0
	Asistencia técnica por fallas del servicio de internet	2
	Fallas con relación a otros aspectos	3
Casos atendidos el mes de octubre		**5**
TOTAL DE FALLAS ATENDIDAS		**34**

Tabla 3.6: Fallas atendidas en la Administración de la red de datos e internet
Fuente: Elaboración Propia

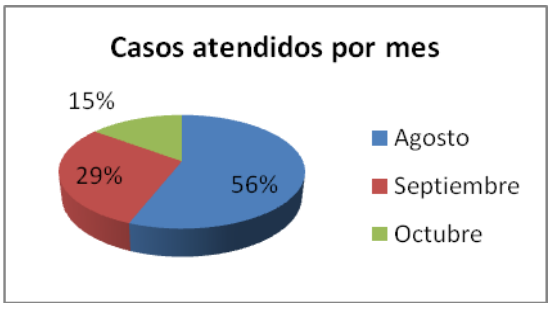


Grafico 3.9
Fuente: elaboración propia

El total de casos atendidos por distintas fallas en la administración de la red de datos e internet son 34. Observando el grafico 3.4 se puede deducir que:

1. El mes de agosto fue donde hubo más solicitudes de servicio técnico por parte de los usuarios y por ende fue el mes donde se soluciono los más problemas producidos llegando a cumplir con un 56% del total de solicitudes de asistencia técnica realizada.
2. Los meses de septiembre, se solucionaron menos problemas debido al de los mismos, llegando a solucionar en un 29% del total de solicitudes de asistencia técnica realizada.

3. El mes de octubre se soluciono menos problemas a las solicitudes del servicio técnico en un 15% el total de solicitudes de asistencia técnica realizadas.

4. Luego de la implementación de nuestro servidor y el seguimiento de las fallas las correcciones de las mismas y la reestructuración de la red, se realizo nuevamente la misma encuesta respecto a la estabilidad en la conexión a la red de datos logrando revertir los datos negativos según las encuestas se obtuvo, 82% establece que la conexión a la red de datos es estable, un 12% regular, un 8% establece que es muy estable como se muestra en la siguiente grafica.

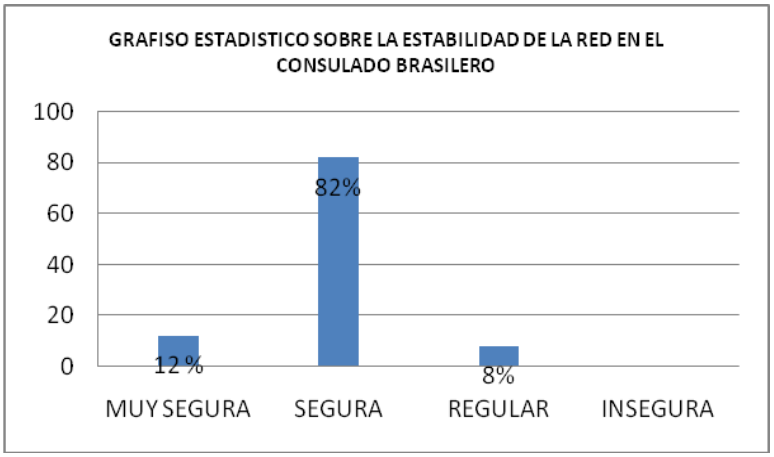


Grafico 3.10
Fuente: elaboración propia

3.5. SEGURIDAD

En cuanto a la seguridad se limito a la prevención de intrusos en nuestra red con el bloqueo de categorías que según el monitoreo se ven peligrosas y desconocidas que no conlleven a las funciones estrictamente administrativas y requeridas por la autoridad consular, como se muestra en el siguiente acápite.

3.5.1. Detección de intrusos

La detección de intrusos se puede lograr mediante nuestro servidor proxy, con el IDS que viene integrado en nuestro proxy como se describe a continuación.

3.5.2. Sistema IDS y Snort

Aumentan la seguridad de nuestro sistema, vigilan el tráfico de nuestra red, examinan los paquetes analizándolos en busca de datos sospechosos y detectan las primeras fases de cualquier ataque como pueden ser el análisis de nuestra red, barrido de puertos, etc. Compuesto por lo siguiente.

a) Snort: es un IDS o Sistema de detección de intrusiones basado en red (NIDS). Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, intentos aprovechar alguna vulnerabilidad, análisis de protocolos, etc conocidos. Todo esto en tiempo real.

b) NIDS (Net IDS): Protege un sistema basado en red. Actúan sobre una red capturando y analizando paquetes de red, es decir, son sniffers del tráfico de red. Luego analizan los paquetes capturados, buscando patrones que supongan algún tipo de ataque.

Bien ubicados, pueden analizar grandes redes y su impacto en el tráfico suele ser pequeño. Actúan mediante la utilización de un dispositivo de red configurado en modo promiscuo (analizan, "ven" todos los paquetes que circulan por un segmento de red aunque estos nos vayan dirigidos a un determinado equipo). Analizan el trafico de red, normalmente, en tiempo real. No sólo trabajan a nivel TCP/IP, también lo pueden hacer a nivel de aplicación.

POLÍTICAS DE USO DE LA RED (VER ANEXO 5**)**

Este capítulo tiene por objetivo mostrar los resultados obtenidos cualitativos y cuantitativos del desarrollo del proyecto de grado Implementación de un Servidor Proxy para la Administración de la Red de Datos e Internet del Consulado General del Brasil.

Además de la experiencia ganada y aporte como guía para posteriores estudiantes del área de ACyT.

4.1. CONCLUSIONES

A través de las actividades realizadas, se ha logrado los siguientes resultados:

- Diagnostico total de la red de datos y el servicio de Internet, que sirvió para identificar las deficiencias en sus prestaciones, para proceder a su análisis y toma de decisiones respecto a la reestructuración parcial de la misma.

- Servidor Proxy SmoothWall Express 3.0. implementado, y utilizando políticas de monitoreo respectivos, se tomo decisiones en cuanto sitios navegados y proceder a sus restricciones, debido a que malgastaban y congestionaban el ancho de banda.
- Con la administración del Ancho de banda optimizado y contralado mediante el servidor, se logro ganar un 27.23 kbps, respectos a la velocidad obtenida en el diagnostico, lo cual optimizo el tiempo de cada funcionario al realizar sus cotidianas funciones.
- Servicio de Internet controlado y monitoreado, logrado gracias a nuestro modulo URLFilter, con la capacidad de controlar y hacer el respectivo seguimiento del tráfico conveniente.
- Minimización del tiempo respecto a los diferentes procesos por los que cada funcionario de la institución es responsable.
- Satisfacción por parte de la población que acude a la realización de los diferentes trámites, por la rapidez en la atención y entrega de sus documentos solicitados, además de las asistencias técnica.
- Reducción de Virus informáticos en los equipos informáticos (computadoras) del Consulado del Brasil**.**

- Políticas de uso de la red y el servicio de internet elaboradas

Al cumplimiento de los resultados, se mejoro los diferentes servicio que presta el Consulado General del Brasil por medio de la implementación del servidor proxy para la administración de la red de datos e de Internet tal cual fue planteado en el objetivo principal, con el monitoreo, control, corrección de fallas oportunamente, alcanzando así un satisfacción tanto en los funcionarios al desarrollar sus funciones diarias y en la población que a diario requiere los diferentes servicios, teniendo funcionamiento de las prestaciones de la red, aprovechamiento del ancho de banda de 27.23 kbps ganados respecto al diagnostico realizado, luego del control y monitoreo del mismo para lograr los procesamientos de los servicios solicitados por los usuarios.

4.2. RECOMENDACIONES

En tal sentido y con el propósito de mejorar el funcionamiento de la red de datos y el servicio de internet de la instalaciones de esta repartición diplomática. Se sugiere las siguientes recomendaciones:

- Ampliar el ancho de banda de conexión a internet. Debido a que el actual ancho banda con el que cuenta el consulado, es insuficiente para satisfacer las necesidades que tienen los usuarios para el uso del servicio de internet, respecto a otras necesidades secundarias.
- Debido a la importancia que tiene el del Departamento de Red de Datos e Internet para el normal funcionamiento de la red e internet, este debe contar con ambiente propio, con amplitud, además tratándose de una importantísima institución caso estudiado por el Itamaraty, de manera que pueda proporcionar comodidad, seguridad y sobre todo cumplir con normas y estándares internacionales, para que así tanto los equipos de red como el personal que trabaje en el puedan cumplir día tras día y con normalidad las funciones que desempeñan.
- Capacitación constante al personal de la Red de Datos y el Servicio de internet en la utilización y manejo de nuevas tecnologías de comunicación

- Aplicar mecanismos de seguridad eléctricas (puestas tierra), extintores, en la sala de donde están los equipos del consulado. para garantizar la confidencialidad, la autenticación, la integridad y el control de accesos.
- Compra y utilización de software original (Windows, Antivirus, Microsoft Office, firewall, etc). Los cuales no solo favorecerán la de Red de Datos e Internet si no al consulado como tal.

5.1. REFERENCIAS BIBLIOGRÁFICAS

BLIOGRAFÍA.

Behourz A. Forouzan, (2006). Transmisión de datos y redes de comunicaciones, cuarta edición, aravaca España.
David W. Chapman, (2002). *Academia Network Cisco Systems,* Guía del primer año segunda edición.
B. Mansfield; L. Mitchell, (1996). *Towards a Competent Workforce*, Hampshire, Gower.

JAMES A. F. STONER & CHARLES WANKEL, (1989). Administration, Tercera edition.

FUENTES ELECTRÓNICAS

Autor(es): Alice Naranjo S., (**2006**). Redes de computadoras, Naranjo.

http://www.monografias.com/trabajos5/redes/redes.zip
(Acceso 25/04/2010)
http://www.AprendaRedes.com
(Acceso 19/06/2010)

(Chávez, 2003)
Protocolos TCP/IP
Autor(es): JULIO CESAR CHÁVEZ URREA
http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml
(Acceso 10/08/2010)

(Dawson, 2000)
Direcciones IP, mascaras y clases
Autor(es): FERRY DAWSON
http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/index.html
(Acceso 10/08/2010)

(Alvarez, 2001)
Redes sociales
Outor: Miguel Angel Alvare
http://www.desarrolloweb.com/articulos/513.php
acceso 25/11/2010

REFERENCIAS BIBLIOGRÁFICAS

BLIOGRAFÍA.

Behourz A. Forouzan, (2006). Transmisión de datos y redes de comunicaciones, cuarta edición, aravaca España.

David W. Chapman, (2002). *Academia Network Cisco Systems,* Guía del primer año segunda edición.

B. Mansfield; L. Mitchell, (1996). *Towards a Competent Workforce*, Hampshire, Gower.

JAMES A. F. STONER & CHARLES WANKEL, (1989). Administration, Tercera edition.

FUENTES ELECTRÓNICAS

Autor(es): Alice Naranjo S., (**2006**). Redes de computadoras, Naranjo.

http://www.monografias.com/trabajos5/redes/redes.zip
(Acceso 25/04/2010)
http://www.AprendaRedes.com
(Acceso 19/06/2010)

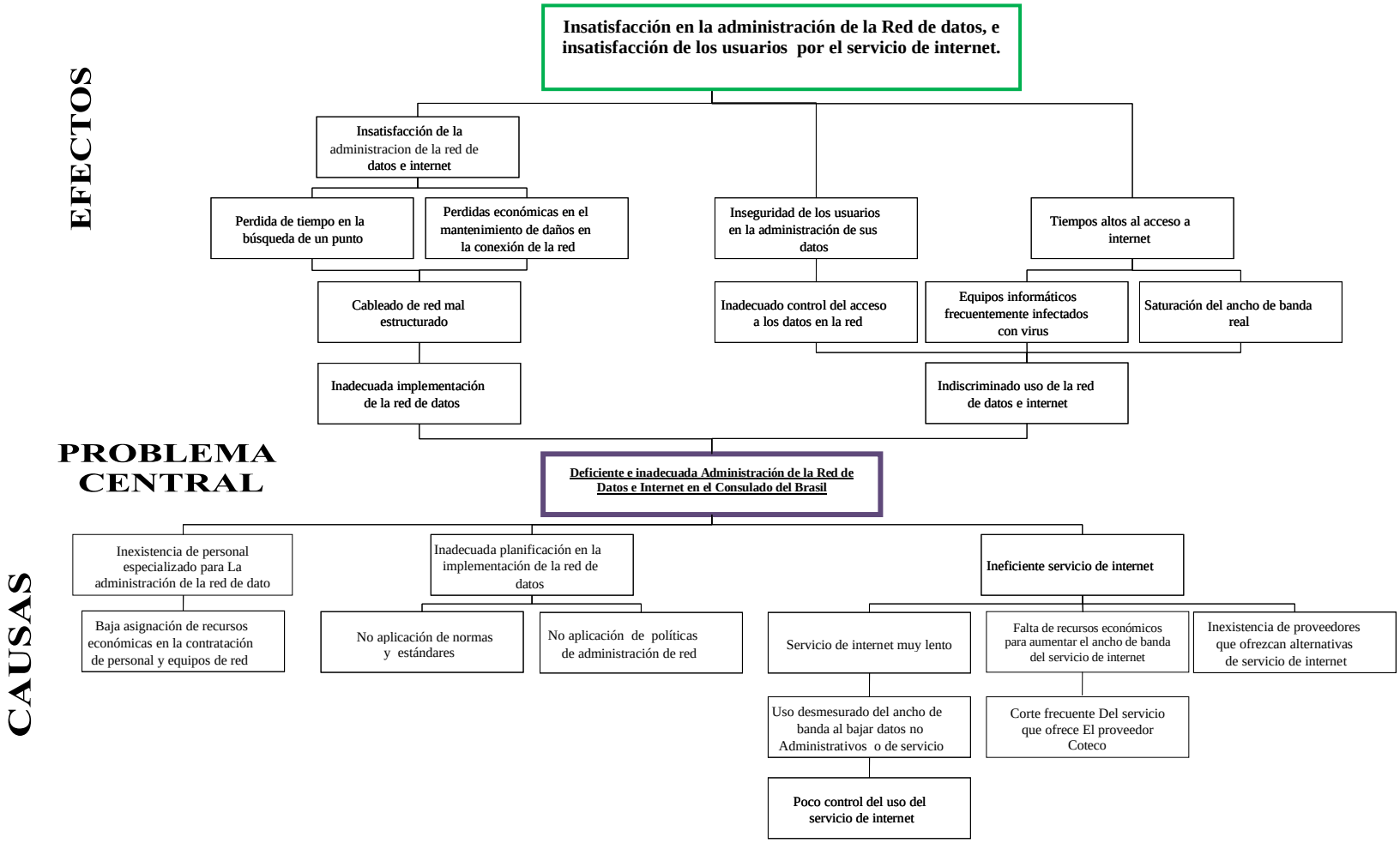
(Chávez, 2003)
Protocolos TCP/IP
Autor(es): JULIO CESAR CHÁVEZ URREA
http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml
(Acceso 10/08/2010)

(Dawson, 2000)
Direcciones IP, mascaras y clases
Autor(es): FERRY DAWSON
http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/index.html
(Acceso 10/08/2010)

(Alvarez, 2001)
Redes sociales
Outor: Miguel Angel Alvare
http://www.desarrolloweb.com/articulos/513.php
acceso 25/11/2010

ANEXO 1

ARBOL DE PROBLEMAS



ANEXO 1

ARBOL DE OBJETIVOS

FIN

FINES

Garantizar la conectividad de los sistemas de información y comunicación del Consulado del Brasil en Cobija

Satisfacción en la administración de La red de Dato e Internet

Satisfaccion de los usuarios en sus funciones cotidiana.

Tiempos bajos al acceso a la información requerida desde Internet.

Facilidad de ubicación de un punto

Gastos mínimos en el mantenimiento de la Red

Políticas de acceso a la Red de Datos

Optimo uso de la Red de datos e Internet

Ancho de Banda descongestionada.

Cableado estructurado de la Red de Datos

OBJETIVO GENERAL

Implementar un Servidor proxy, para la Administración de la Red de Datos e Internet del Consulado General del Brasil en Cobija, mediante la metodología del modelo funcional, garantizando el buen funcionamiento de los sistemas de información.

MEDIOS

Implementación de un servidor proxy

Reconfiguración de la Red de Datos

Controlar acceso de usuarios

Monitoreo del servicio de internet.

Planificación de la red

Diseñar la topología de la red

Administrar el rendimiento de la red

Administrar las posibles fallas de la red

Experiencia en el área de redes

Tabla 2. Metodología y herramientas utilizadas

Fuente: Elaboración Propia

Proceso de la Metodología	Actividades de cada proceso	Objetivos específicos	Relación entre actividades y objetivos	Herramienta utilizada en cada actividad
Administración de la Configuración	• Planeación y diseño de la red	• Evaluar el estado y las prestaciones de la red datos consulado	• Evaluar el funcionamiento de la red de datos del consulado del Brasil. • Detectar fallas en el nivel de rendimientos de las prestaciones.	• Encuestas a los usuarios con preguntas cerradas. • Observación
	• Selección de la infraestructura de red y el gabinete central, instalación y configuración de software	• Reestructuración de la red.	• Para un buen funcionamiento en la red de datos y sus prestaciones.	• Switch, cable de red UTP cat. 5e, conectores RJ-45, equipo informático (computadora), pack panel, rack, etc.

	• Elaboración de políticas y normas para la administración de la red.	• Mejorar la organización normativa del uso de la red de datos y el servicio de Internet.	• Que la aplicación del documento de políticas de red e internet sirva para el control del uso de los mismos.	• Elaboración de un documento sobre políticas sobre el uso de la red.
Administración del Rendimiento	• Monitoreo	• Implementación y configuración de un servidor proxy para la administración de internet.	• La finalidad es de obtener información referente al servicio de internet.	• Monitoreo del servicio de internet
	• Análisis		• Tiene la finalidad controlar acceso a internet de usuarios, restricción de paginas indebidas, priorizar usuarios, etc.	• CPU Pentium IV, Intel y Software SmoothWall Express 3.0, con Open Source, disponible para todo el mundo y de manera gratuita.
Administración de fallas	• Monitoreo de alarmas.	• Gestión eficiente de la de Red de Datos del Consulado del Brasil.	• La finalidad de esta actividad fue dar a los usuarios del Consulado apoyo técnico especializado en redes e internet.	• Testeador de cable de red, alicate de red, utilización del ping y la verificación física
	• Localización de fallas.		• La finalidad de esta actividad es dar a los usuarios de la red apoyo técnico especializado en redes e internet.	• Testeador de cable de red, alicate de red, utilización del ping y la verificación física.
	• Corrección de fallas.		• La finalidad de esta actividad fue dar a los usuarios del hospital apoyo técnico especializado en redes e internet.	• Testeador de cable de red, alicate de red, utilización del ping y la verificación física

ANEXO 3

Tabla 1. Metodología y herramientas utilizadas

Fuente: Elaboración Propia

Operabilización de variables

Variables	Concepto	Dimensión	Indicador	Instrumentos
• **Sistemas de información Actuales**	Se refiere a la descripción de los actuales sistemas con los cual cuenta el Consulado del brasilero, como es el SCI, SCEDV y el de comunicación.	• **Tipos de sistema** • **Conexión a la red.**	• **Funcionalidad del SCI (Sistema Consular Integrado), e internet.** • **Sistema SCEDV (sistema de Control de emisión de documentos de viajes).**	**Encuestas, entrevistas, observación.**
• **Personal**	**Personal**, el grupo de personas que forman una empresa, institución, o algo parecido.	✓ **Conocimientos en ofimática** ✓ **Conocimient**	• **Formación Profesional** • **Experiencia laboral**	**Encuestas, entrevistas, observación.**

ANEXO 3

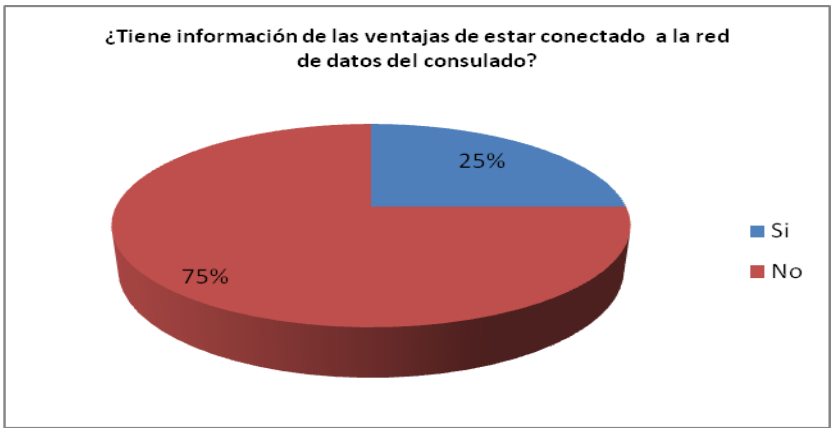
		os sobre redes e internet	• **Cursos de capacitación** • **Experiencia laboral**	
• **Organización**	Organización: Es un sistema de actividades conscientemente coordinadas formado por dos o más personas la cooperación entre ellas es esencial para la existencia de la organización.	• **Elaborar políticas de red.** • **Administrar del servicio de Internet**	• **Control del buen uso a la red por los usuarios.** • **Servicio de internet** • **Priorizar acceso de usuarios.**	**Implementación de un servidor proxy.**
• **Estructura de la Red**	Es la interconexión de varias computadoras y periféricos. El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.	• **Planificar** • **Organizar** • **Diseñar la topología.**	• **Según Normas, estándares.** • **Experiencia en el área.**	• **Materiales de hardware de red.** • **Software Microsoft office Visio.**

DIAGNÓSTICOS DE LA RED DE DATOS E INTERNET DEL CONSULADO BRASILERO

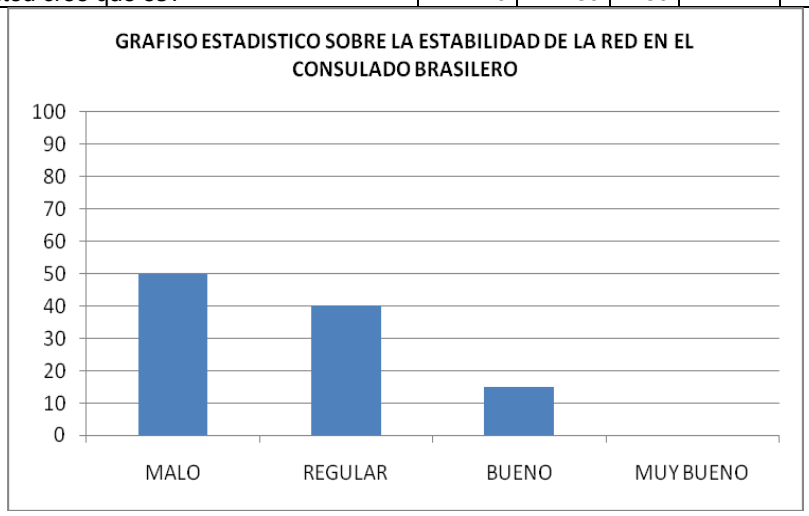
A continuación se describe el diagnostico realizado respecto a la red de datos del Consulado, descripción respecto al diagnostico realizado al servicio de internet, respecto al personal y su formación y conocimientos en informática y otras.

Datos tabulados

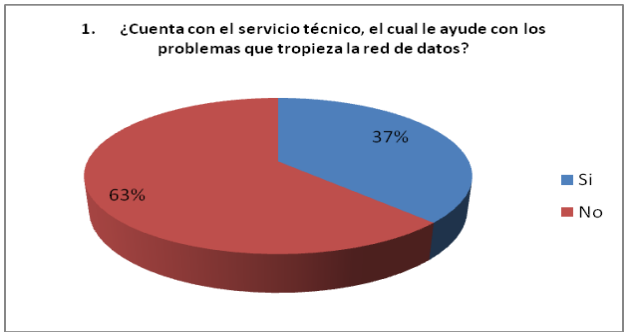
Nº	Pregunta	Si	No	Total
1	¿Tiene información de las ventajas de estar conectado a la red de datos del consulado?	2	6	8



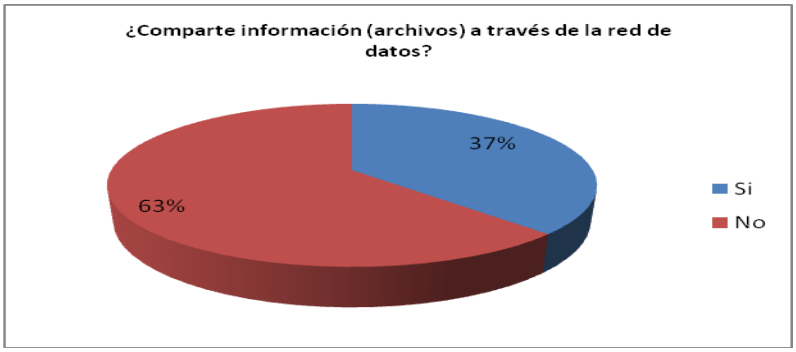
Nº	Pregunta	Buena	Regular	Mala	Muy buena	Total
5	¿Respecto a la conectividad y estabilidad de la red usted cree que es?	20	30	50		100



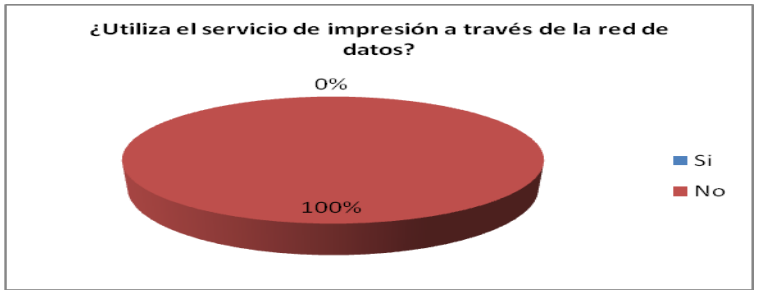
Nº	Pregunta	Si	No	Total
3	¿Cuenta con el servicio técnico, el cual le ayude con los problemas que tropieza la red de datos?	3	5	8



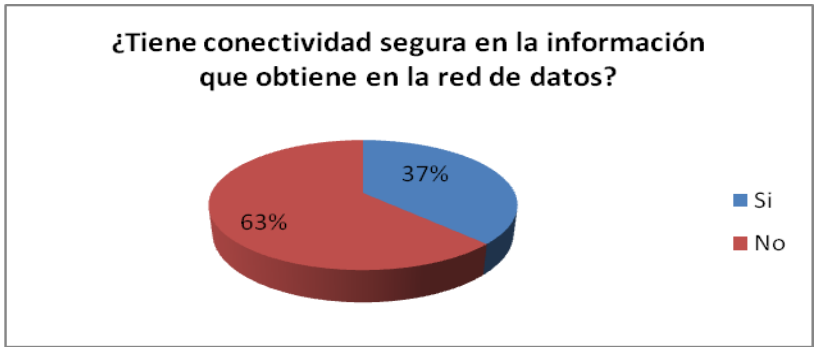
Nº	Pregunta	Si	No	Total
4	¿Comparte información (archivos) a través de la red de datos?	3	5	8



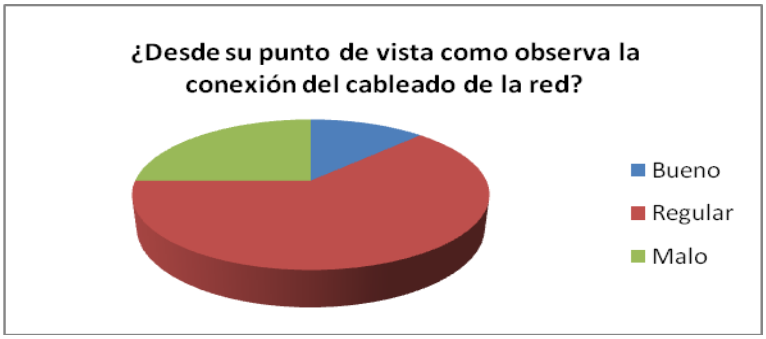
Nº	Pregunta	Si	No	Total
5	¿Utiliza el servicio de impresión a través de la red de datos?	0	8	8



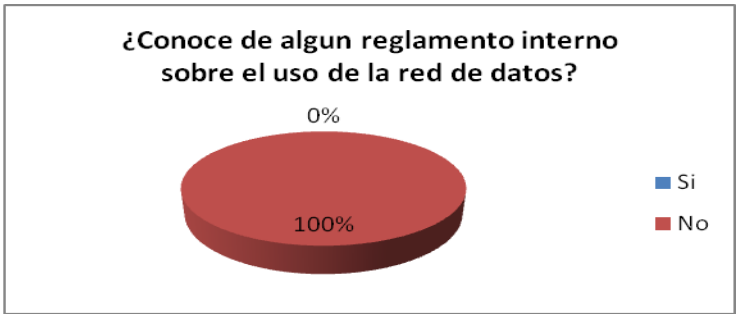
Nº	Pregunta	Si	No	Total
6	¿Tiene conectividad segura en la información que obtiene en la red de datos?	3	5	8



Nº	Pregunta	Bueno	Regular	Malo	Total
7	¿Desde su punto de vista como observa la conexión del cableado de la red?	1	5	2	8

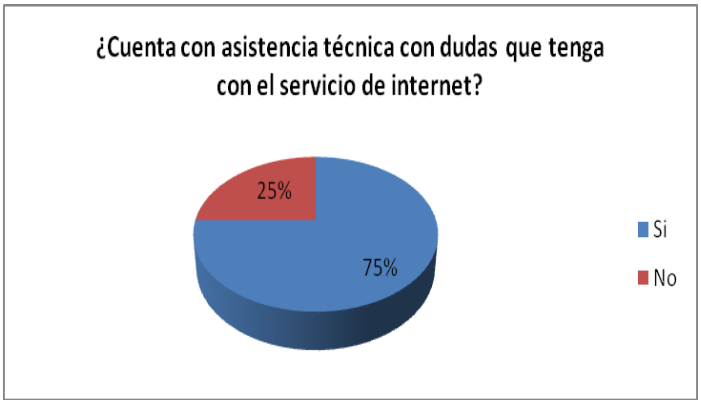


Nº	Pregunta	Si	No	Total
8	¿Conoce de algún reglamento interno sobre el uso de la red de datos?	0	8	8

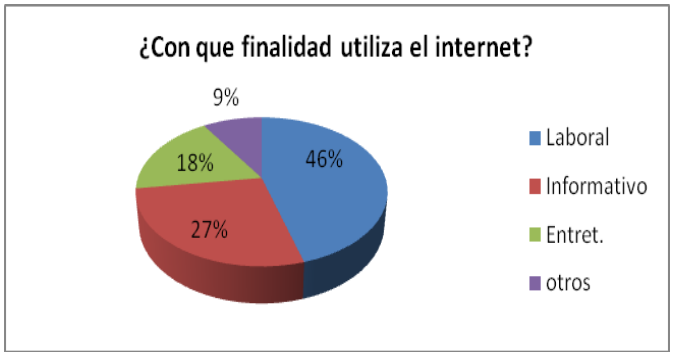


Descripción respecto al diagnostico realizado al servicio de internet del Consulado:

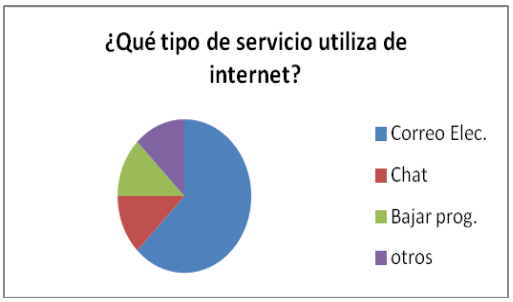
Nº	Pregunta	Si	No	Tatal
1	¿Cuenta con asistencia técnica con dudas que tenga con el servicio de internet?	6	2	8



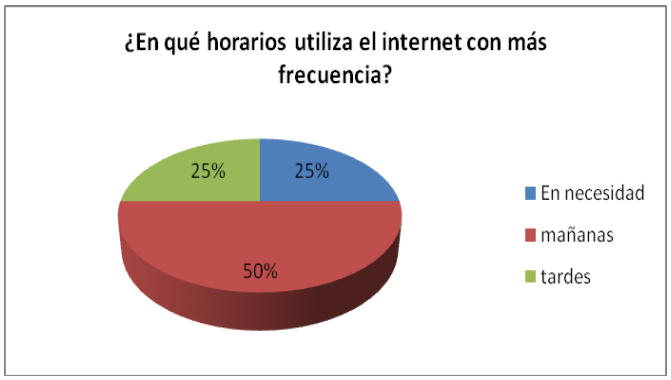
Nº	Pregunta	Laboral	Informativo	Entret.	otros	Total
2	¿Con que finalidad utiliza el internet?	5	3	2	1	8



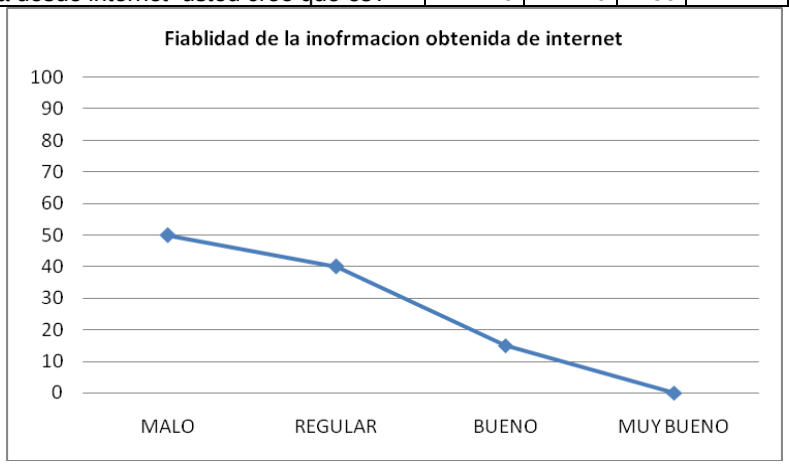
Nº	Pregunta	Correo Elec.	Chat	Bajar prog.	otros	Total
3	¿Qué tipo de servicio utiliza de internet?	5	1	1	1	8



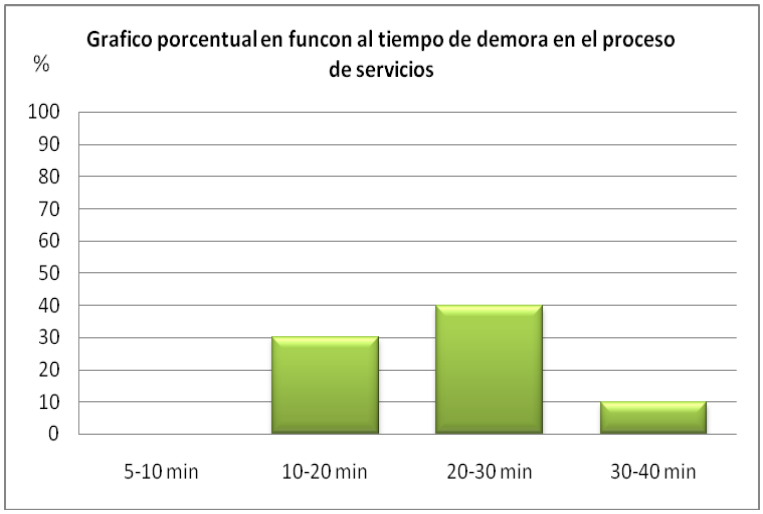
Nº	Pregunta	En necesidad	mañanas	tardes	otros	Total
4	¿En qué horarios utiliza el internet con más frecuencia?	2	4	2		8



Nº	Pregunta	Buena	Regular	Mala	Muy buena	Total
5	¿Respecto a la fiabilidad de la información obtenida desde internet usted cree que es?	10	40	50		100

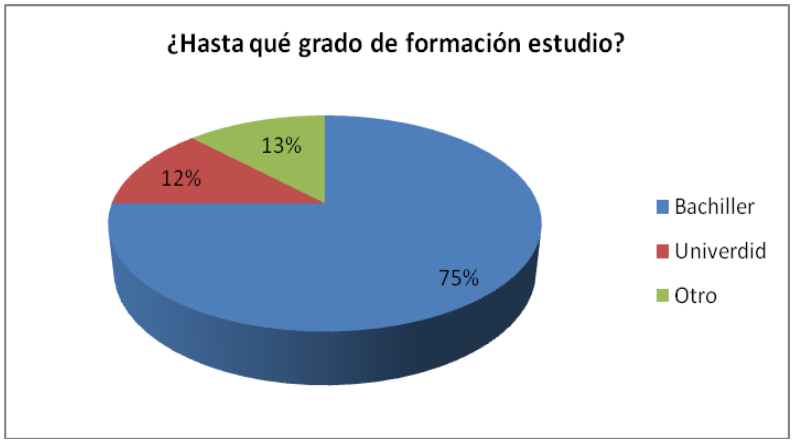


Nº	Pregunta	5-10 min	10-20 min	20-30 min	30-40 min	Total
6	¿Cuánto tiempo demora en procesar un servicio (pasaporte, visa, actos notariales, etc.) con el servicio de internet?	0	3	4	1	8

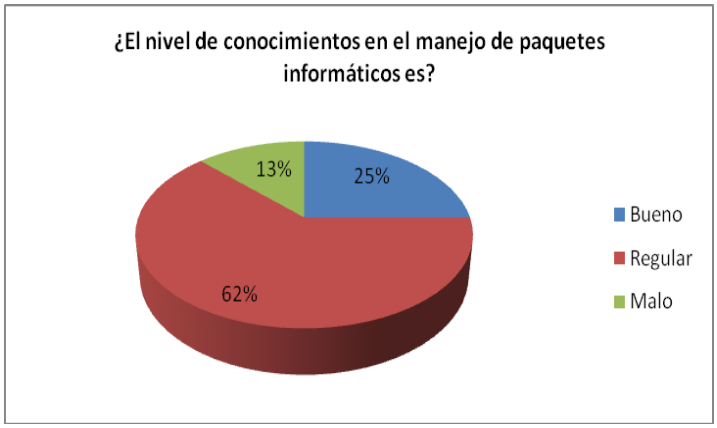


Diagnostico respecto al personal y su formación y conocimientos en informática del Consulado:

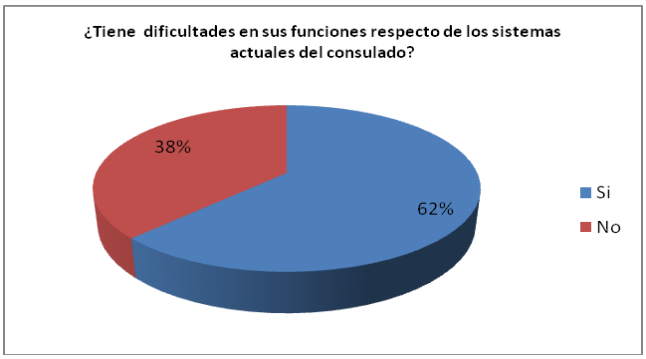
Nº	Pregunta	Bachiller	Univerdid	Otro	Total
1	¿Hasta qué grado de formación estudio?	6	1	1	8



Nº	Pregunta	Bueno	Regular	Malo	Total
2	¿El nivel de conocimientos en el manejo de paquetes informáticos es?	2	5	1	8

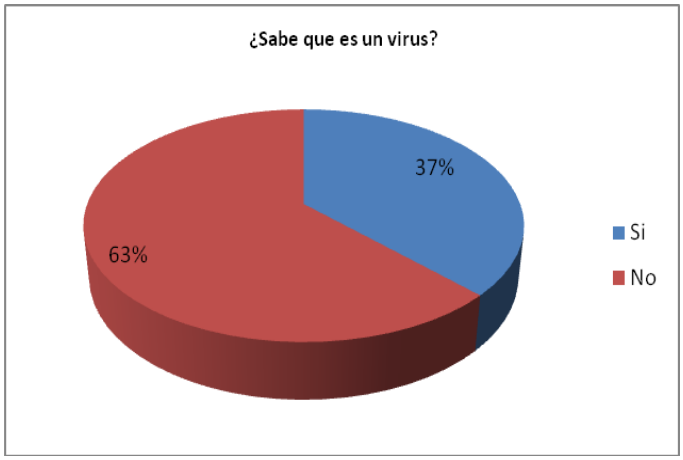


Nº	Pregunta	Si	No	Tatal
3	¿Tiene dificultades en sus funciones respecto de los sistemas actuales del consulado?	5	3	8

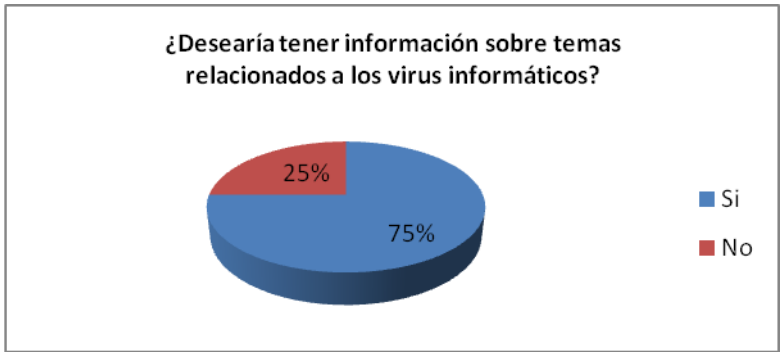


Otras preguntas complementaria

Nº	Pregunta	Si	No	Tatal
4	¿Sabe que es un virus?	3	5	8



Nº	Pregunta	Si	No	Total
5	¿Desearía tener información sobre temas relacionados a los virus informáticos?	6	2	8



Nº	Pregunta	Si	No	Tatal
6	¿Sabe cuando una computadora está infectada con virus?	3	5	8

Conclusiones del Diagnostico

De acuerdo a los requerimientos que se obtuvo del levantamiento la información se plantea las siguientes conclusiones:

- Mejorar el Servicio de Internet.
- Reestructurar parcialmente la red de datos.
- Implementar el Servidor Proxy.
- Elaborar e implementar políticas de uso de la Red de Datos y el Servicio de internet.
- Brindar asistencia técnica a los usuarios de forma rápida e inmediata.

POLITICAS DE USO DE LA RED CONBRAS

Introducción:

Las siguientes políticas servirán como referencia y en ningún momento pretenden constituirse como normas absolutas. Todos aquellos actos que se consideren como violaciones a las normativas vigentes (Leyes de la republica del Brasil, reglamento del Consulado general del Brasil y/o cualquier otra disposición debidamente establecida en el ámbito laboral) y que no mencionen expresamente en este documento, están prohibidas.

Al utilizar la red del Consulado, se espera que el usuario (funcionario del cuadro como Administrativos locales) use los servicios con respeto, cortesía y responsabilidad, en procura de no vulnerar los derechos de los derechos de los demás usuarios de la red.

Toda persona que utilice los servicios que ofrece la red CONBRAS deberá conocer y aceptar el reglamento vigente sobre su uso. El desconocimiento del mismo no **exonera** de las responsabilidades asignadas.

Las autoridades consulares y administrativas y en particular el de Red de Datos e Internet, se comprometen a publicar y difundir estas políticas de uso para y entre los usuarios de los bienes y recursos informáticos provistos a través de la red CGCOBIJA.

Los casos no provistos por el presente reglamento serán resueltos la autoridad consular del consulado como encargado de la Red de Datos e Internet y la situación lo amerita.

Definiciones de Términos:

1. **Red CONBRAS**: Es el nombre dado al conjunto de instalaciones y recursos informáticos del Consulado General del la Republica Federativa del Brasil particularmente. También hacen parte de ella la infraestructura de telecomunicaciones y los servicios teleinformáticos prestados por otras dependencias de la sede y que se encuentren bajo la supervisión del Centro de Cómputo.

2. **Usuario:** Se entiende por usuarios de la red, todo ente que reciba o provea información a través de la Red **CONBRAS**; en particular, caben bajo esta denominación, las dependencias consulares administrativas y las personas que tengan alguna vinculación laboral con el publico requerente de los servicios y cumplan con los requerimientos de acceso a la Red. Las presentes políticas serán aplicadas a todos los usuarios.

   El Departamento de Red de Datos e Internet divide a dos tipos de usuarios:

   Usuarios con Privilegio: Vice-Cónsul, Vice-Cónsul a.i, Vice-Cónsul a.i, agentes de atendimiento, y Secretarios, Oficiales de Cancillería, Asistente de Cancillería, designados por misiones temporales a esta Repartición Consular.

   Usuarios sin Privilegio: Auxiliares locales, personas ajenas a esta repartición consular

3. **Servicio:** Se entiende por servicio, los aplicativos y/o conjuntos de programas (software) que apoyan la labor consular administrativa del quehacer cotidiano de los usuarios que requieran y/o proveen información a través de la Red CONBRAS.

4. **Recurso:** Cualquier insumo involucrado en la prestación de los servicios asociados a la red CONBRAS.

Personal Autorizado:

Están autorizados a utilizar los **servicios** de la Red CONBRAS, todo el personal de esta repartición consular, ocasionales y externos autorizados). La clasificación de usuarios es la siguiente:

- Vice-Cónsules
- Personal de Cuadro Oficial.
- Agentes de atendimiento locales
- Dependencias administrativas.

Uso de los servicios en la Red CONBRAS

I. De los recursos

La infraestructura de la Red CONBRAS se utilizara únicamente para desarrollos actividades de servicio consulares, técnicos y administrativos de la institución, incluyendo los actos promociónales de la misma, así como actividades que contengan insumo designado por el Ministerio de Relaciones Exteriores. Así mismo los recursos de la Red CONBRAS solo podrán ser usados de acuerdo con lo previsto por las normas de manejo de bienes de este Consulado, las políticas presentadas en este documento y todas las demás normativas asociadas a las mismas.

Se prohíben, salvo previa autorización y supervisión expresa de la autoridad consular encargada de la Red de Datos e Internet, la intervención física de los usuarios sobre los recursos de la Red CONBRAS (Cables, enlaces, equipos activos y/o pasivos) y el acceso a los centros de cableado de los edificios.

Los recursos asociados a la Red CONBRAS solo podrán utilizarse para propósitos legales.

II. Usos inaceptables

- Envió de material ofensivo o contenidos difamatorios.
- Transmisión de información de terceros sin previa autorización de la autoridad competente.
- Acoso informático y/o electrónico a cualquier miembro usuario de la red.
- Difusión de información de carácter comercial o cualquier otra forma que representa un lucro para la persona que lo origina o la procura.
- Difusión de material obsceno o que incite a la violencia.+

III. Seguridad del Sistema y de la Red

Se prohíbe cualquier tipo de acción o comportamiento que vaya en contra de la seguridad física y/o lógica de los recursos asociados a la red CONBRAS. Dichos comportamientos podrán acarrear sanciones institucionales, civiles y/o penales y no se encuentran limitados a los siguientes:

- Acceso, uso, puesta a prueba o exploración no autorizada de los servidores, dispositivos o aplicaciones comprometidas en la prestación de los servicios de la Red CONBRAS.
- Bombardeo de correo (uso de mail bombers), inundación de trafico, intentos de denegación de servicio y/o difusión de virus, troyanos o cualquier otro tipo de software malicioso a usuarios, redes y/o servidores de la Red CONBRAS o de cualquier otra red de Internet.
- Realizar cualquier tipo de suplantación mediante información falsa a nivel de direcciones (MAC)[1], encabezados IP o TCP y/o encabezados a nivel de datos de protocolos de aplicación.
- Cambios en las configuraciones de hardware o software de la red, que puedan ocasionar inestabilidad o caídas en el rendimiento de la Red o de otros recursos comprometidos en la prestación de servicios a través de la misma.

Todos los usuarios de la red deberán acogerse a las políticas de seguridad establecidas y difundidas por la autoridad competente de Red de Datos e Internet.

IV. De los derechos y responsabilidades de los usuarios de la Red

Derechos:

- Los usuarios internos pueden utilizar los recursos de la red con las limitantes consignadas en el punto de usos inaceptables.
- Los usuarios dispondrán de pleno acceso a los recursos de la red, de acuerdo a lo consignado en el presente documento y en las normativas asociadas.
- Los usuarios gozan la privacidad de su información, con la salvedad de aquellos casos en que se detecten acciones que pongan en riesgo la seguridad de la Red CONBRAS o de cualquier otra red.
- Los usuarios podrán acceder a Internet, cobijados bajo las políticas implementadas mediante firewall y proxy diseñada por la administración de Red de Datos e Internet para brindar seguridad a la red CONBRAS y hacer un buen uso del ancho de banda.

Responsabilidades:

- El usuario velará por asegurar que sus archivos cuenten con protecciones para escritura, lectura ejecución adecuadas.

[1] (Control de Acceso al Medio)

- EL usuario debe asegurar de acatar las disposiciones dictadas en las políticas de seguridad con referencia a este tipo de protección y que el software y medios que introduzcan en la Red CONBRAS no contengan virus.
- Cualquier cambio en el hardware de red de estación de trabajo deberá ser notificado a la Red de Datos e Internet en un lapso no mayor de 1 hora después de efectuar dicho cambio.
- Los usuarios no deben alterar o corromper información ajena.
- Es responsabilidad del usuario realizar el respaldo de su información.

V. De las restricciones de uso

Dadas las limitantes que existen en lo que tiene que ver con la cantidad de recursos informáticos disponibles en el consulado, se formulan algunas restricciones asociadas a los mismos, sin prejuicio de las que puedan surgir como parte de las necesidades de servicio.

Restricciones asociados al acceso a los servicios

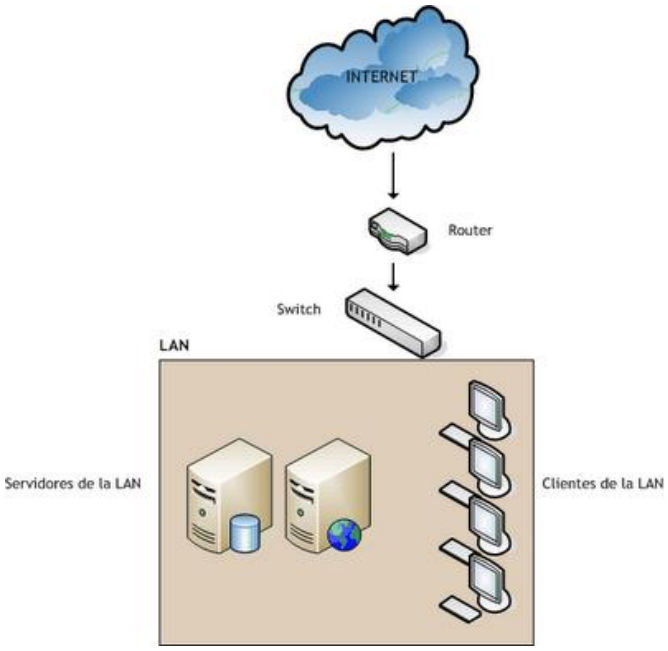
- El servicio de mensajería (messenger) se habilitara solo en horarios fuera del establecido para las funciones cotidianas. de lunes a viernes, esta medida servirá para el mejoramiento de los demás servicios que nos brinda Internet. Esta medida se optara con los usuarios sin privilegios.
- El servicio de mensajería(messenger) esta habilitado en el horario de oficina en los siguientes horarios 09:00 a 18:30 p.m. Esta medida servirá para el mejoramiento de los demás servicios que nos brinda Internet. Esta medida se optara con los usuarios con privilegios.
- El tiempo de conexión a la Red CONBRAS y los servicios que esta ofrece no tendrán ningún costo para los miembros de la esta repartición consular, con excepción a las personas que hacen uso del Servicio de Internet del consulado.
- La reubicación de equipos de red, inicialización de servidores cambio de parámetros en configuraciones de equipos activos de la red y la instalación y modificación de redes físicas al interior de la Red CONBRAS serán competencia y responsabilidad exclusiva del personal del encargado de la administración de Red de Datos e Internet; la instalación de nuevos equipos con conexión a la Red CONBRAS deberá ser notificado previamente a la autoridad competente.

Restricciones asociadas de las páginas de web

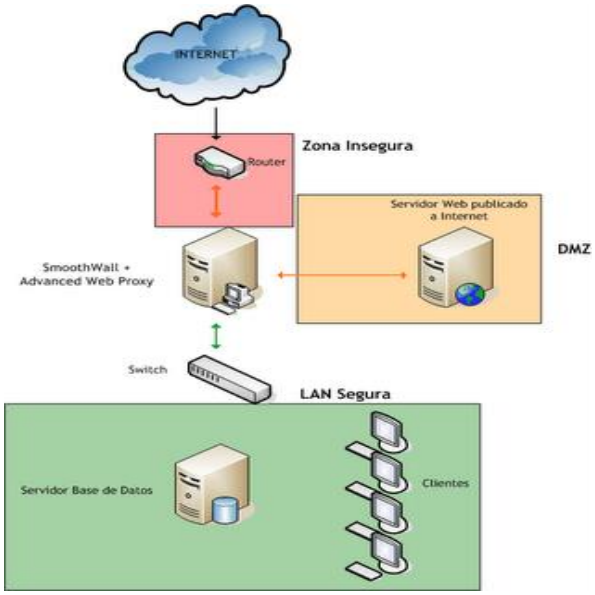
- Se prohíbe el acceso a páginas con contenido erótico (xxx).

Guía de instalación y Configuración del
Servidor Proxy SmoothWall Express 3.0

Escenario de partida:
Nuestro escenario de partida es el siguiente:

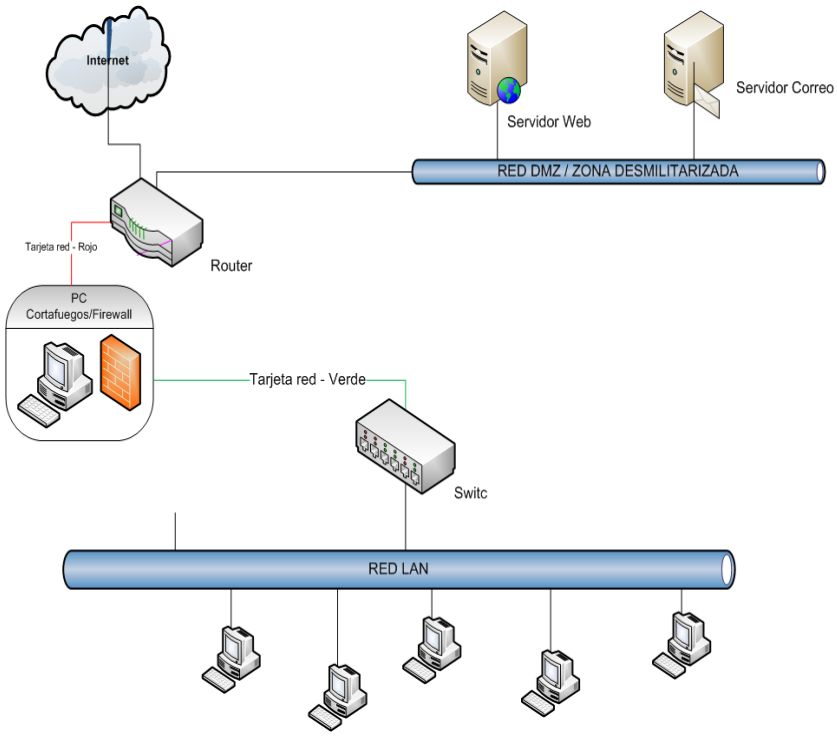


Escenario Objetivo:
Nuestro objetivo será llegar a un escenario como este:



Esquema y explicación general sobre cómo montaremos el firewall en nuestra LAN

A continuación mostramos y explicamos cómo montaremos un firewall mediante **GNU Linux SmoothWall**, que servirá para controlar todo el tráfico de nuestra red LAN (red local):



En primer lugar, a nuestro equipo (el que usemos como cortafuegos), le pondremos **dos tarjetas de red**, esto es imprescindible para poder montar el firewall. Prepararemos el **router**, conectaremos una de las tarjetas de red del equipo cortafuegos al router (será la tarjeta "roja", más adelante explicaremos este concepto). Prepararemos el **switch** (si aún no lo tenemos) y conectaremos la otra tarjeta de red al switch (será la "verde").

Quitaremos cualquier cable de red que vaya desde el switch al router pues ambos **NO DEBEN ESTAR CONECTADOS entre sí**. Todos los equipos de nuestra red estarán conectados al switch, nunca al router, salvo los equipos que queramos "poner" en la zona DMZ (desmilitarizada), que serán aquellos propensos a ataques externos (como un servidor de páginas web o un servidor de correo electrónico). Estos equipos de la DMZ quedarán aislados de nuestra red LAN, de esta forma, si se produce un ataque con éxito a uno de estos equipos, el atacante no podrá tener acceso a nuestra LAN, donde residirán los datos realmente importantes de nuestra organización.

Básicamente, la idea es que todo el tráfico de red de Internet, tanto peticiones desde fuera hacia dentro como desde dentro hacia fuera: navegación web, correo electrónico, FTP, chat, etc. pasen únicamente a través de la tarjeta de red verde hacia nuestro equipo cortafuegos y éste, conectará y transferirá todo ese tráfico al router mediante la tarjeta de red roja. De esta

forma todo el tráfico de Internet pasará a través de los cortafuegos, para que éste controle y gestione las reglas que luego podremos añadirle.

Requisitos necesarios (hardware y software) para montar un firewall en la red

Componentes hardware básico para el firewall o cortafuegos

1. Equipo de sobremesa sencillo, puede servir incluso un Pentium II a 400MHz, con unos 8GB de disco duro y 512MB de memoria RAM, sólo necesitaremos el monitor para la instalación, una vez instalado y configurado el cortafuegos ya no será necesario el monitor, pues se podrá administrar vía web desde cualquier otro equipo de la red, en nuestro caso contamos un equipo más actualizado.
2. Dos tarjetas de red para el equipo anterior.
3. Dos latiguillos de cable de red para conectar las dos tarjetas al router y al switch.
4. Un modem o cualquier otro tipo de dispositivo para conexión a Internet, sólo el equipo con los cortafuegos o firewall irá conectado a este modem.
5. Un switch o varios donde irán conectados todos los equipos de nuestra red y también el segundo cable de red de la segunda tarjeta de red de nuestro equipo con el firewall.

Componentes software para el firewall o cortafuegos

Como componente software sólo necesitaremos descargar una distribución de GNU Linux específica para ser utilizada como cortafuegos o firewall para todos los equipos de nuestra red. Dicha distribución es: **SmoothWall Express** (gratuita).

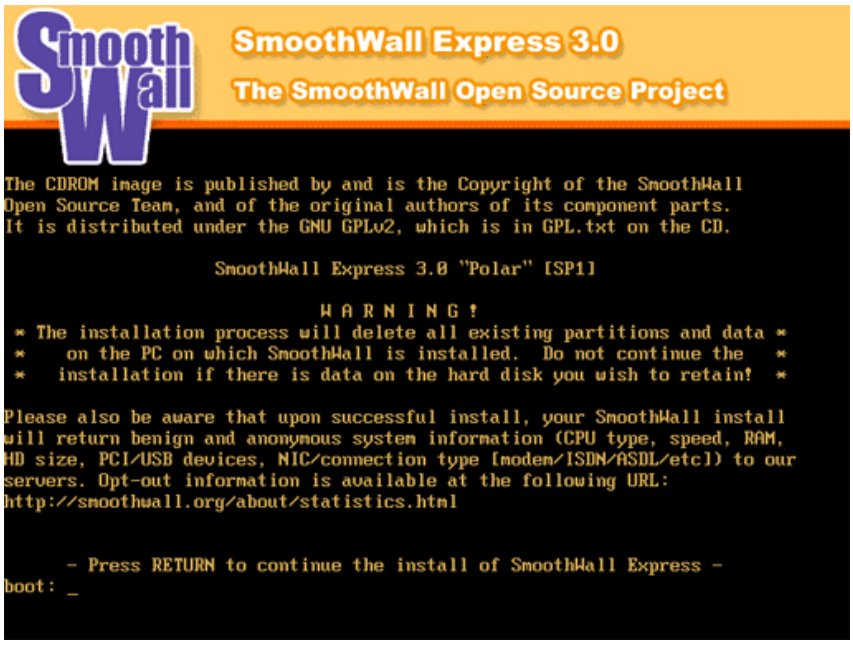
Descargaremos el fichero ISO desde:

http://www.smoothwall.org/get

En nuestro caso, descargaremos la versión: ***SmoothWall Express 3.0 SP1 Released – 8th January 2009***.

Instalar el firewall SmoothWall Express en un equipo

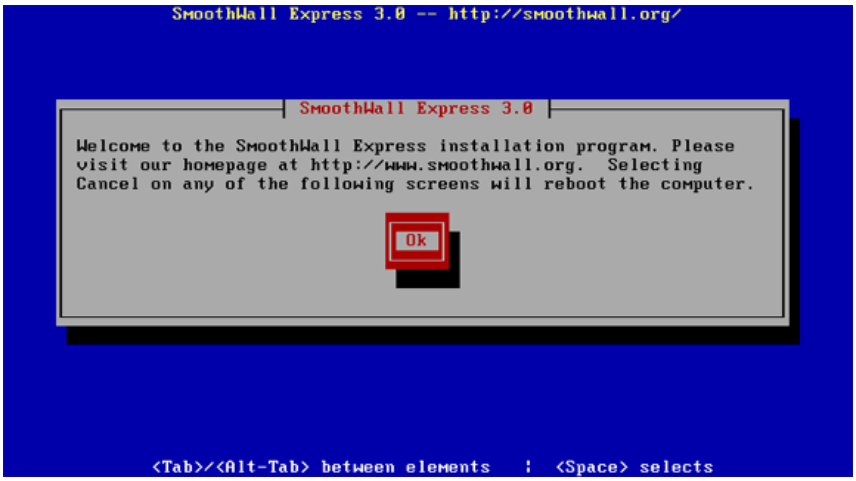
Una vez descargado SmoothWall Express 3.0 y generado el CD correspondiente con la imagen ISO, lo introduciremos en el equipo que utilizaremos de firewall o cortafuegos y arrancaremos desde el CD, aparecerá la siguiente ventana de inicio de SmoothWall Open Source Project:



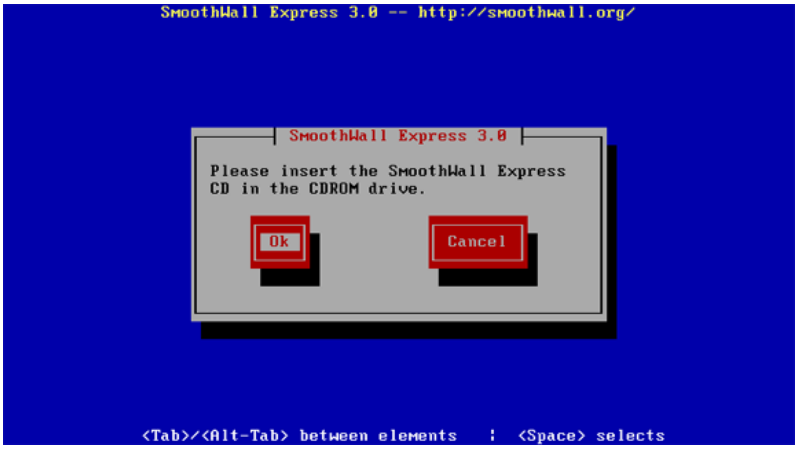
La pantalla anterior avisa de que los datos del disco duro del equipo serán **eliminados** para instalar el nuevo sistema, obviamente esto hay que tenerlo en cuenta y haber hecho copia de seguridad de los datos (si los hubiera) del disco duro del equipo. Pulsaremos INTRO para iniciar la instalación de los cortafuegos SmoothWall Express.

Nos mostrará la ventana de bienvenida, con el texto: "Welcome to the SmoothWall Express installation program. Please visit our homepage at http://www.smoothwall.org. Selecting Cancel on any of the following screens will reboot the computer.".

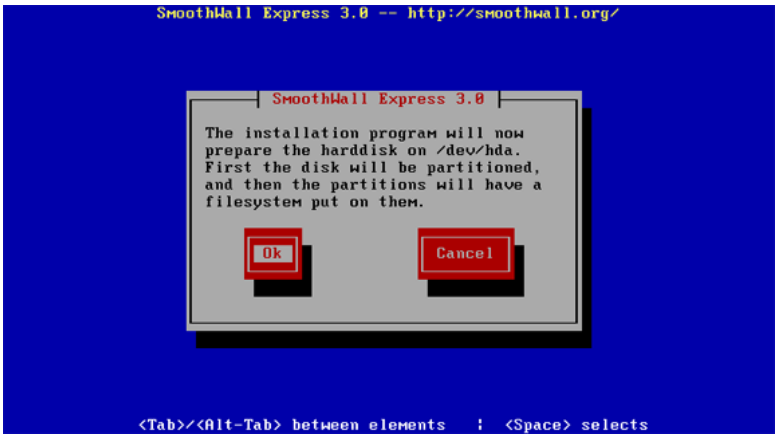
Pulsaremos "Ok" (pulsando la barra espaciadora o INTRO, en la instalación no funcionará el ratón):



Nos indicará que introduzcamos el CD de SmoothWall express, puesto que ya lo tenemos pulsaremos "Ok" (pulsando INTRO o barra espaciadora):

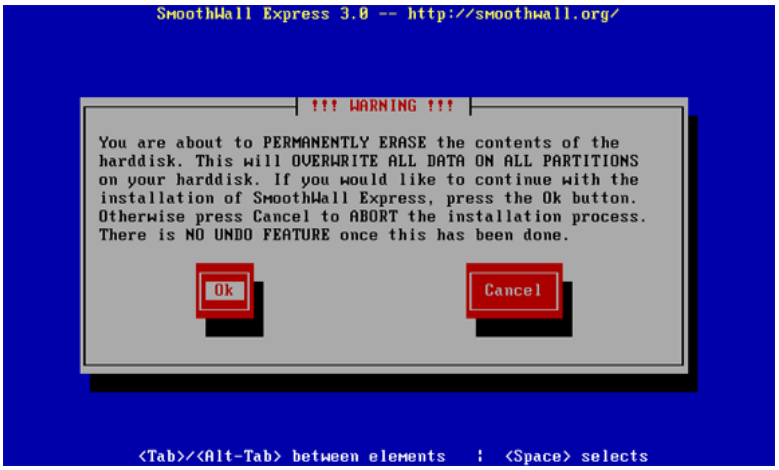


A continuación nos avisará de que se preparará el disco duro /dev/hda para ser particionado, con el texto: "The installation program will now prepare the harddisk on /dev/hda. First the disk will be partitioned, and then the partitions will have a filesystem put on them". Pulsaremso "Ok":

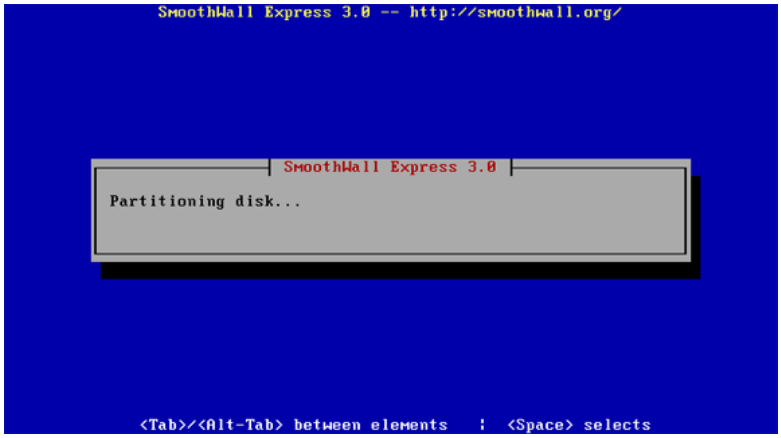


Nos volverá a avisar de que el proceso de particionado eliminará todos los datos del disco duro, con el texto: "You are about to PERMANENTLY ERASE the contents of the harddisk. This will OVERWRITE ALL DATA ON ALL PARTITONS on your harddisk. If you would like to continue with the installation of SmoothWall Express, press the Ok button. Otherwise press Cancel to ABORT the installation process. There is NO UNDO FEATURE onde this has beed done".

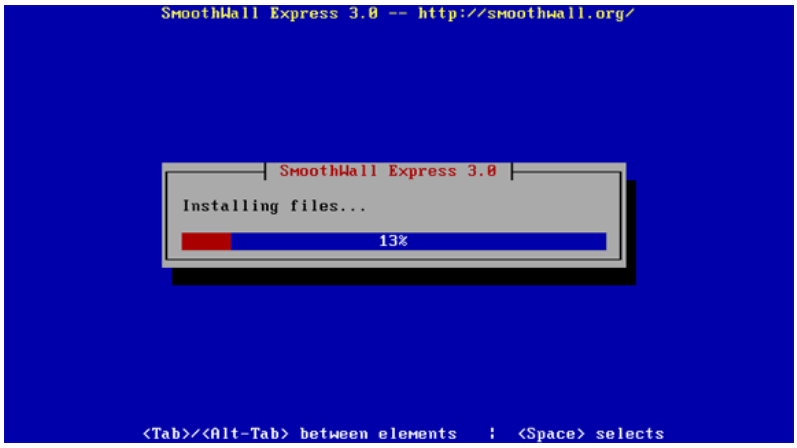
Pulsaremos "Ok" para continuar:



Se iniciará el proceso de preparación y particionado del disco:



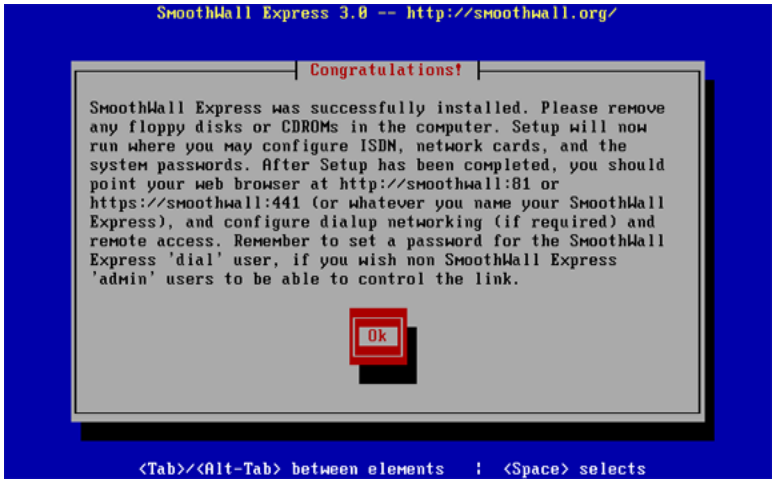
Tras el particionado y formateo, se iniciará la instalación de los ficheros necesario para el funcionamiento del firewall o cortafuegos de SmoothWall Express:



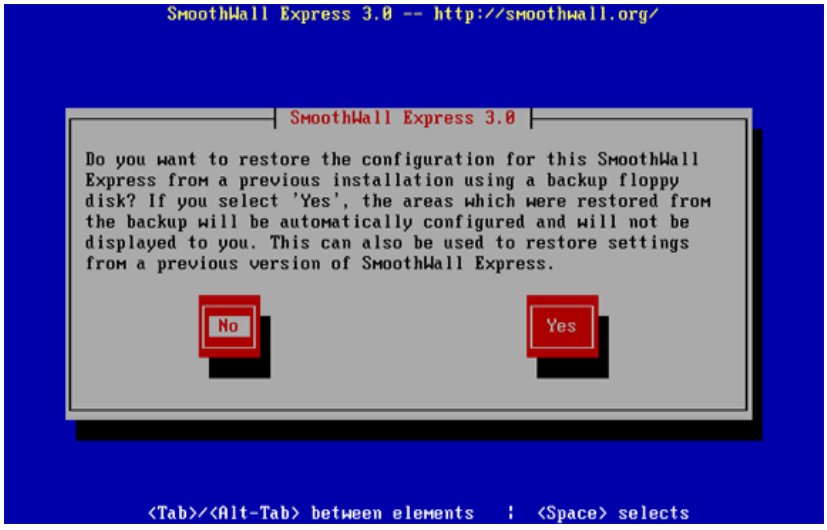
Una vez instalado, nos avisará de que extraigamos el CD de instalación y pulsaremos Ok para iniciar el proceso de configuración de SmoothWall, con el texto "SmoothWall Express was sucessfully installed. Please remove any floppy disks or CDROMs in the computer.

Setup will now run where you may configure ISDN, network cards, and de system passwords. After Setup has been completed, you should point your web browser at http://smoothwall:81 or https://smoothwall:441 (or whatever you name your SmoothWall Express, and configure dialup networking (if required) and remote access. Remember to set a password for the SmoothWall Express 'dial' user, if you wish non SmoothWall Express 'admin' users to be able to control the link".

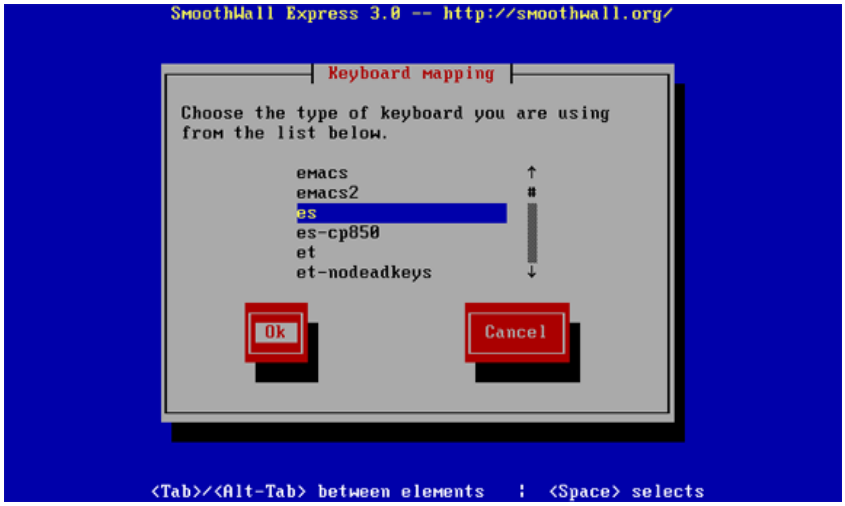
Pulsaremos "Ok":



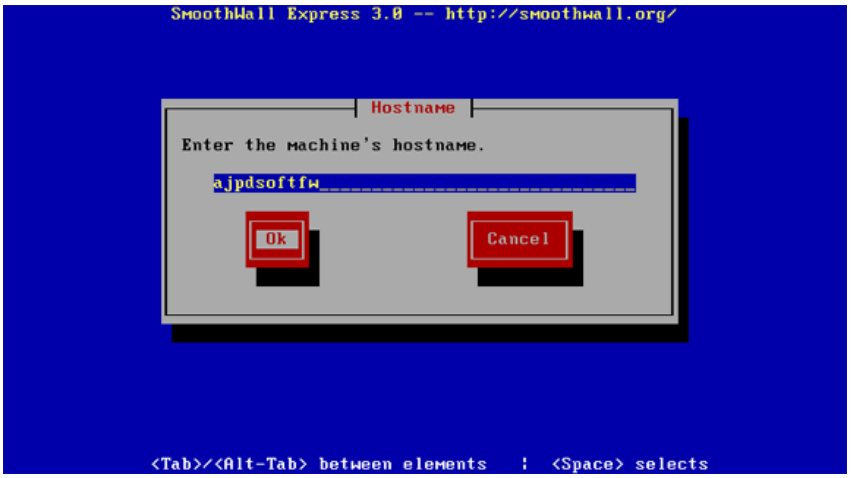
A continuación, si disponemos de un disquete de configuración de SmoothWall de una instalación anterior, podremos usarlo ahora para restaurar dicha configuración, para ello introduciremos el disquete y pulsaremos en "Yes", si es la primera vez que instalamos SmoothWall pulsaremos "No". El texto original de la ventana: "Do you want to restore the configuration for this SmoothWall Express from a previous installation using a backup floppy disk? If you select 'Yes', the areas which were restored from the backup will be automatically configured and will not ve displayed to you. This can also be used to restore settings from a previous version of SmoothWal Express".



Seleccionaremos el idioma del teclado (en nuestro caso "es"):



Introduciremos un nombre para el equipo corgafuegos en la red (hostname), por ejemplo "conbras":



A continuación seleccionaremos el tipo de política o directiva de seguridad para las solicitudes o peticiones salientes. Esta configuración no afecta a las solicitudes entrantes, que siempre estarán bloqueadas a menos que explícitamente sean permitidas (mediante las reglas del cortafuegos o firewall). Las posibilidades son:

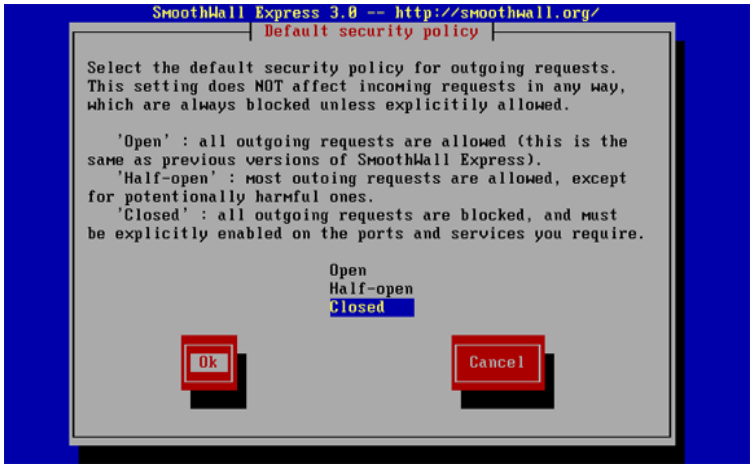
- **Open** (abierto): todas las peticiones salientes serán permitidas (como en las versiones anteriores de SmoothWall Express).
- **Half-open** (entreabierta): la gran parte de las peticiones saliente serán permitidas, salvo las consideradas dañinas o peligrosas.
- **Closed** (cerrado): todas las peticiones salientes serán bloqueadas. Si se quiere permitir alguna petición saliente se deberá especificar en la administración del firewall SmoothWall Express (en las reglas).

El texto original de esta ventana:

"Select the default security policy for outgoing requests. This settings does not affect incoming requests in any way, which are always blocked unless explicity allowed.

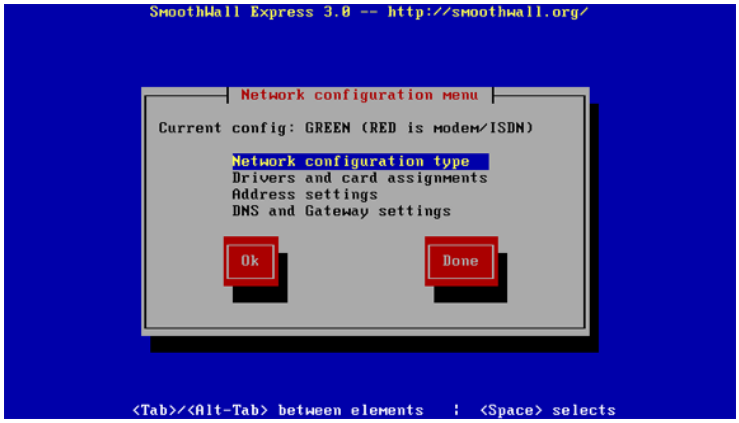
- open: all outgoing requests are allowed (this is the same as previous versions of SmoothWall Express).
- half-open: most outoing request are allowed, except for potentionally harmful ones.
- closed: all outgoing requests are blocked, and must be explicity enabled on the port and services you require.

En nuestro caso seleccionaremos "Closed", todas las peticiones quedarán bloquedas y sólo permitiremos aquellas que indiquemos en la administración del firewall o cortafuegos SmoothWall Express:



A continuación indicaremos las opciones de configuración siguientes:

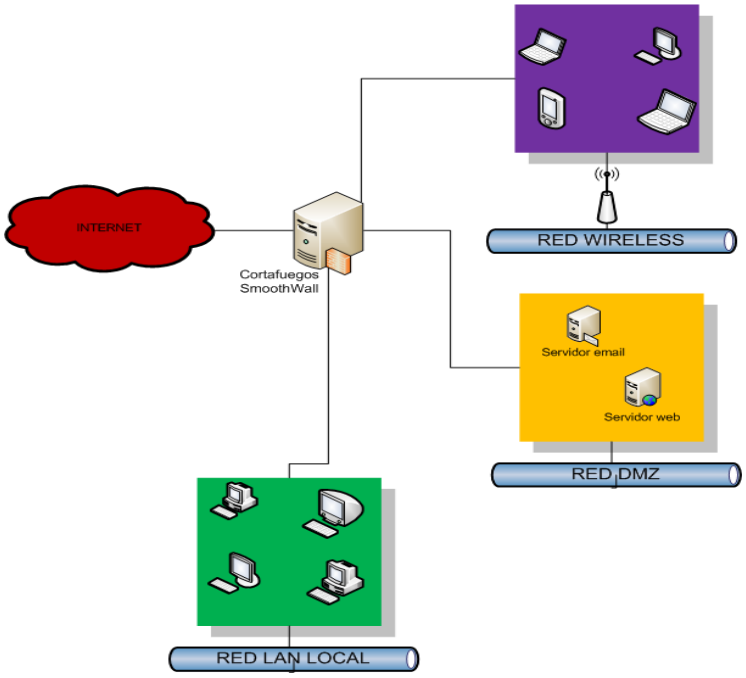
- **Network configuration type**: seleccionaremos esta opción y pulsaremos "Ok", desde aquí indicaremos un dato muy importante, el tipo de configuración de red que utilizaremos:



Indicaremos la configuración de red de nuestra organización, las posibilidades:

- GREEN (RED is modem/ISDN).
- GREEN + ORANGE (RED is modem/ISDN).
- GREEN + RED.
- GREEN + ORANGE + RED.
- GREEN + PURPLE (RED is modem/ISDN).
- GREEN + PURPLE + ORANGE (RED is modem/ISDN).

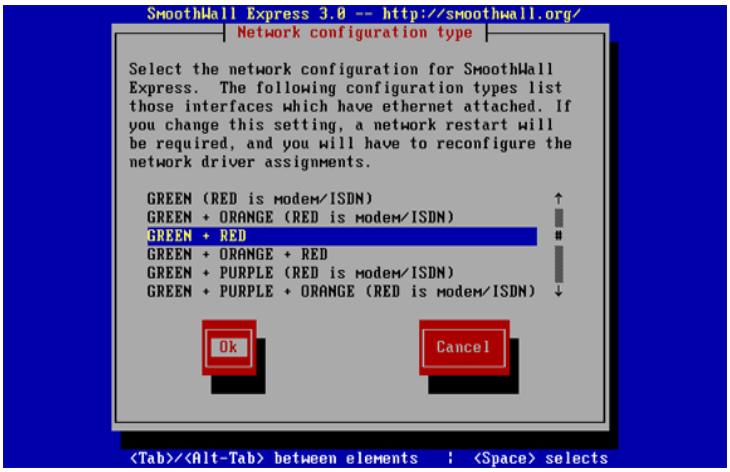
Teniendo en cuenta el siguiente diagrama:



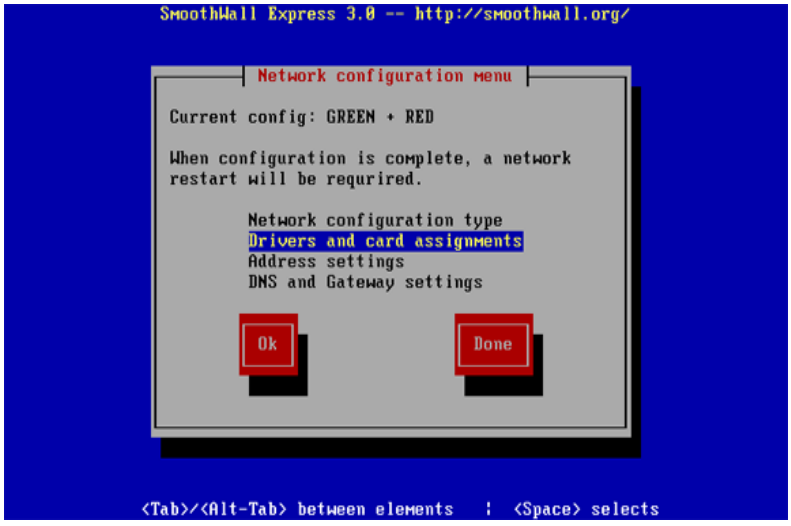
Teniendo en cuenta que:

- Red wireless (purple): red inalámbria si tenemos router wireless con este tipo de conexión activada.
- Red DMZ (orange): zona desmilitarizada, normalmente en este segmento de red se suelen colocar los servidores propensos a antaques externos, como el servidor web o el de correo electrónico.
- Red LAN local (green): red de área local, red privada, donde están todos los equipos y los servidores de terminal server, servidores de bases de datos, servidores de ficheros, etc.

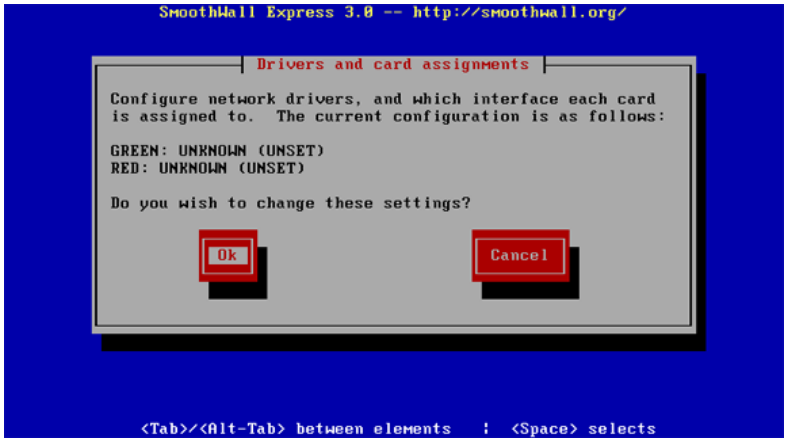
En nuestro caso, puesto que no tenemos DMZ ni wireless, seleccionaremos GREEN + RED. Esta nomemclatura indica que de las dos tarjetas de red, la RED será la que esté conectada al modem (dispositivo que nos proporciona la conexión a Internet) y la GREEN será la tarjeta de red conectada al swith donde están conectados el resto de equipos de la LAN:



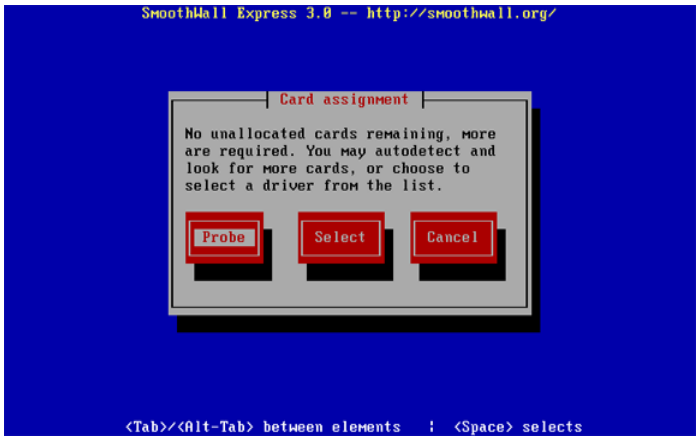
A continuación deberemos indicar los drivers y la asignación de las dos tarjetas a RED y a GREEN, para ello seleccionaremos "Drivers and card assignments" y pulsaremos "Ok":



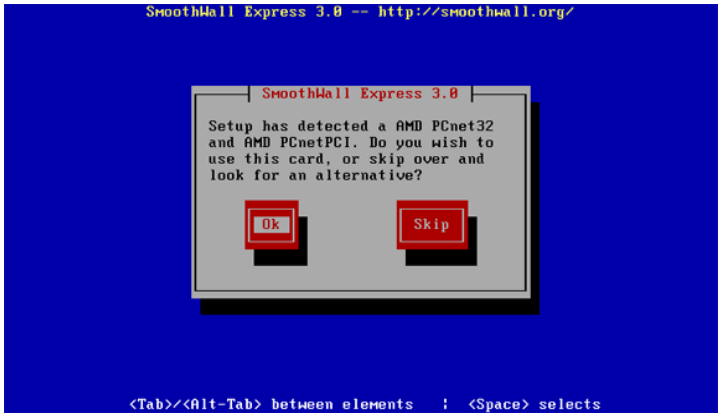
A continuación pulsaremos "Ok" para que el sistema detecte las tarjetas de red instaladas en nuestro equipo:



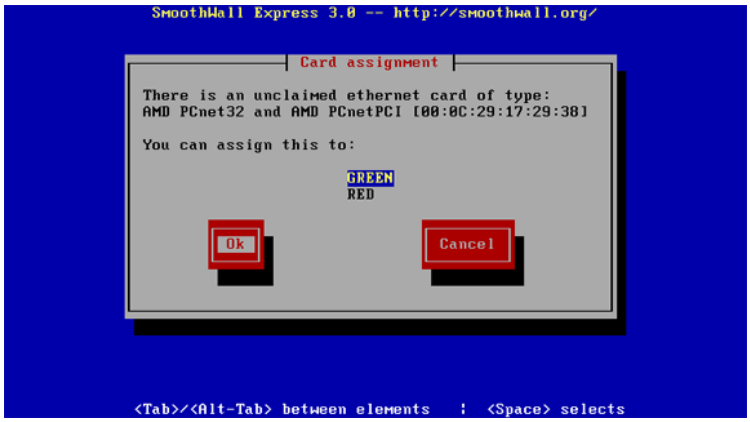
A continuación pulsaremos "Probe" para que el sistema autodetecte las tarjetas de red de nuestro equipo, si no las detecta pulsaremos "Select" para seleccionarlas de una lista o para añadir los drivers manualmente:



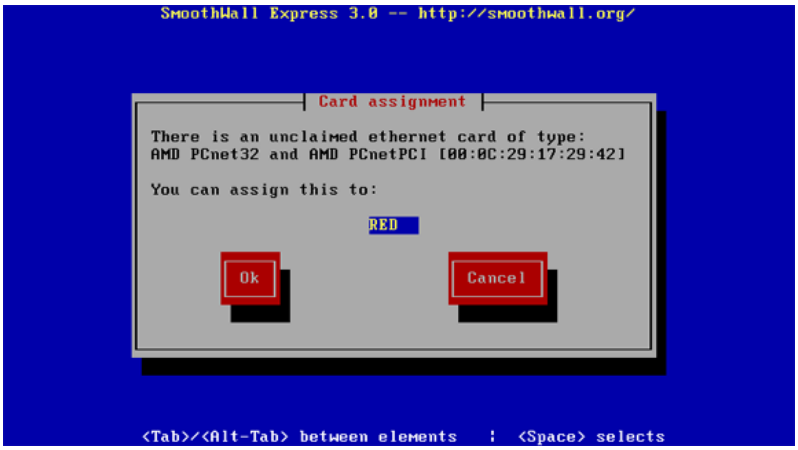
Si el sistema detecta las tarjetas de red mostrará un mensaje como el siguiente, si es correcta la detección pulsaremos "Ok", en caso contrario pulsaremos "Skip":



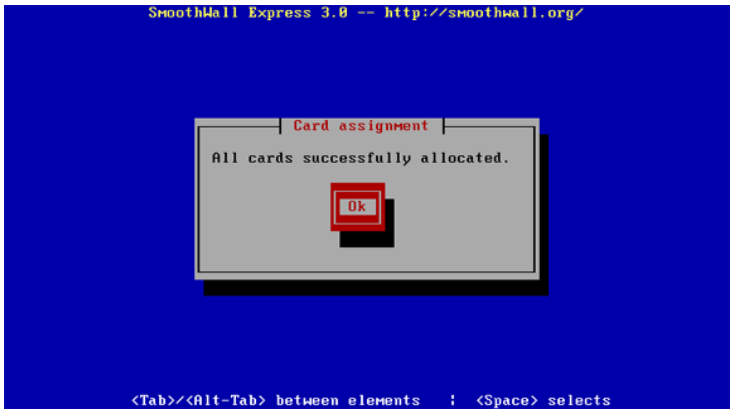
A continuación, SmoothWall pedirá que se asigne el color GREEN o RED a la tarjeta de red indicada por la MAC:



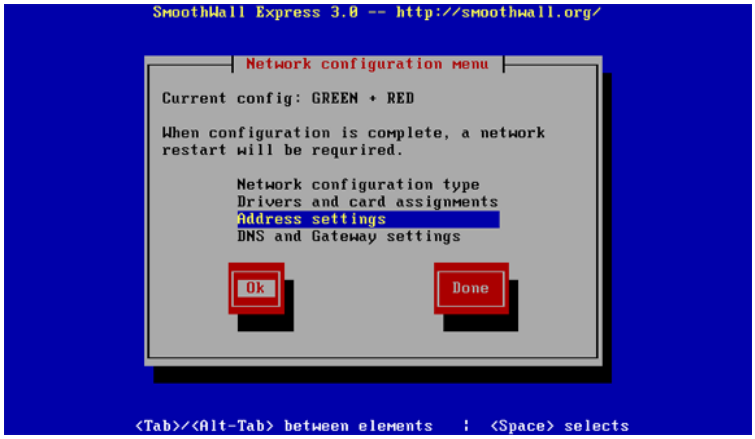
Si a la anterior le hemos asignado la GREEN (tarjeta de red que irá conectada del equipo al swith donde están el resto de los equipos de la LAN), la queda será la RED (tarjeta de red que irá conectada al router o dispositivo que nos proporciona la conexión a Internet):



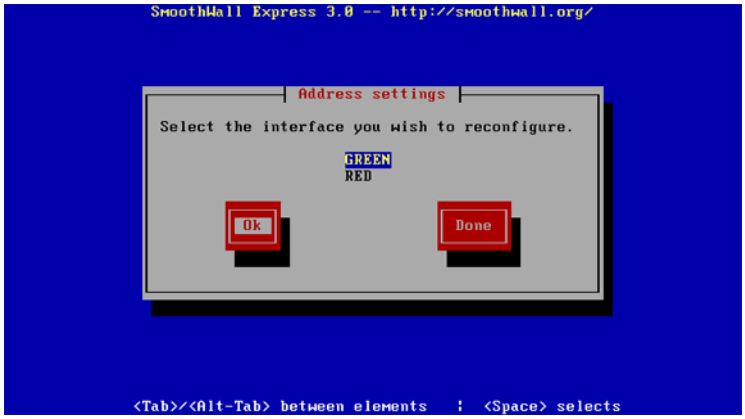
Nos indicará que las tarjetas han sido correctamente identificadas, pulsaremos "Ok":



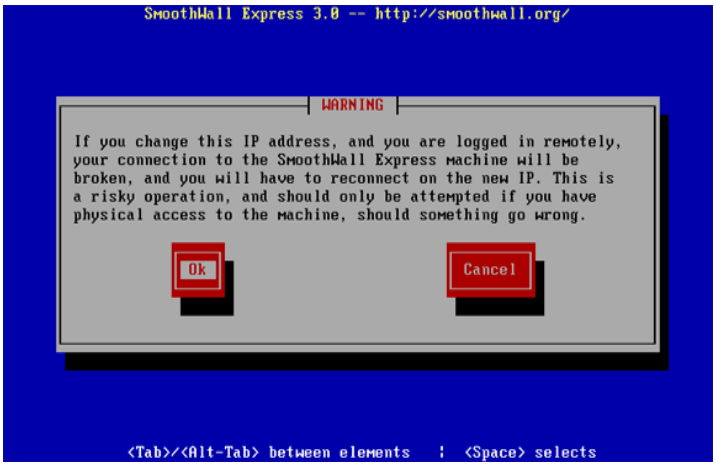
A continuación podremos configuar las direcciones IP de cada tarjeta de red del equipo, para ello seleccionaremos "Address settings":



Seleccionaremos la interfaz a la que le configuraremos la IP y la máscara de subred:

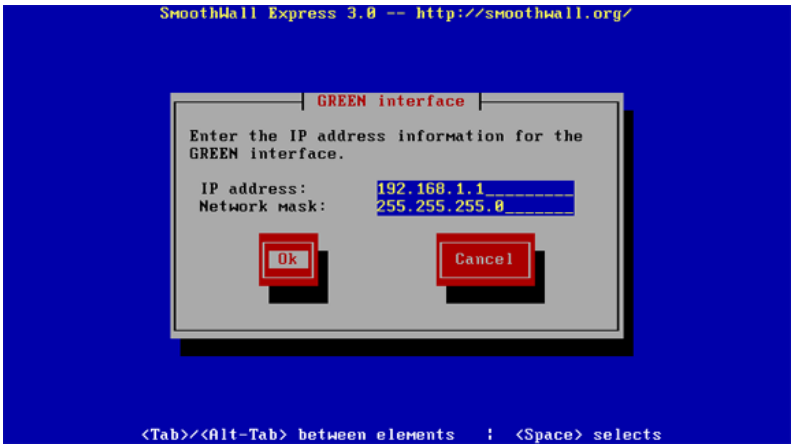


Nos avisará de que si cambiamos la IP, las conexiones remotas se desconectarán y tendremos que volver a conectarnos de nuevo con la nueva IP. En nuestro caso, puesto que es una instalación desde cero de SmoothWall, no habrá conexiones remotas, pulsaremos "Ok":

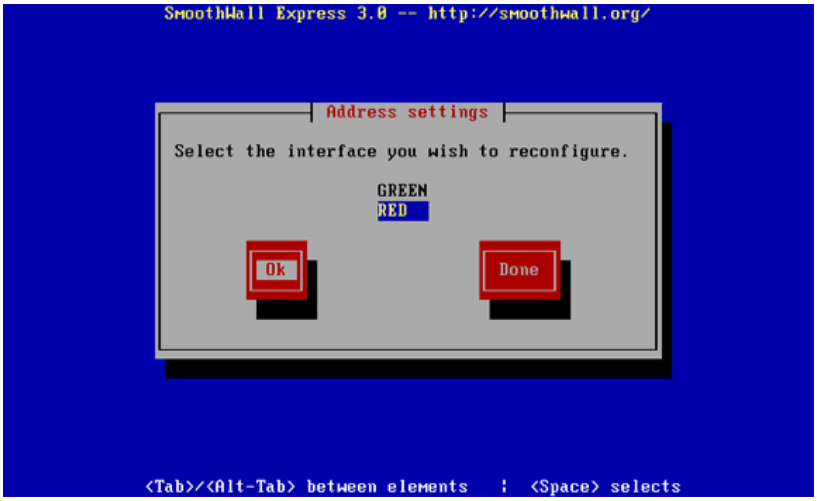


Si hemos seleccionado la interfaz GREEN, se corresponderá con la red LAN (red local), por lo que esta tarjeta de red tendrá que tener una IP y una máscara de red correspondiente a la del resto de equipos de la LAN. Además, hay que tener en cuenta la IP que le asignemos a esta interfaz de red GREEN será la puerta de enlace o gateway de todos los equipos.

En nuestro caso, puesto que los equipos de la red tienen IPs del rango 192.168.1.xxx, asignaremos a la interfaz GREEN la IP: 192.168.1.1 y la máscara: 255.255.255.0:



A continuación configuraremos la IP para la interfaz RED (la tarjeta de red conectada al router):



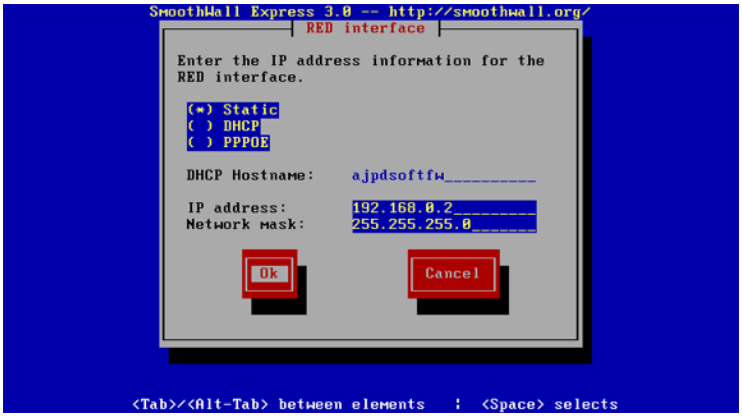
Es importante que se entienda lo siguiente: la subred de los equipos de la LAN y de la tarjeta de red GREEN debe ser **diferente** a la de la tarjeta de red RED y la del router. Por ejemplo, si la subred de la LAN es la 192.168.1.xxx, la subred de la tarjeta RED y del modem puede ser 192.168.0.xxx.

Explicamos esto más detenidamente: el modem (o dispositivo de conexión a Internet) debe tener una IP perteneciente a un rango diferente al de la red LAN (local o privada). En nuestro caso, el router tiene la IP: 192.168.0.1. En el caso de que el router tenga la IP correspondiente a la subred de la LAN (que es lo normal antes de tener el cortafuegos o firewall), habrá que cambiarle la IP por una de una subred diferente.

Puesto que la interfaz de red RED está conectada al router, esta tarjeta de red debe tener una IP del mismo rango. Por ejemplo, si el router tiene la 192.168.0.1, esta tarjeta de red podría tener la 192.168.0.2.

Además, SmoothWall Express permite que si el router tiene activado el servicio DHCP, la tarjeta de red RED puede obtener una IP y una máscara de forma automática que le será proporcionada por el router, para ello habrá que marcar "DHCP" en la siguiente ventana.

Si queremos establecer una IP fija manual para la interfaz RED marcaremos "Static" e introduciremos la IP para la interfaz RED:

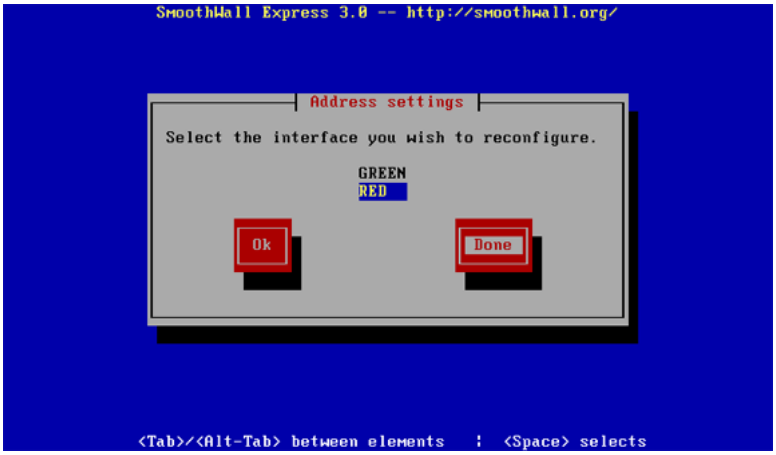


En resumen: el rango de red del router y de la interfaz RED debe ser diferente al de la LAN y la interfaz GREEN.

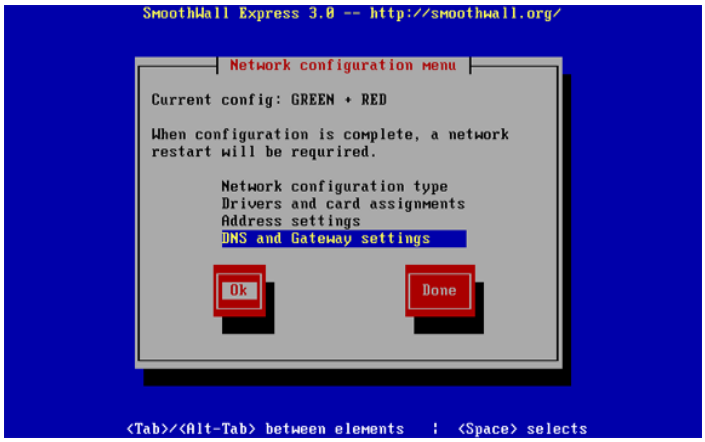
En nuestro caso:

- IP del router: 192.168.0.1.
- IP de la interfaz RED: 192.168.0.2.
- IP de la interfaz GREEN: 192.168.1.1.

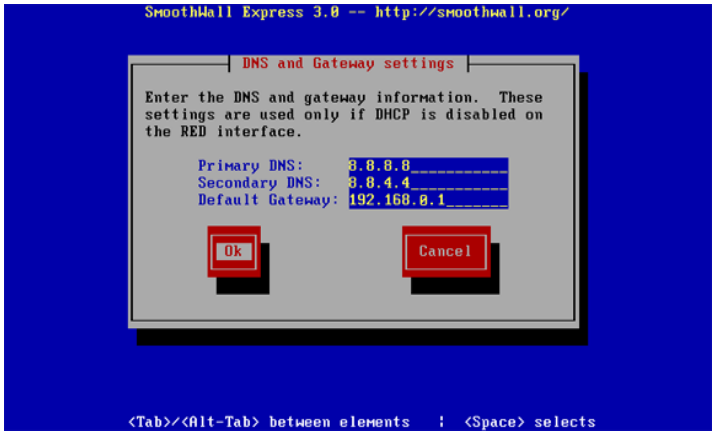
Una vez configuradas las IPs de la interfaz GREEN y RED pulsaremos "Done":



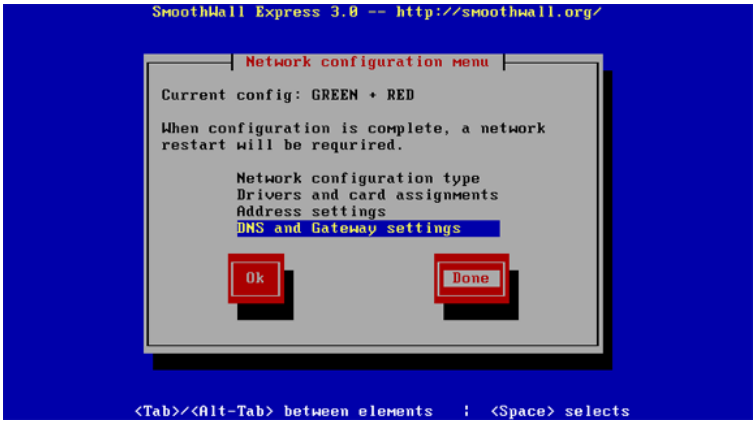
A continuación configuraremos las DNS y el Gateway, para ello seleccionaremos "DNS and Gateway settings":



Introducremos el servidor DNS primario (Primary DNS), el servidor DNS secundario (Secondary DNS) y la puerta de enlace (Default Gateway). La puerta de enlace deberá ser la IP del router de nuestra red (dispositivo que nos proporciona conexión a iInternet y que estará conectado únicamente a la tarjeta RED de nuestro equipo cortafuegos), en nuestro caso 192.168.0.1:

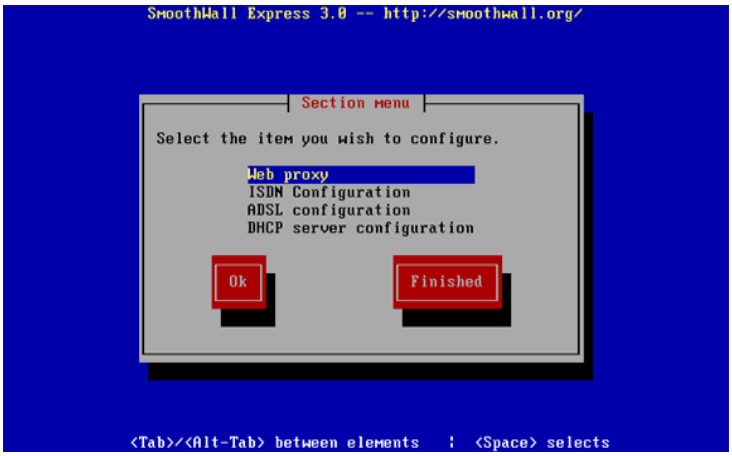


Una vez configurados estos parámetros pulsaremos en "Done":

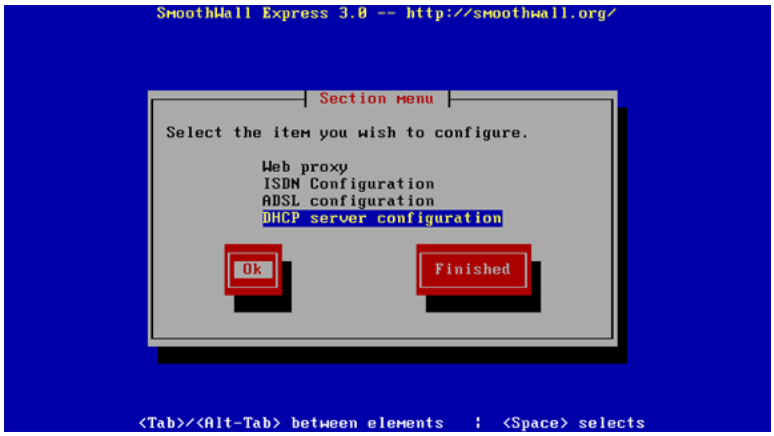


A continuación podremos configurar otros parámetros como:

- Web proxy: si tenemos un proxy en nuestra red y queremos que el tráfico pase a través de él.
- ISDN Configuration: si queremos establecer alguna configuración específica en el caso de que dispongamos de conexión RDSI (Red Digital de Servicios Integrados) para la conexión a Internet.
- ADSL configuration: si queremos establecer alguna configuración específica en el caso de que dispongamos de ADSL para la conexión a Internet.
- DHCP server configuration: si queremos activar y configurar el servicio de DHCP para los equipos de nuestra LAN desde el equipo con SmoothWall Express, que hará de servidor de DHCP.



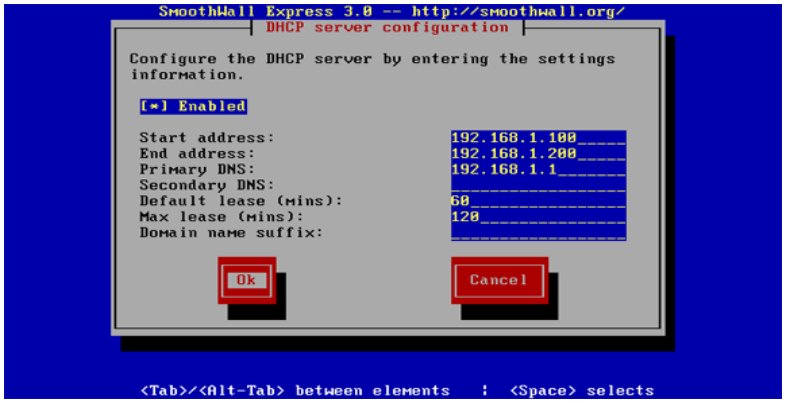
Por ejemplo, seleccionando "DHCP server configuration" y pulsando "Ok":



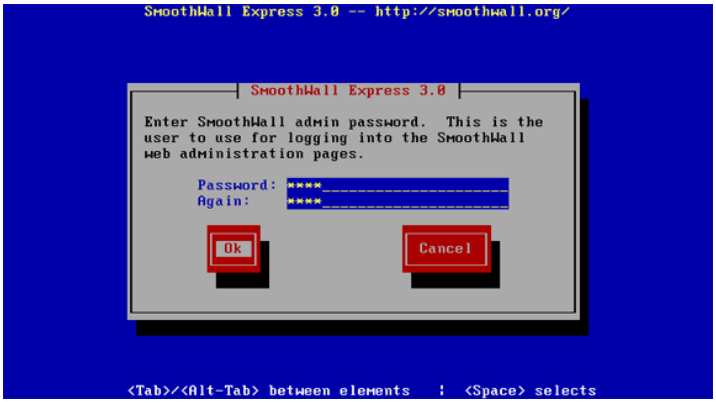
Para activar el servidor de DHCP, para que el equipo con Smooth Wall, además de cortafuegos, sea servidor de DHCP, marcaremos "Enabled" y estableceremos los siguientes parámetros:

- Start address: dirección IP del rango de la interfaz GREEN a partir de la cual se empezará a asignar IPs.

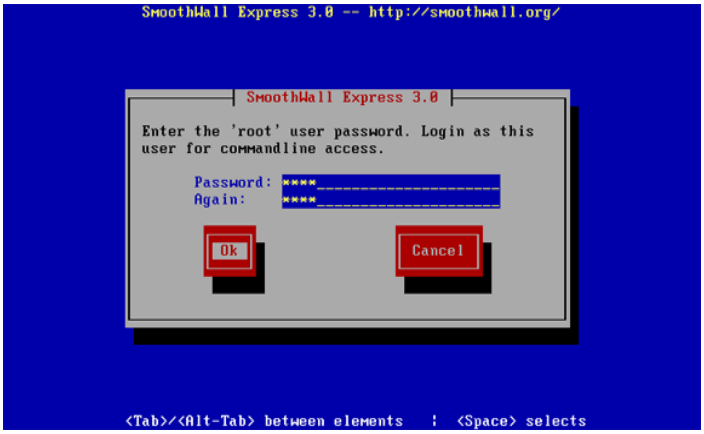
- End address: dirección IP final, a partir de esta no se asignarán mas IPs.
- Primary DNS: dirección IP del servidor de DNS primarios, si hemos establecido en las ventanas anteriores el servidor de DNS primario y segundario, introduciremos aquí como servidor DNS la propia IP de la interfaz GREEN: 192.168.1.1.



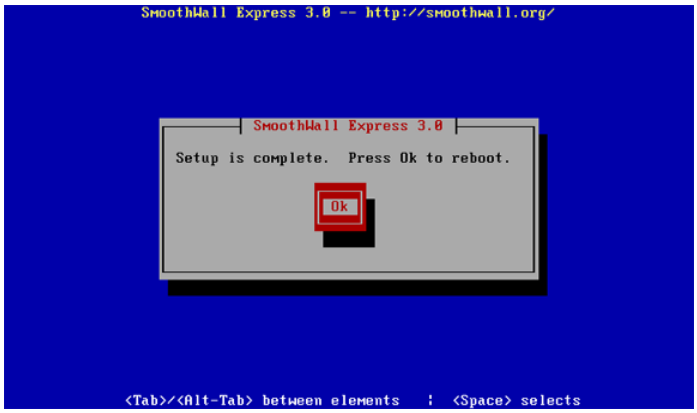
A continuación deberemos introducir la contraseña para el usuario "admin" de SmoothWall Express, será el usuario y la contraseña para el acceso a la consola de administración web de SmoothWall:



A continuación estableceremos también la contraseña para el superusuario "root" de GNU Linux (del sistema operativo):

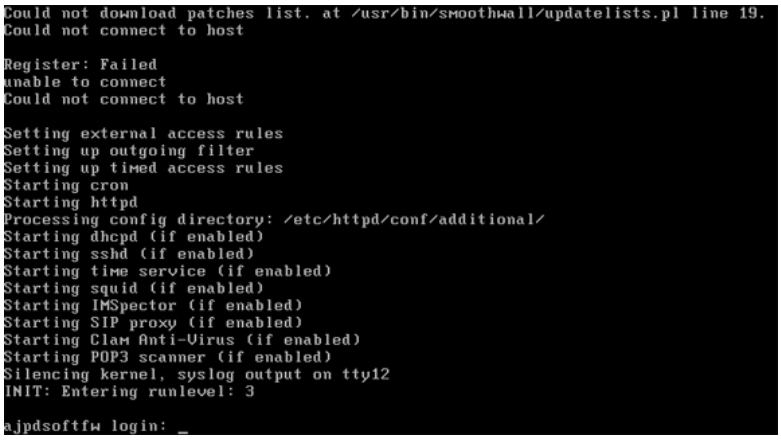


Con los parámetros anteriores habrá quedado instalado y configurado SmoothWall Express, pulsaremos "Ok" para reiniciarlo e iniciar por primera vez el cortafuegos o firewall SmoothWall Express:



Se iniciará SmoothWall Express:

No se iniciará en modo gráfico pues no lo incorpora, la configuración normal se realizará vía web y, si queremos configurar algún otro parámetro del sistema operativo, deberemos hacerlo en modo comando:

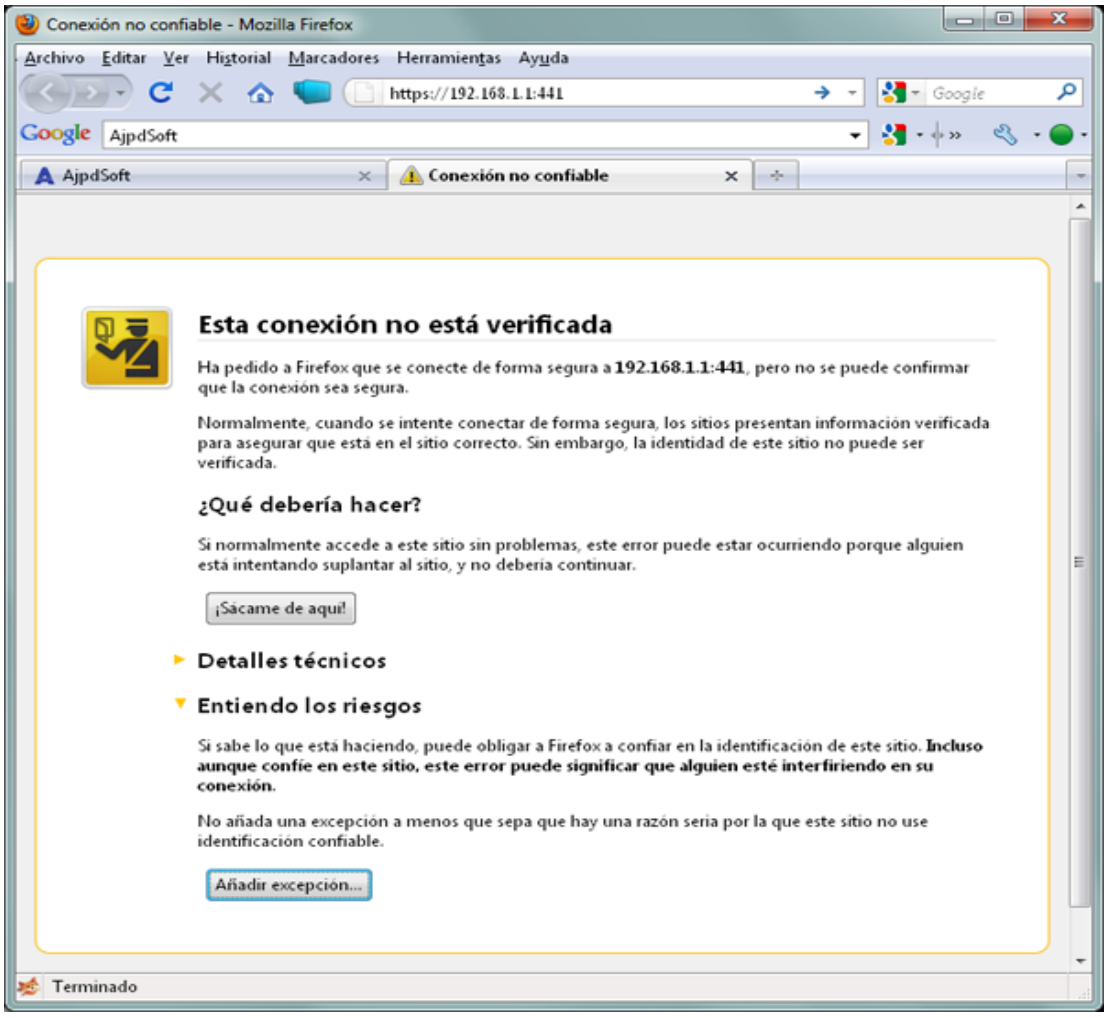


Cómo administrar el cortafuego o firewall SmoothWall Express

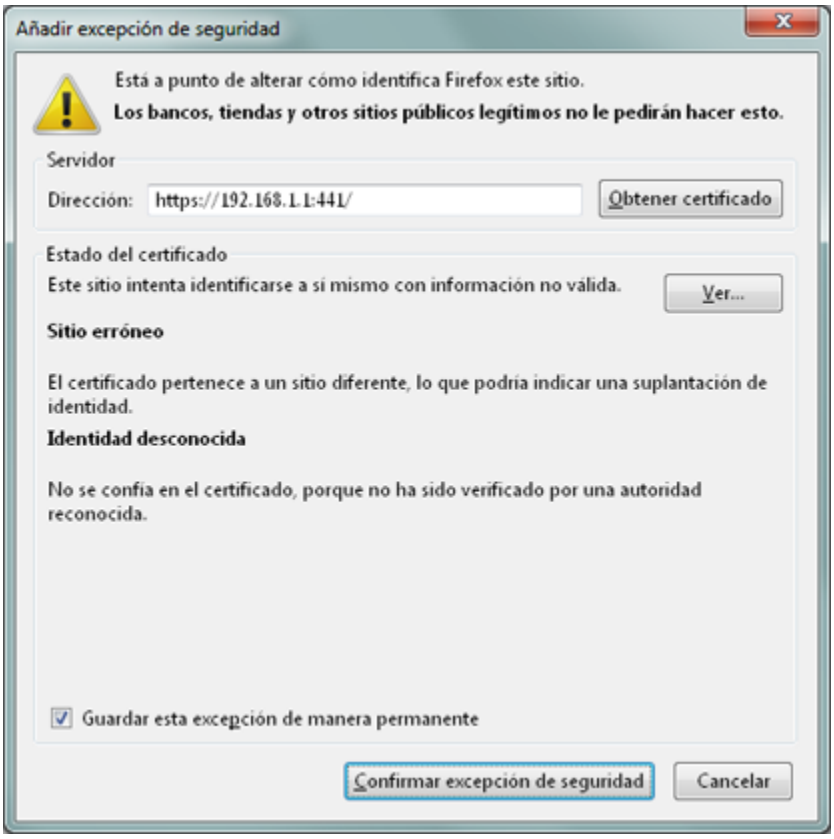
Para administrar y configurar el cortafuego SmoothWall Express, abriremos en cualquier navegador desde cualquier equipo de la red LAN, introduciremos la URL:

https://192.168.1.1:441

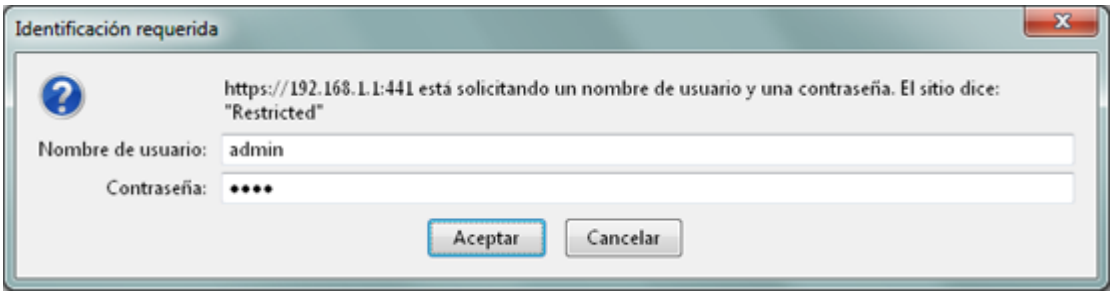
(Cambiando 192.168.1.1 por la IP que le hayamos asignado a la interfaz GREEN del equipo SmothWall).



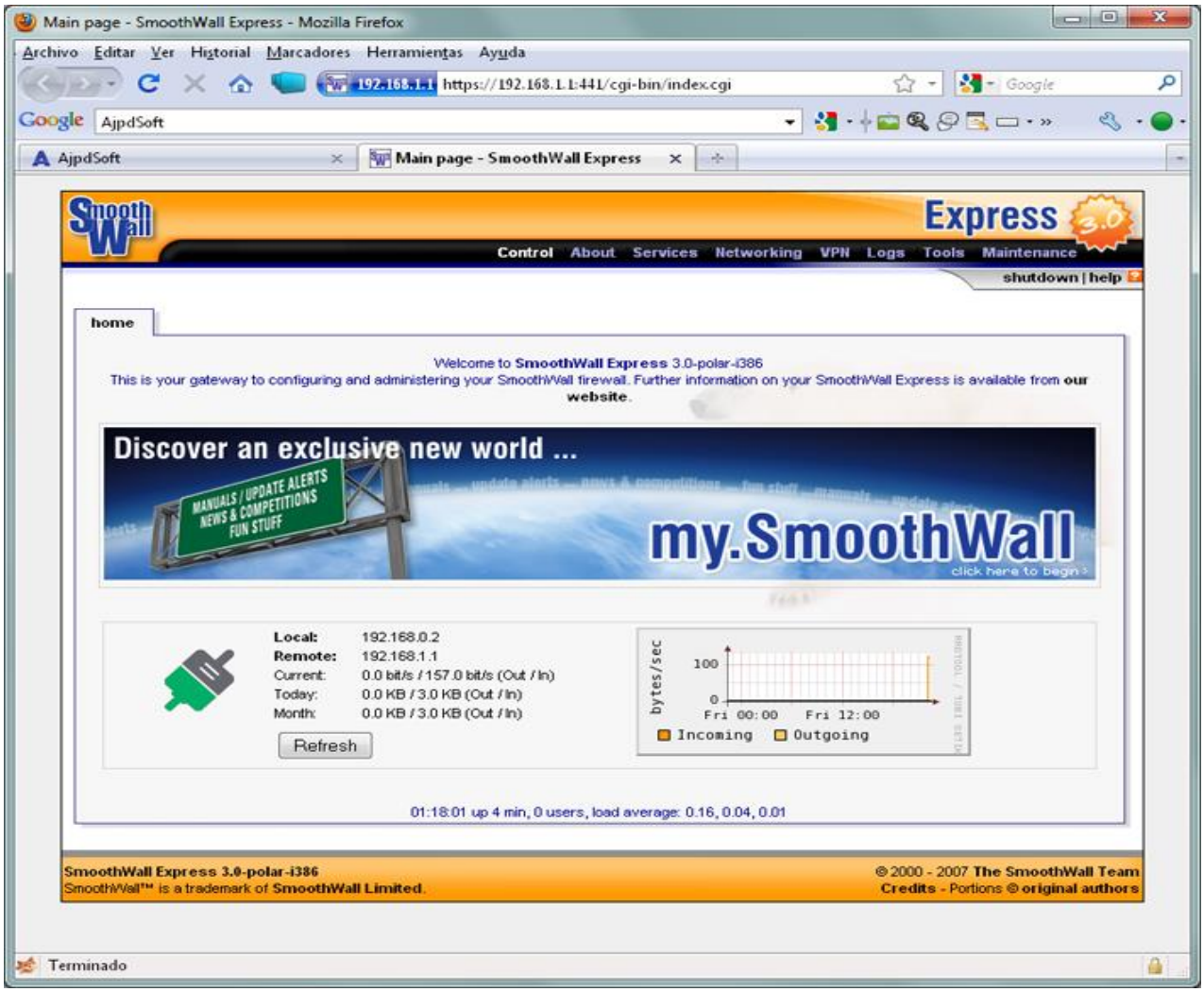
Pulsaremos "Obtener certificado" y "Confirmar excepción de seguridad":



Nos pedirá usuario y contraseña, introduciremos como usuario "admin", como contraseña la que hayamos asignado en pasos anteriores:



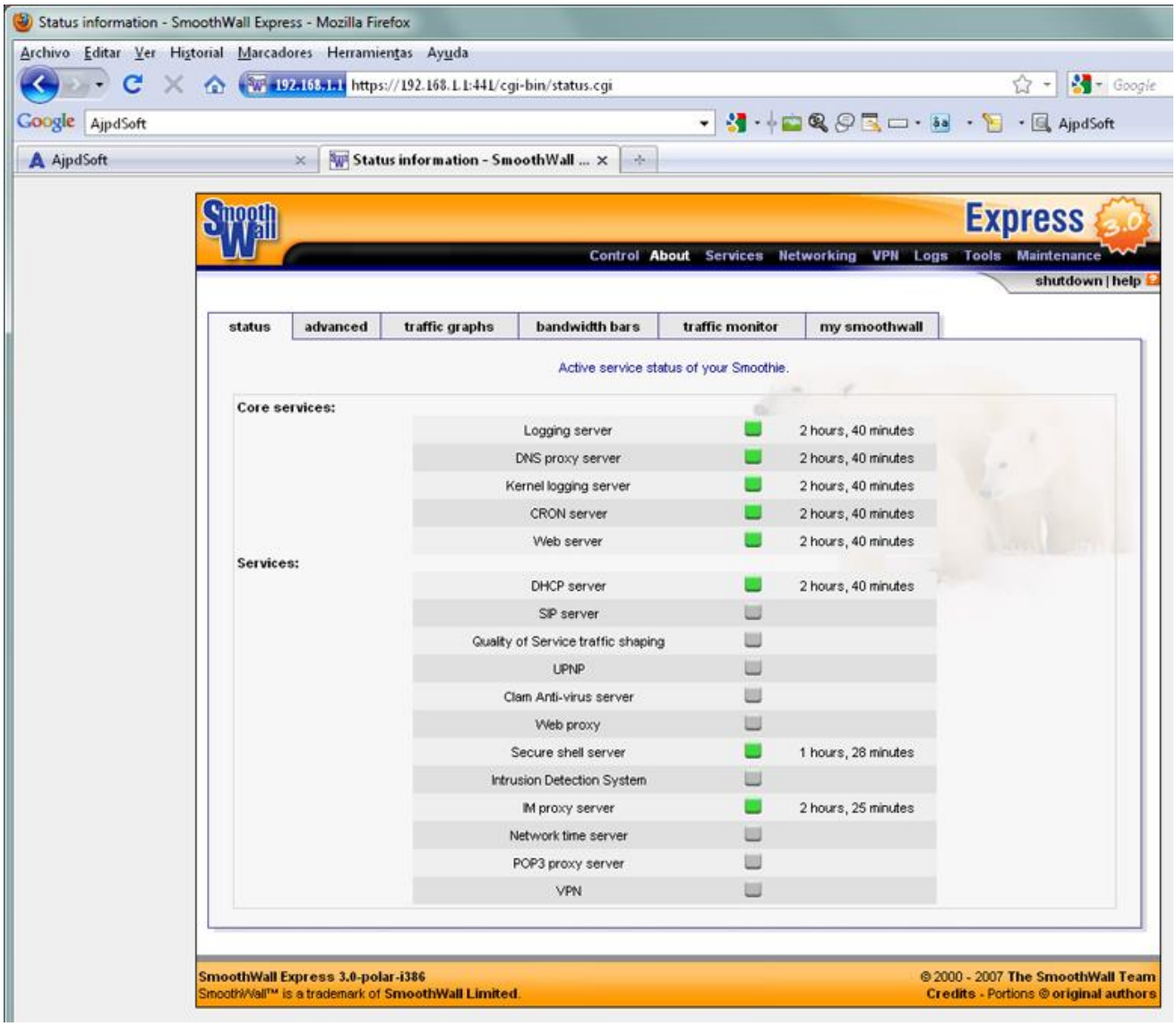
Y tendremos acceso a la consola de administración del firewall SmoothWall Express, desde donde podremos ver el estado actual, habilitar o deshabilitar servicios, añadir o eliminar reglas de seguridad, ver log y monitorizar, actualizar SmoothWall, etc.:



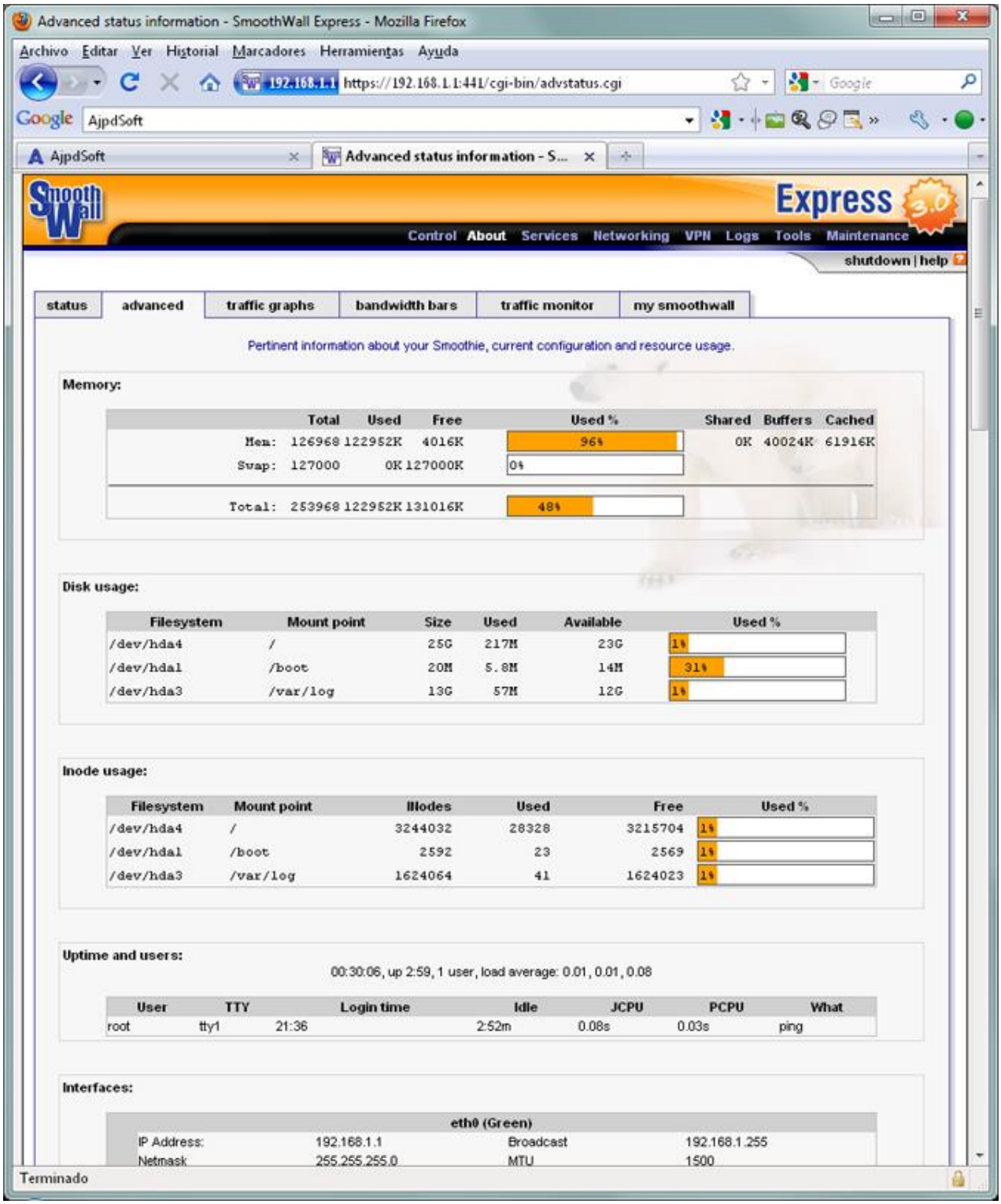
Menú About de la administración del firewall o cortafuegos SmoothWall

Desde el menú About de SmoothWall tendremos las siguientes opciones:

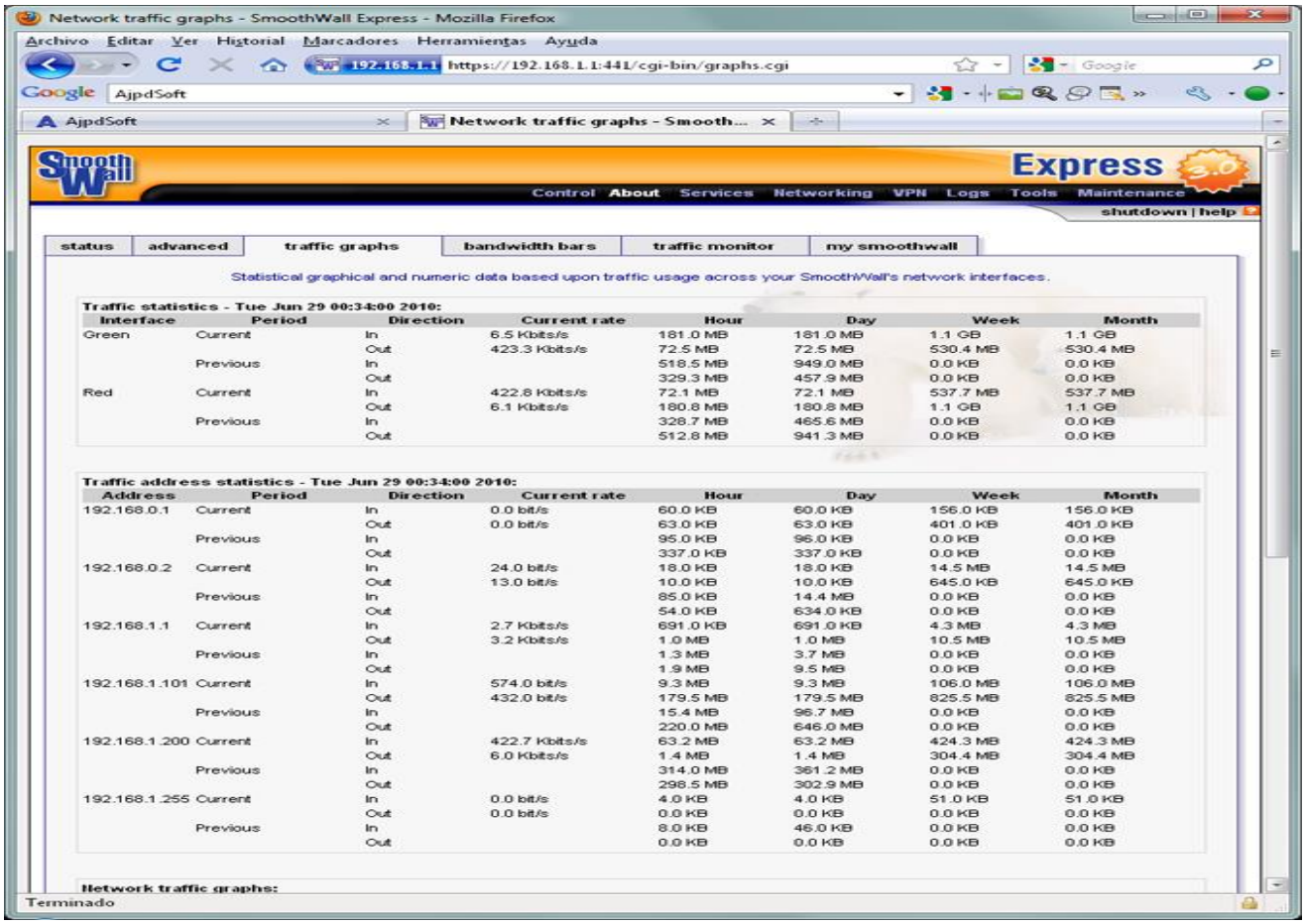
- **Status**: muestra el estado de los servicios de SmoothWall: Logging server, DNS proxy server, Kernel logging server, CRON server, Web server, DHCP server, SIP server, Quality of Service traffic shapping, UPNP, Clam Anti-Virus server, Web proxy, Secure shell server, Intrusion Detection System, IM proxy server, Network time server, POP3 proxy server, VPN:



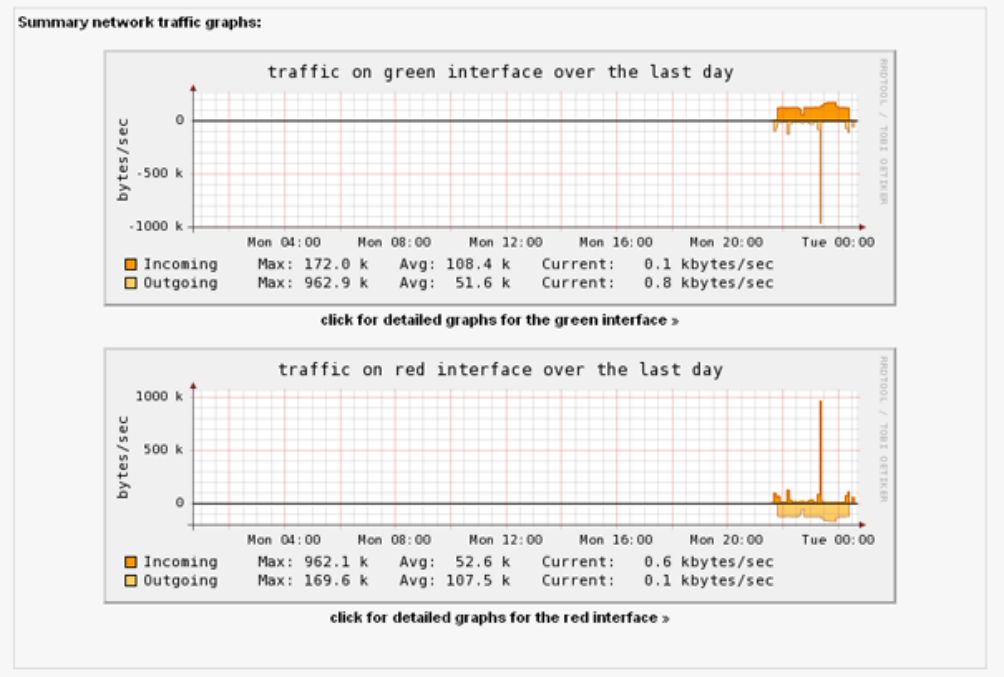
- **Advanced**: información general del sistema operativo y de las interfaces de red: memoria usada y libre, disco usado y libre, tabla de rutas, paquetes enviados y recibidos por cada interfaz de red, módulos cargados, versión del kernel, etc.:



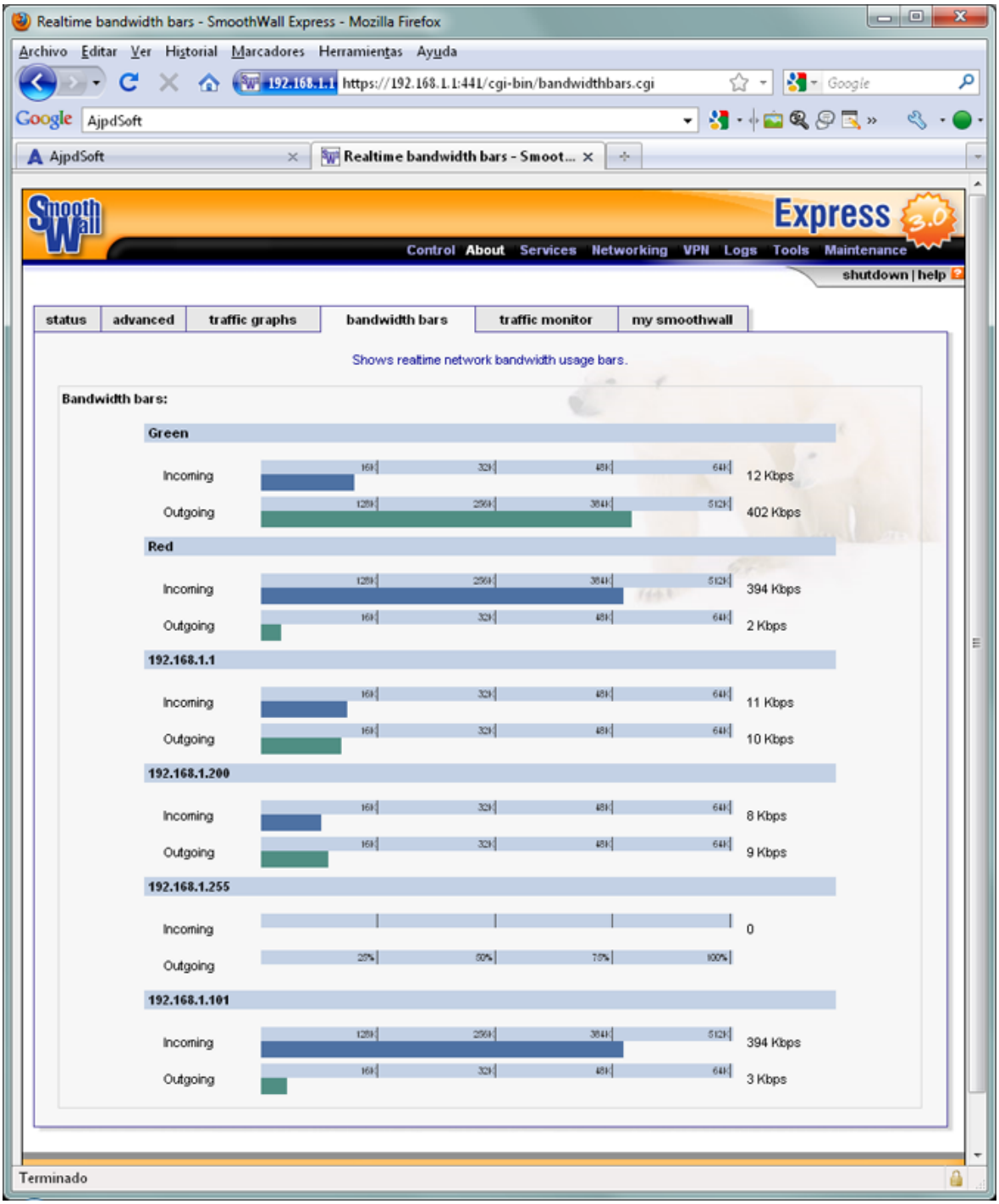
- **Traffic grahs**: información del tráfico por cada interfaz de red y por cada equipo de la red (tráfico en tiempo real, tráfico acumulado por hora, por día, por semana y por mes).



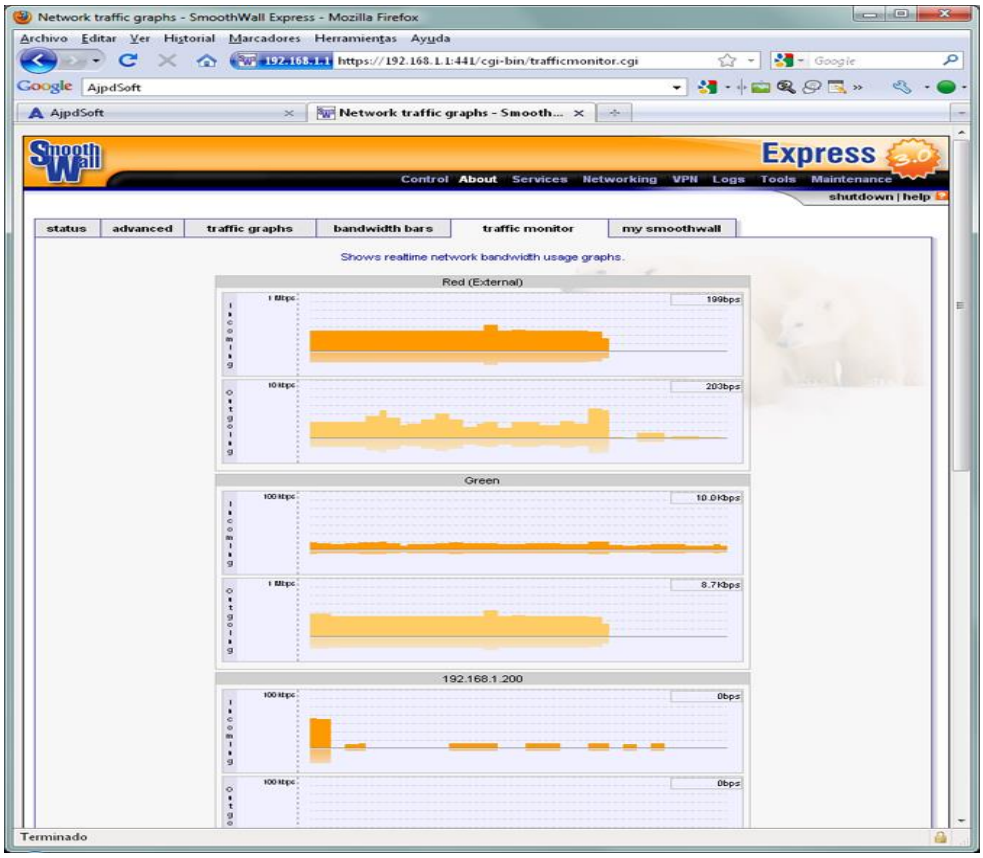
Además, gráfico con el tráfico de cada interfaz del último día:

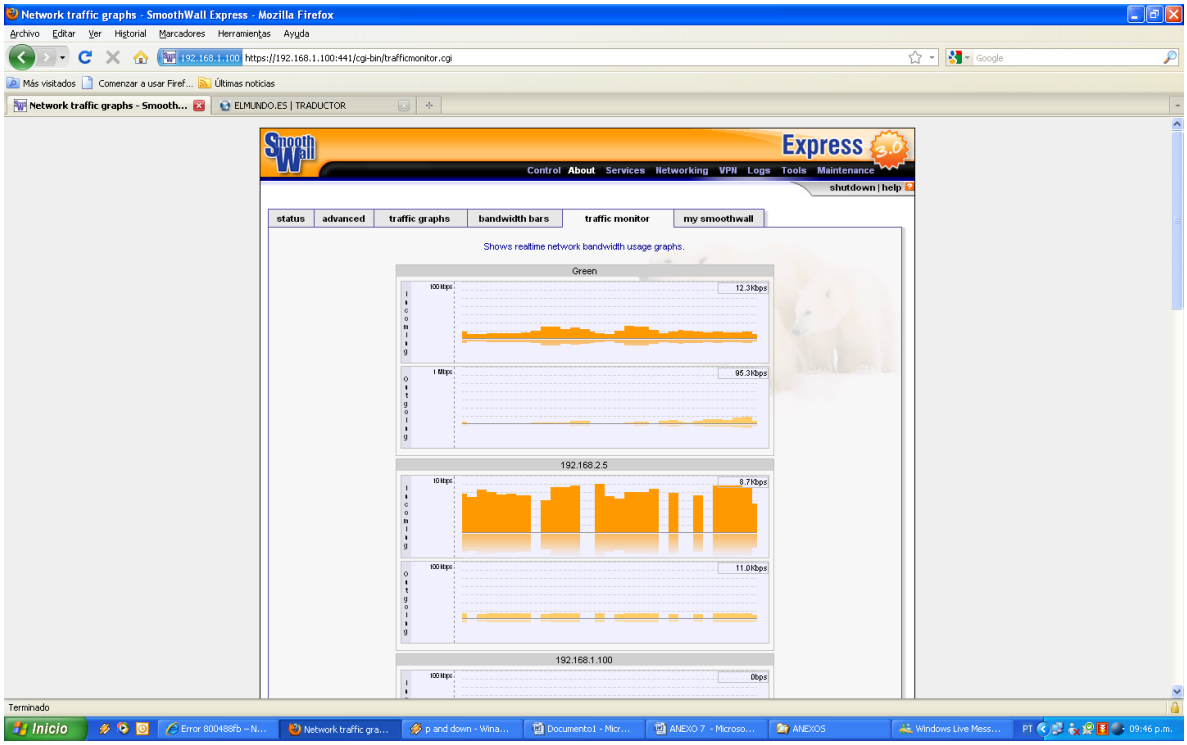


- **Bandwidth bars**: tráfico entrante y saliente en tiempo real por cada IP (equipo) de la red. Interesante utilidad para ver posibles equipos realizando subidas o bajadas que consuman tráfico en exceso:

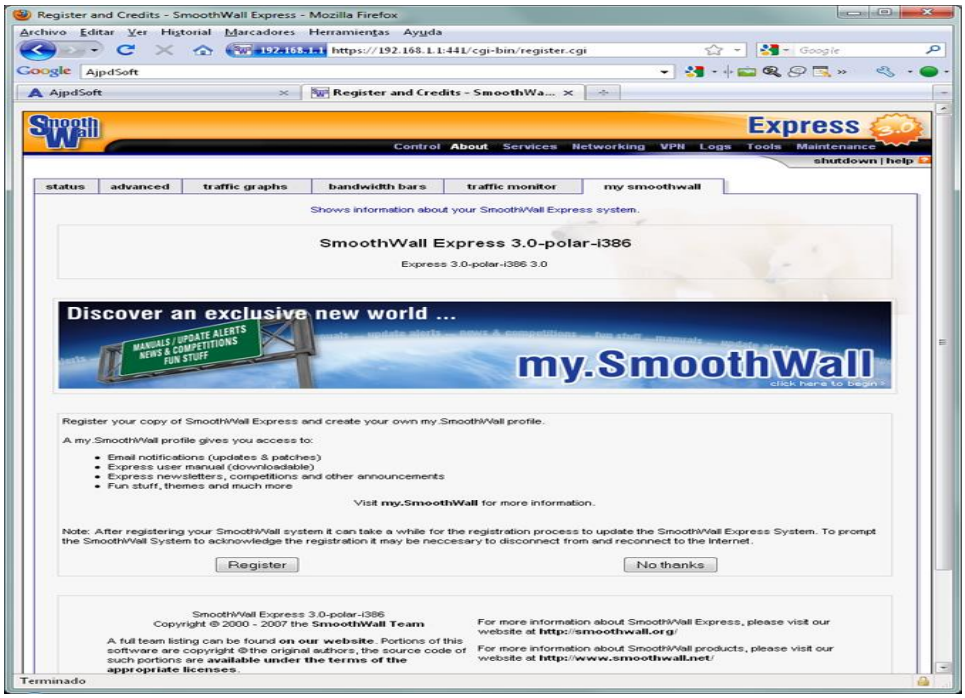


- **Traffic monitor**: muestra un gráfico con el tráfico saliente y entrante por cada equipo de la red y por cada interfaz del cortafuegos





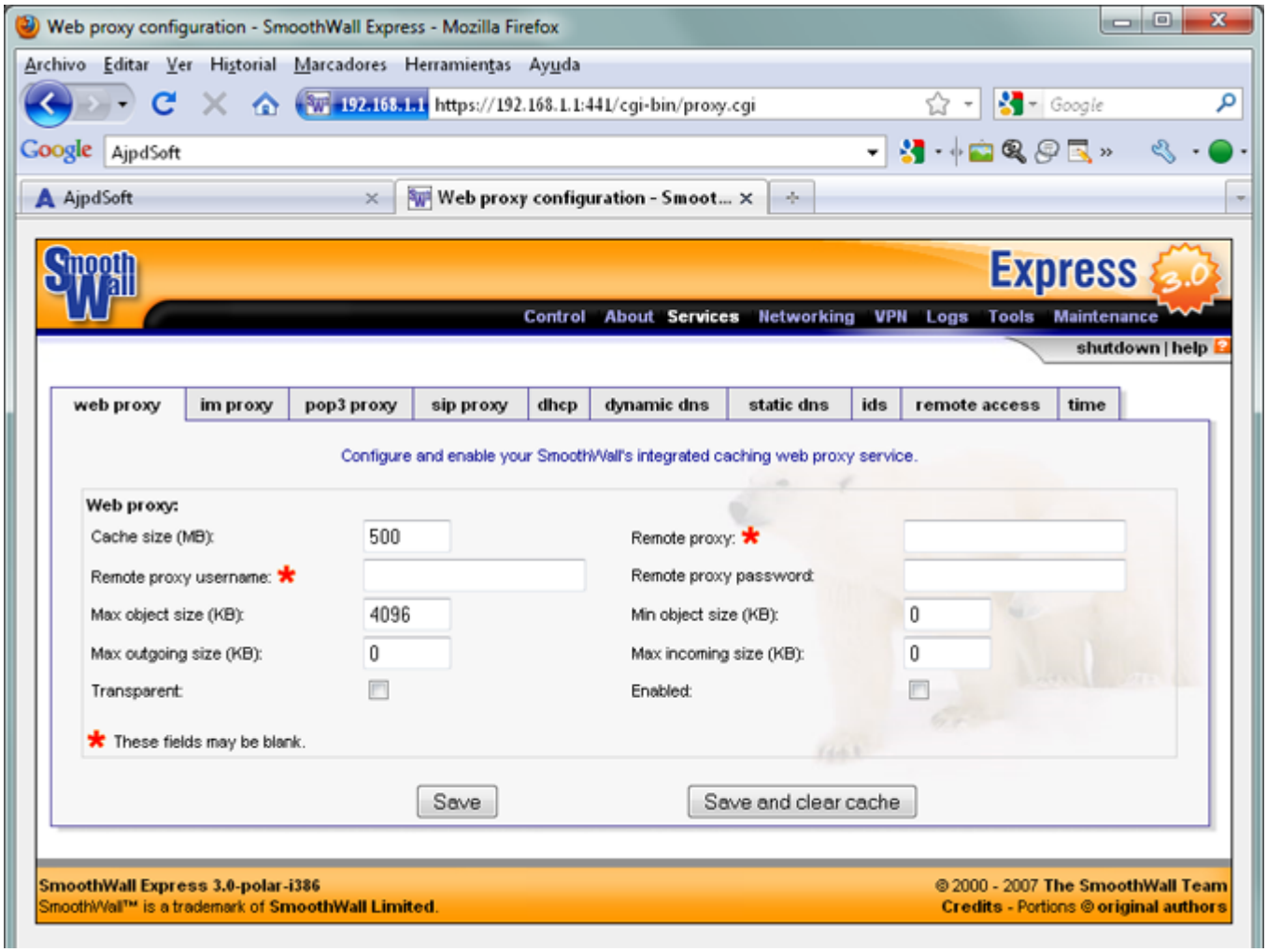
- **My SmoothWall**: versión actual de SmoothWall instalado en el equipo y registro:



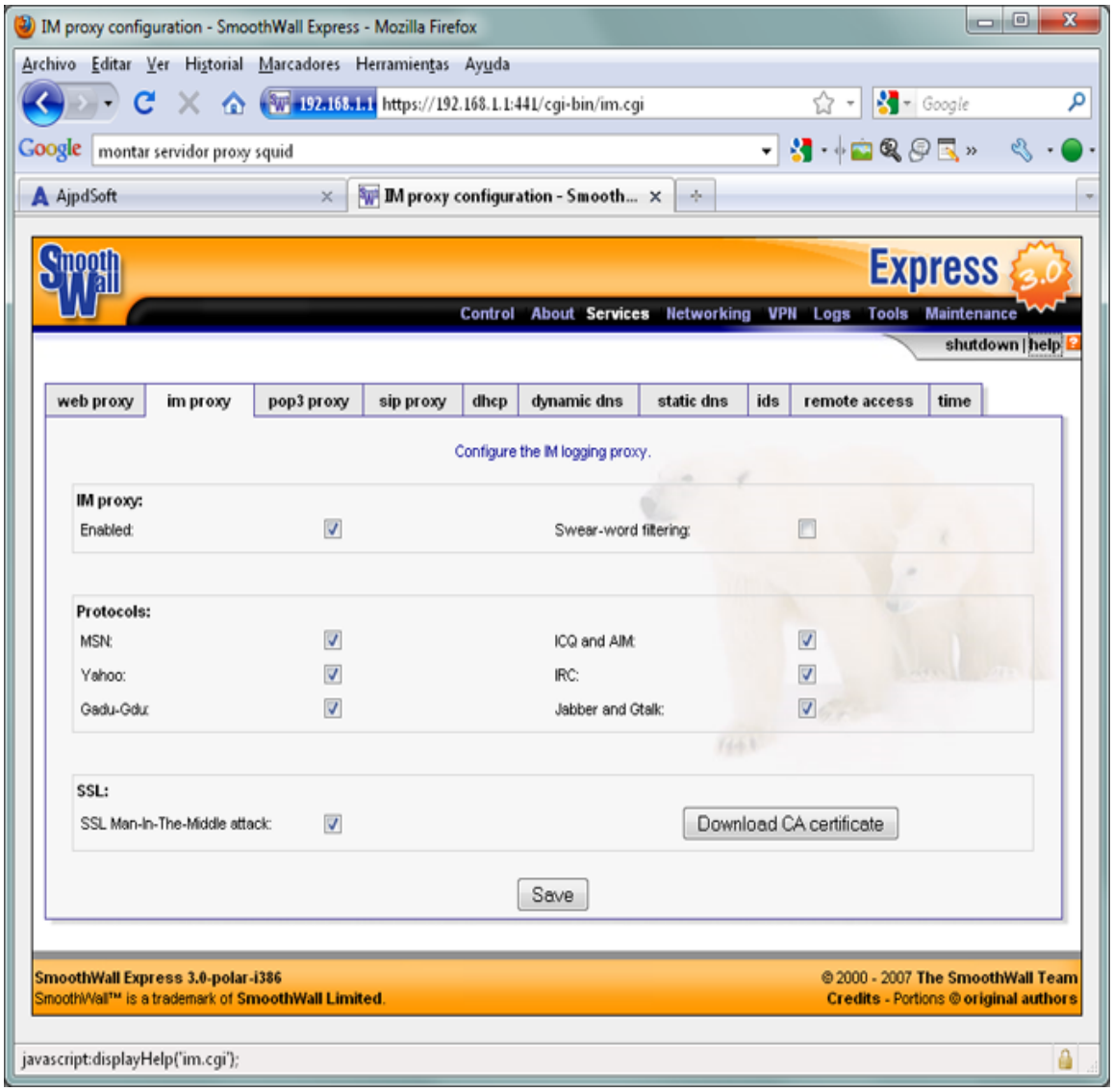
Menú Services de la administración del firewall o cortafuegos SmoothWall

Desde el menú Services de SmoothWall tendremos las siguientes opciones:

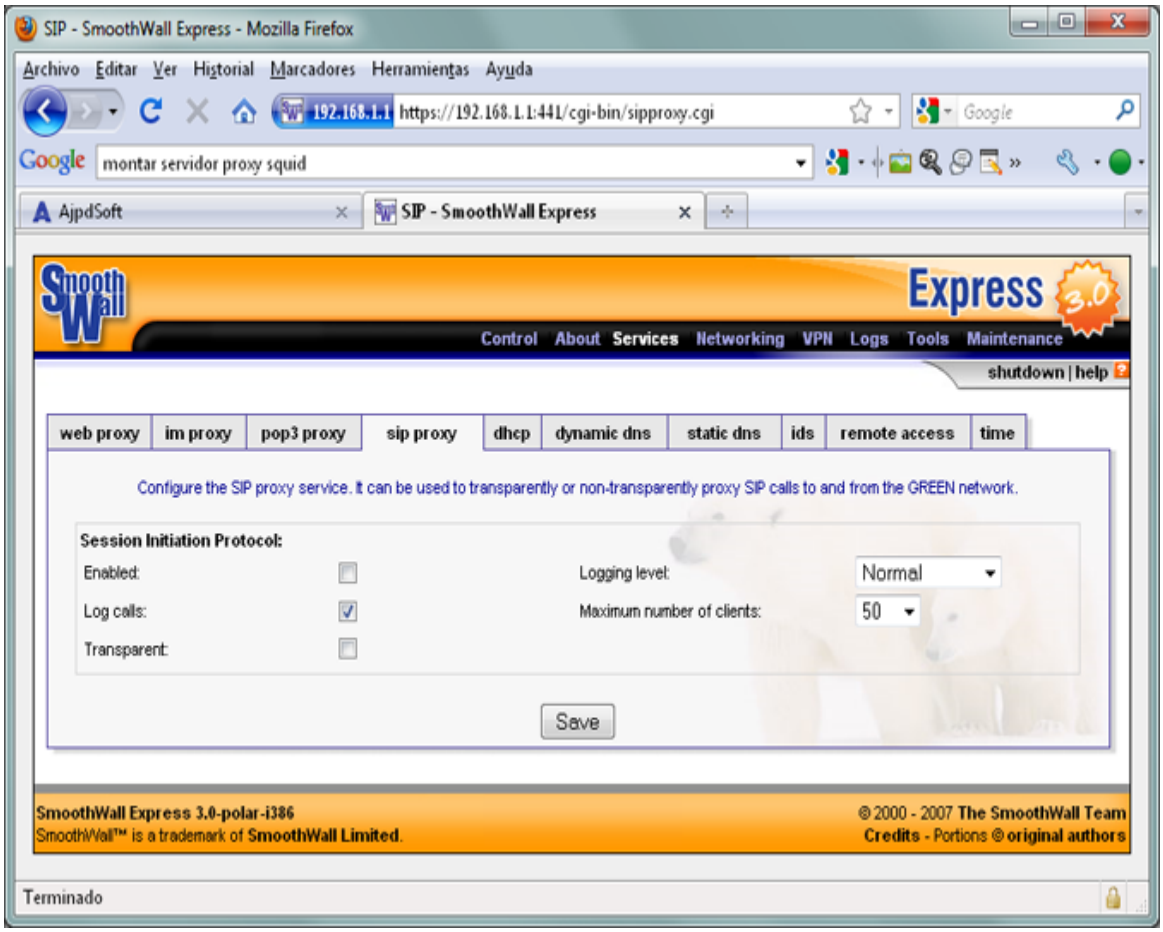
- **Web proxy**: posibilidad de activar el servidor proxy Squid que incluye SmoothWall:



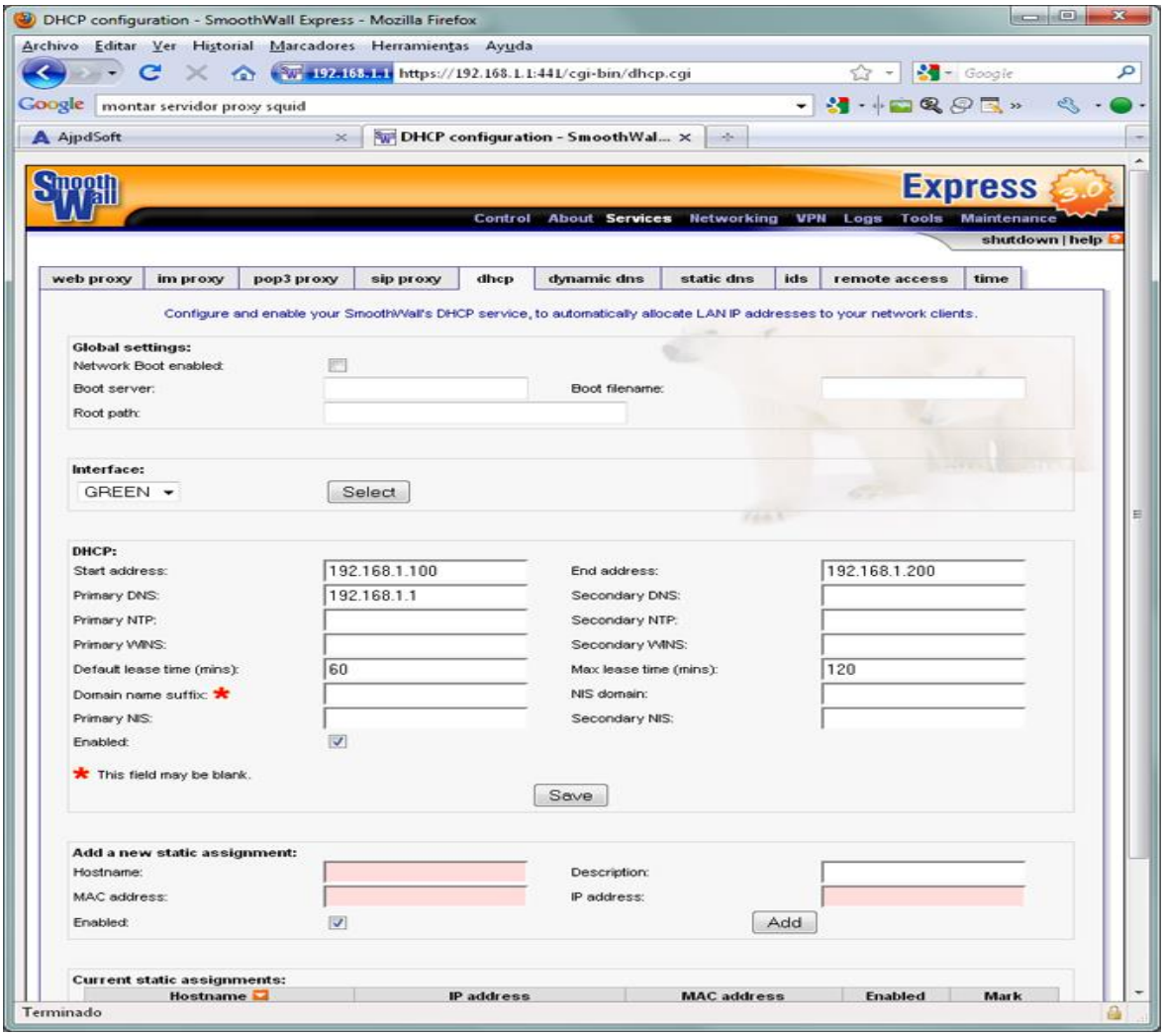
- **IM proxy**: permite activar los servicios de Instant Messenger Proxy, para capturar las conversaciones de chat de los distintos servicios: MSN, ICQ, IAM, IRC, Jabber, GTalk, Yahoo, Gadu-Gdu, facebook:



- **POP3 proxy**: posibilidad de activar el servicio POP3 proxy, de forma que el tráfico del correo electrónico será analizado por el antivirus incluido en SmoothWall: ClamAV, en busca de virus, de esta forma, antes de que llegue un correo con virus a un usuario, será analizado y eliminado por SmoothWall:



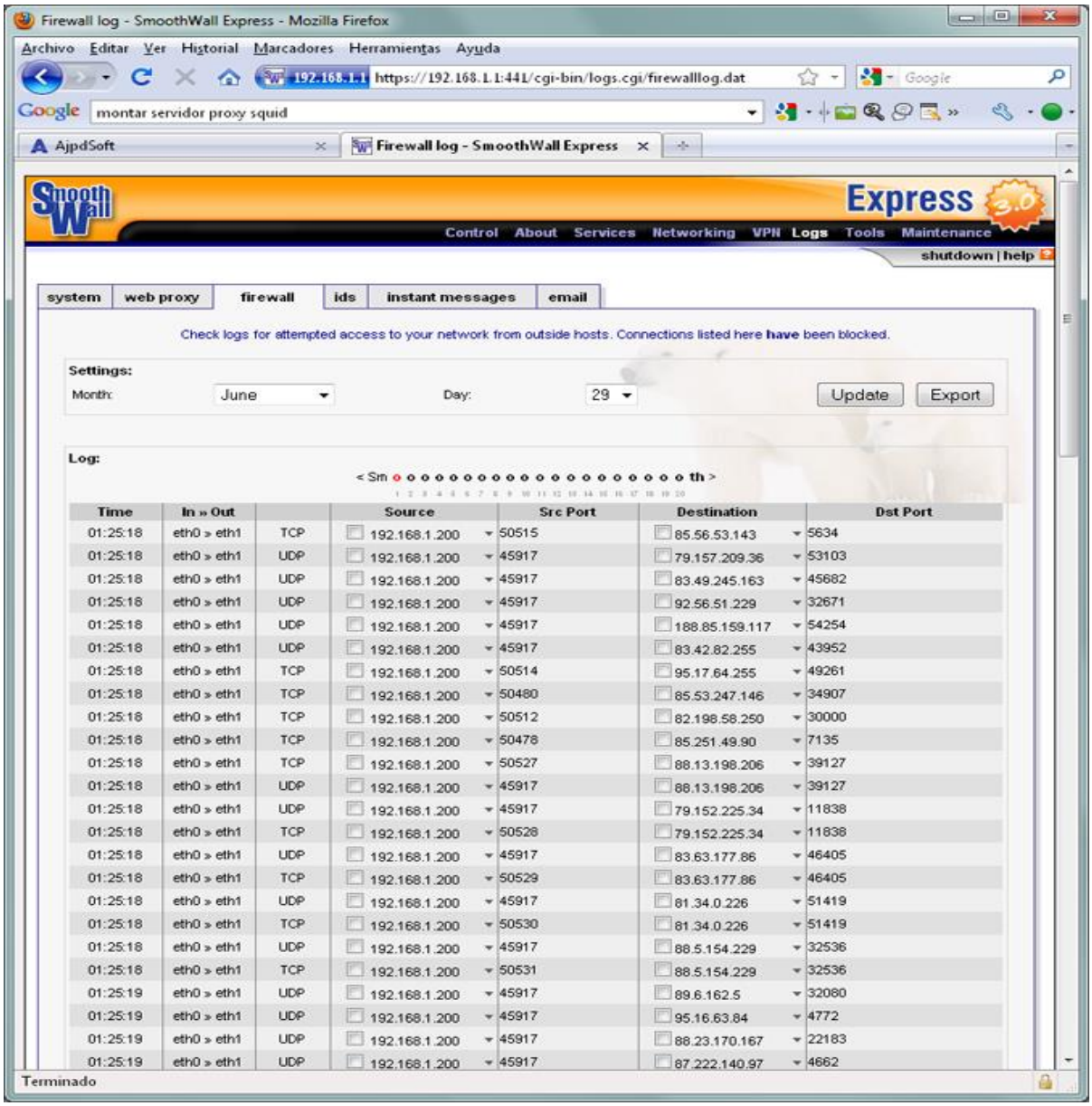
- **DHCP**: activar servicio de DHCP, con esta utilidad el equipo con SmoothWall podrá asignar direcciones IP y configuración de red (IP, DNS y gateway) al resto de los equipos de la red de forma automática, será suficiente con que los equipos de la red tengan habilitada la optención de la IP mediante DHCP:



Probando el firewall o cortafuegos, monitorizar, ver log

Desde el menú "Logs" de la administración de SmoothWall podremos analizar el tráfico y los distintos servicios activados de SmoothWall (web proxy, firewall, Snort IDS (detección de intrusiones), instant messages (chat), email, etc.

Desde la opción "firewall" podremos ver todos los paquetes enviados y recibidos entre nuestra red e Internet:



Desde la opción de monitorización anterior, podremos ver o guardar en fichero (filtrando adecuadamente) todo el tráfico que se produce entre Internet y nuestros equipos informáticos, con los siguientes datos:

- **Time**: hora en la que se produce el envío o recepción del paquete.
- **In Out**: desde qué interfaz de red hacia qué interfaz de red del cortafuegos se envía el paquete.
- Tipo de protocolo (TCP, UDP, etc.).
- **Source**: IP origen del paquete, desde donde procede el paquete.
- **Src Port**: puerto origen por el que se envía el paquete.
- **Destination**: IP destino del paquete enviado.
- **Dst Port**: puerto de destino del paquete.

Conclusión:
Finalmente hemos conseguido montar nuestra infraestructura de seguridad para poder realizar las dos tareas que nos planteamos en un principio:

- Tener una red LAN segura
- Tener control sobre el acceso a internet por parte de los usuarios