Universidad Tecnológica de El Salvador

FACULTAD DE INFORMÁTICA Y CIENCIAS APLICADAS

TÉCNICO EN INGENIERÍA DE REDES COMPUTACIONALES

Tema:

Propuesta de solución unificada de administración de los recursos de TI, que garantice la disponibilidad de los servicios; optimizando el manejo y el control de los activos informáticos reduciendo los costos de inversión en adquisición e implementación de los servicios de red en la Pequeña y Mediana Empresa (PYME)

Trabajo de graduación presentado por:

Gloria Marisol de López

Juan Pablo López

Frank Baltazar Ayala

Para optar al grado de:

Técnico en Ingeniería de Redes Computacionales.

Septiembre de 2012

San Salvador, El Salvador, Centro América.

HOJA DE REVISIÓN DESPUÉS DE LA DEFENSA

Por este medios los miembros del jurado evaluador del trabajo de Graduación titulado: Propuesta de solución unificada de administración de los recursos de TI, que garantice la disponibilidad de los servicios; optimizando el manejo y el control de los activos informáticos reduciendo los costos de inversión en adquisición e implementación de los servicios de red en la Pequeña y Mediana Empresa (PYME).

Presentado por:

1. Juan Pablo López
2. Gloria Marisol de López
3. Frank Baltazar Ayala

Después de la defensa Oral, hemos revisado el Trabajo escrito y se han incluido en él las observaciones realizadas durante la misma.

Por lo que damos por APROBADO y finalizado el Trabajo:

San Salvador, a los _____ días del mes de _____ de _____

F_____ F_____

Ing. Oscar Ernesto Rodríguez Alfaro Lic. Jorge Alberto Portillo Chaves

F_____

Ing. Salvador Alcides Franco Sánchez

PÁGINA DE AUTORIDADES

LIC. JOSÉ MAURICIO LOUCEL

RECTOR

ING. NELSON ZÁRATE SÁNCHEZ

VICERRECTOR ACADÉMICO

ING. FRANCISCO ARMANDO ZEPEDA

DECANO

JURADO EXAMINADOR

LIC. JORGE ALBERTO PORTILLO CHAVES

PRESIDENTE

ING. OSCAR ERNESTO RODRÍGUEZ ALFARO

PRIMER VOCAL

ING. SALVADOR ALCIDES FRANCO SÁNCHEZ

SEGUNDO VOCAL

SEPTIEMBRE 2012

SAN SALVADOR, EL SALVADOR, CENTROAMERICA

AGRADECIMIENTOS.

Agradezco ante todo a Dios por la vida, por darme la fuerza y sabiduría necesaria para salir adelante.

A mis padres quienes me instruyeron desde la infancia a poder ser alguien en la vida y poder llegar a tener éxito y a mis hermanas y hermano quienes con sus palabras de aliento me han apoyado.

Al Ing. Alcides Franco por haberme instruido en toda mi carrera técnica y a todas mis amistades y compañeros de trabajo que depositaron su confianza en mí.

A mi esposo quien me motiva a poder triunfar profesionalmente y me ha dado todo su apoyo incondicional para terminar esta carrera, y en especial a mi hija Sofía Marisol quien es y será mi fuerza para toda la vida.

Gloria Marisol Amaya de López

AGRADECIMIENTOS.

Este espacio lo dedico principalmente para darle gracias a Dios por la fortaleza y sabiduría que me ha dado durante todo el desarrollo de mis estudios, a mis padres y hermano por la paciencia, ayuda y los consejos sabios que siempre me han brindado.

A mí amada esposa y compañera quien siempre me brinda todo su apoyo incondicional. A mi compañero Frank Ayala quien ha sido de gran ayuda durante este proceso.

Al Ingeniero Alcides Franco por su confianza y tiempo que dedicó para guiar este trabajo a su culminación.

Y en especial a mi hija Sofía Marisol por ser mi luz y el motivo más grande para seguir adelante superándome día con día.

Juan Pablo López Aguilar

AGRADECIMIENTOS.

La realización del presente trabajo de graduación, lo agradezco de manera muy especial al que es digno de toda la gloria, honra y honor, a Dios, por guiarme, darme la sabiduría y fortaleza en el momento que lo necesitaba. Gracias Señor.

A mis padres y hermanos:

Gracias a mis padres por su esfuerzo, sacrificio y tiempo. Por la educación académica y espiritual que me han brindado. Por ayudarme a alcanzar mis metas. Gracias a mis hermanos por darme apoyo moral y económico cuando lo he necesitado.

A nuestro asesor:

Ing. Alcides Franco, por brindarnos una mano siempre que la necesitamos. Por ayudarnos a ser responsables en todo sentido de la vida.

A mis compañeros:

Juan Pablo y Gloria Marisol, doy gracias por su amistad y por haberse mantenido firmes durante toda realización de este trabajo de graduación.

A todos mis familiares y amigos:

Que de una u otra manera estuvieron pendientes a lo largo de este proceso, brindado su apoyo incondicional.

Frank Baltazar Ayala

ÍNDICE

CAPITULO II

DOCUMENTACIÓN TÉCNICA Y DISEÑO DE LA SOLUCIÓN

CAPITULO III

Propuesta de la solución

INTRODUCCIÓN

En la actualidad los problemas de seguridad informáticos los cuales enfrentan mayoría de las PYMES y la demanda de desarrollo empresarial, obliga a la actualización o adquisición de herramientas tecnológicas que ayuden a incrementar la productividad y mejoren la seguridad de la información, optimizando el manejo y control de los datos, la mayoría de estas pequeñas o medianas empresas no cuentan con un presupuesto establecido para este tipo de necesidades y se ven obligados a trabajar de una forma inadecuada con pocos mecanismos de protección o ningún mecanismo.

Con el fin de analizar dichas problemáticas se toma como ejemplo una PYME, de nombre Droguería Universal S.A de C.V la cual no está exenta a esa necesidad, y no cuenta con los recursos necesarios para solventar las deficiencias de seguridad en la red.

En el desarrollo de este proyecto se realiza un análisis exhaustivo de la problemática existente, infraestructura de la red, tecnologías y herramientas Open Source, con las cuales se plantea como solventar la problemática, beneficiando a la compañía con la implementación de estas herramientas no incurriendo en costos de licenciamiento y mantenimiento de estos.

CAPITULO I
Situación Actual

1.1 Situación Problemática

Actualmente la empresa Droguería Universal S.A de C.V compañía sólidamente constituida dedicada al rubro de venta y distribución de insumos farmacéuticos y productos médicos, presenta algunas deficiencias de administración adecuada de sus recursos tecnológicos de internet, conllevando a los empleados a tener dificultades para ejecutar adecuadamente las actividades diarias, para la compañía el internet se ha convertido en un recurso indispensable para la búsqueda de información que apoye sus funciones laborales; sin embargo estas mismas actividades que hacen al personal eficiente y productivo exponen a la compañía a riesgos de seguridad muy serios como los son los virus, spyware y códigos maliciosos que se propagan por la web y pueden afectar en gran medida la disponibilidad confidencialidad e integridad de la información que maneja la empresa.

Se cuenta con una persona de TI[1] el cual está destinado a resolver fallas en los equipos y a la administración de un sistema de inventarios, pero no le ha sido

[1] (Information technology, IT). Tecnologías de la información o simplemente TI, es un amplio concepto que abarca todo lo relacionado a la conversión, almacenamiento, protección, procesamiento y transmisión de la información.

posible solventar algunos inconvenientes por falta de herramientas que le permitan una buena administración de los recursos.

La empresa carece de una adecuada estrategia de seguridad que proteja los recursos y activos informáticos, adicionalmente a esto se le suma el uso inadecuado de los recursos de Internet; volviéndose lento e imposibilitando el acceso a la información alojada en la web, no se cuenta con la administración y monitoreo centralizado de las bitácoras de registros de tráfico de navegación. Por lo cual se dificulta anticiparse e identificar incidentes de seguridad en los equipos de la compañía, no cuenta con la documentación necesaria de su infraestructura de red y esto causa mayores inconvenientes al presentarse una falla y no es posible identificar fácilmente, todas estas situaciones afectan significativamente la productividad y el desarrollo de la compañía.

1.2 Justificación del proyecto

El desarrollo de este proyecto permite la adecuada gestión de los recursos tecnológicos, referente a la administración y manejo de incidentes de seguridad que pueden suscitarse en la red a nivel básico.

Se pretende la implementación de una tecnología que permita el balance entre seguridad, accesibilidad y un óptimo rendimiento, solventando las necesidades; reduciendo fallas y armonizando el entorno de las tecnologías que actualmente están implementadas.

Permitiendo en un futuro adaptar nuevas herramientas adecuándose al crecimiento de la empresa, este proyecto adicionalmente del beneficio tecnológico, permitirá la reducción en costos de implementación y mantenimiento de estos, ya que no se requiere licenciamiento de productos por utilizarse herramientas de código abierto.

Otros beneficios adicionales que se lograran con dicha implementación se enumeran de forma general:

- Evitar el acceso a la información confidencial por personas no autorizadas.
- Optimizar el trabajo y el uso de ancho de banda, garantizándolo para aplicaciones críticas del negocio
- Minimizar el riesgo de amenazas de código malicioso virus, troyanos, spyware etc.
- Mayor control del tráfico de internet

1.3 Objetivos

1.3.1 General

Implementar una la solución unificada Open Source[2] de administración de seguridad básica de infraestructura de red y servicios, que permita ejecutar

[2] Open Source: término con el que se conoce al software distribuido y desarrollado libremente (Código Abierto).

estándares y políticas para el fortalecimiento de la red existente como un complemento y beneficio para la compañía y cada uno de los usuarios permitiendo el acceso a la información de forma segura y eficaz.

1.3.2 Específicos

- Analizar exhaustivamente la situación actual de la compañía e identificar cuáles son los recursos con los que se cuentan, identificar las deficiencias y necesidades tecnológicas por parte de la corporación.
- Realizar una investigación de las tecnologías de seguridad y administración Open Source que mejor se adecuen a la arquitectura lógica y física. permitiendo solventar las necesidades tecnológicas y llevar a cabo una estrategia de gestión de recursos informáticos seguros.
- Realizar la propuesta de implementación de solución unificada en base al análisis y diseño tecnológico en la compañía a fin de distribuir correctamente las herramientas que mejor se adecuen a la compañía; permitiendo un balance entre seguridad y accesibilidad de la información.

1.4 Alcances

- Documentar como se encuentra actualmente la infraestructura de red y realizar las modificaciones necesarias para la implementación de forma estratégica de la o las herramientas que nos permitirán gestionarla

- La Implementación de la herramienta Open Source permitirá realizar administración de la seguridad y el monitoreo de la red de forma efectiva y eficaz
- La tecnología de Open Source permitirá obtener grandes beneficios y ahorro a la corporación y al personal de TI para la gestión de recursos tecnológicos.

1.5 Estudio de Factibilidad

1.5.1Técnica

El análisis exhaustivo de factibilidad técnica determina que: La compañía está en la facultad de la implementación de la solución unificada de seguridad; ya que la infraestructura de red está en las condiciones adecuadas para ejecutar la solución, contando con un pequeño MDF[3] y 3 IDFS[4] los cuales se encargan de interconectar físicamente los equipos de la compañía.

El cableado fue renovado en la mayoría de las áreas, adicionalmente a esto se cuenta con una cantidad considerable de ordenadores con sistemas operativos Microsoft. Ver cuadro 1.1 para llevar a cabo la ejecución del proyecto, se cuenta

[3] MDF: armario de distribución principal o punto de control central de la red

[4] IDF: Armario de distribución secundaria o punto de control secundario de la red

con un servidor de directorio Microsoft Windows Server 2008 R2, que de igual forma ejecuta el rol de DNS Server.

Información brindada por encargado de departamento de informática: Carlos Pacheco

Imagen 1.1 MDF

Imagen 1.2 IDF Contabilidad

Imagen 1.4 oficina de contabilidad

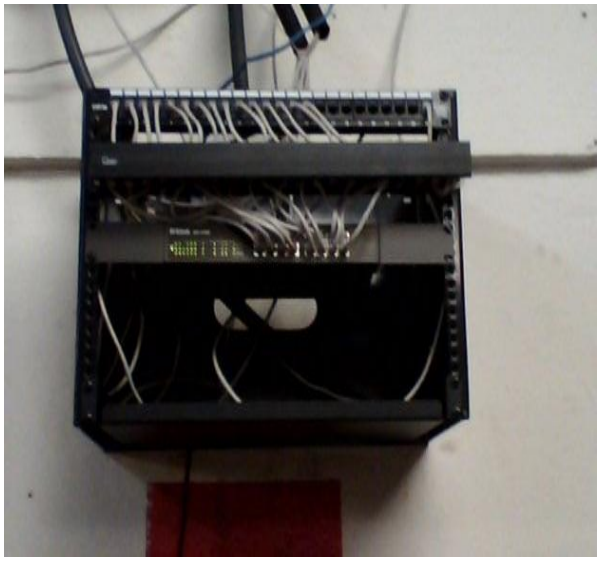

Imagen n 1.3 IDF segundo nivel

Cuadro 1.1 Tabla de ordenadores existentes

N	Dirección de IP	Sistema Operativo	Equipo
1	192.168.1.11	Windows Server 2008 R2 Enterprise	Servidor IBM
2	192.168.1.42	Microsoft Windows 7 Professional	CPU
3	192.168.1.39	Microsoft Windows XP Professional	CPU
4	192.168.1.37	Microsoft Windows 7 Ultimate	CPU
5	192.168.1.33	Microsoft Windows XP Professional	CPU
6	192.168.1.29	Microsoft Windows XP Professional	CPU
7	192.168.1.112	Microsoft Windows XP Professional	CPU
8	192.168.1.70	Microsoft Windows XP Professional	CPU
9	192.168.1.62	Microsoft Windows XP Professional	CPU
10	192.168.1.67	Microsoft Windows XP Professional	CPU
11	192.168.1.52	Microsoft Windows XP Professional	CPU
12	192.168.1.49	Microsoft Windows XP Professional	CPU
13	192.168.1.61	Microsoft Windows XP Professional	CPU
14	192.168.1.38	Microsoft Windows 7 Professional	CPU
15	192.168.1.20	Microsoft Windows XP Professional	CPU
16	192.168.1.13	Microsoft Windows XP Professional	CPU
17	192.138.1.55	Microsoft Windows XP Professional	CPU
18	192.168.1.70	Microsoft Windows XP Professional	CPU
19	192.168.1.27	Microsoft Windows XP Professional	CPU
20	192.168.1.14	Microsoft Windows 7 Professional	CPU
21	192.168.1.38	Microsoft Windows XP Professional	CPU
22	192.168.1.51	Microsoft Windows XP Professional	CPU

1.5.2 Económica

El análisis de factibilidad económica determina que la compañía está en la disposición de tomar a consideración la implementación de la solución unificada de seguridad brindando el apoyo en cuanto la disponibilidad de tiempo para investigación e implementación de la solución.

Adicionalmente la empresa da su visto bueno, ya que comprenden los múltiples beneficios que se obtendrán la implementarse herramientas de software libre y no se tendrá que incurrir en gastos de licenciamiento[5] e implementación; pero se evaluara la adquisición del equipo cuando ya se tenga establecido que herramientas son las necesarias a implementar para solventar las necesidades con las que se cuenta actualmente en la compañía

1.5.3 Operacional

Se estudió detenidamente evidenciando cuales son los procesos adecuados y necesarios en la compañía para efectuar el proyecto, sin interferir con la productividad.

[5] Una **licencia de software** es un contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor)

Se desarrollaran las pruebas previas a la implementación en un entorno virtual fuera de las instalaciones de la empresa, recreando la infraestructura lógica de la red, además se contara con el apoyo del encardo de TI de la compañía.

El cual realizara la evaluación de las directivas de seguridad y los servicios de red, antes de cualquier instalación.

Compaginando la implementación con las tecnologías existentes dentro de las cuales destacan: Directorio Activo de Microsoft, Pryme (Software de control de Inventario y facturación).

La nueva implementación deberá coexistir con estas tecnologías sin provocar inconveniente alguno, para luego al obtener la aprobación podrá implementarse y colocarse en producción

1.6 Carta de autorización del beneficiario.

San Salvador, marzo de 2012

Asunto: Beneplácito de proyección social

(Proyecto de Tesis)

Universidad Tecnológica de El Salvador

Presente:

Es un placer saludarles deseándoles muchos éxitos en las diferentes actividades Laborales, la presente es para hacer de su conocimiento que los alumnos **Juan Pablo López, Gloria Marisol de López y Frank Baltazar Ayala,** en calidad de egresados de la Universidad Tecnológica de El Salvador. Planteando su proyecto de tesis en Soluciones Open Source, la cual se desarrolla bajo los siguientes pasos:

- Analizar exhaustivamente la situación actual de la compañía e identificar las deficiencias y necesidades tecnológicas por parte de la corporación.
- Realizar una investigación de las tecnologías de seguridad y administración Open Source que mejor se adecuen a la arquitectura lógica y física. permitiendo solventar las necesidades tecnológicas y llevar a cabo una estrategia de gestión de recursos informáticos seguros.
- Realizar La propuesta de implementación de solución unificada en base al análisis y diseño tecnológico en la compañía a fin de distribuir correctamente las herramientas que mejor se adecuen a ella, permitiendo un balance entre seguridad y accesibilidad de la información.

Para ello se ha tomado a bien proponer dicho proyecto en la empresa **Droguería Universal S.A de C.V**, Empresa sólidamente constituida y dedica al rubro de venta y distribución de insumos médicos y farmacéuticos.

La cual ha brindado la oportunidad de realizar dicho proyecto, a través del encargado del área de informática **Carlos Alberto Henrique Pacheco**. Quien ha brindado la aprobación del desarrollo de la actividad, sin más que añadir, nos despedimos cordialmente adicionando las firmas de aceptación del desarrollo de dicho proyecto.

_____	_____
Encargado de TI Carlos Pacheco	**Asesor** Ing. Salvador Alcides Franco
_____	_____
Catedrático Ing. Salvador Alcides Franco	**Alumna** Gloria Marisol de López
_____	_____
Alumno Juan Pablo López	**Alumno** Frank Baltazar Ayala

CAPITULO II
Documentación técnica y diseño de la solución

2.1 Marco teórico de la solución

Los conceptos necesarios para el entendimiento de este proyecto de propuesta de solución están relacionados con las normas y tecnologías de seguridad que existen en la actualidad en cuanto a redes y sistemas informáticos.

En esta categoría de normas, se consideran las relacionadas directamente con todo tipo de necesidades puntuales de seguridad para sistemas, protocolos de comunicación y aplicaciones.

Se pretende cubrir las necesidades existentes en la compañía que está siendo objeto de investigación, y se requiere la implementación de una estrategia de seguridad apoyado en herramientas open source, que brinden cierto nivel de seguridad y garanticen la funcionabilidad de la comunicación de la red interna con el exterior.

Las herramientas propuestas podrán ser implementadas anticipándose al crecimiento y desarrollo empresarial o tecnológico que la compañía pueda tener a mediano o largo plazo.

2.2 Documentación técnica de la solución

2.2.1 Open Source

El software Open Source se define por la licencia[6] que lo acompaña, que garantiza a cualquier persona el derecho de usar, modificar y redistribuir el código libremente.

Open Source es una marca de certificación propiedad de la Open Source Initiative. Los desarrolladores que diseñan software para ser compartido, mejorado y distribuido libremente, pueden usar la marca registrada Open Source si sus términos de distribución se ajustan a la definición Open Source de la OSI[7]. Básicamente, el modelo de distribución requiere que: **Libre distribución**. No haya restricciones para vender o distribuir el software.

- **Código fuente**. El software debe incluir el código fuente y debe permitir crear distribuciones compiladas siempre y cuando la forma de obtener el código fuente esté expuesta claramente.
- **Trabajos derivados**. Se debe permitir crear trabajos derivados, que deben ser distribuidos bajo los mismos términos que la licencia original del software.

[6] El uso de un programa o aplicación computacional sin ser uno el dueño,

[7] (OSI) Open Source Initiative.

- **Integridad del código fuente del autor**. Se debe permitir la distribución del código fuente modificado, aunque pueden haber restricciones para que se pueda distinguir el código fuente original del código fuente del trabajo derivado.
- **No discriminar personas o grupos**. La licencia no debe discriminar a ninguna persona o grupo.
- **No discriminar ningún tipo de uso del programa**. La licencia no debe impedir a nadie el uso del programa en una determinada actividad. Por ejemplo, no puede impedir el uso en una empresa, o no puede impedir el uso en investigación genética.
- **Distribución de la Licencia**. Los derechos que acompañan al programa deben aplicarse a todo el que redistribuya el programa, sin necesidad de licencias adicionales.
- **La licencia no debe ser específica a un producto**. Los derechos que da la licencia no deben ser diferentes para la distribución original y para la que funciona en un contexto totalmente diferente.
- **La licencia no debe ir en contra de otro software**. La licencia no debe restringir otro software que se distribuya con el mismo. Por ejemplo, la licencia no debe indicar que todos los programas distribuidos conjuntamente con el deben ser Open Source.

Software libre y de código abierto

El **software libre y de código abierto** (también conocido como ***FOSS*** o ***FLOSS)***[8], es el software que está licenciado de tal manera que los usuarios pueden estudiar, modificar y mejorar su diseño mediante la disponibilidad de su código fuente.

El término "software libre y de código abierto" abarca los conceptos de software libre y software de código abierto, que, si bien comparten modelos de desarrollo similares, tienen diferencias en sus aspectos filosóficos.

El software libre se enfoca en las libertades filosóficas que les otorga a los usuarios mientras que el software de código abierto se enfoca en las ventajas de su modelo de desarrollo. "FOSS" es un término imparcial respecto a ambas filosofías.

El software gratis no necesariamente tiene que ser libre o de código abierto.

Organizaciones y licencias tras el FOSS

Existen organizaciones detrás de cada iniciativa de distinción del software.

[8] Free/libre and open source software

Por parte del software libre, existe la Free Software Foundation (FSF); apoyando el concepto de software de código abierto.

Ambas se enfocan en diferentes aspectos del uso y distribución del software, y su disponibilidad y responsabilidades que competen al usuario tener. Por este motivo existen diferentes licencias que las diferencian:

Licencias de código abierto (para el software de código abierto), licencias de software libre (para el software libre), entre otras, sin protección heredada y con protección heredada.

Seguridad informática, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida).

Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

Estrategia de Seguridad

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

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

Estrategia proactiva (proteger y proceder) o de previsión de ataques es un conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes en las directivas de seguridad y a desarrollar planes de contingencia.

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

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

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

- Lo que no se permite expresamente está prohibido: significa que la organización proporciona una serie de servicios bien determinados y documentados, y cualquier otra cosa está prohibida.
- Lo que no se prohíbe expresamente está permitido: significa que, a menos que se indique expresamente que cierto servicio no está disponible, todos los demás sí lo estarán.

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

Estos son ejemplos de unos ataques mas comúnmente usados en la red

- ARP Spoofing (es una técnica usada para infiltrarse en una red Ethernet)

- Cross-site scripting (agujero de seguridad típico de las aplicaciones Web)

- Spoofing (uso de técnicas de suplantación de identidad)

- Syn Flood (flujo de paquetes muchas veces con la dirección de origen)

- SQL Injection (método de infiltración de código intruso para realizar consultas a una base de datos).

2.2.2 Soluciones de seguridad unificadas

Debido al rápido crecimiento y evolución de las tecnologías basadas en Linux y Software Libre, actualmente existe una gran diversidad en las soluciones profesionales que giran entorno a este concepto.

Por esta razón, las soluciones unificadas estandarizan las soluciones más demandadas en las empresas, con el objeto de facilitar soluciones según sus necesidades.

Soluciones de seguridad unificadas ofrece una amplia y completa gama de servicios, así como su integración con las principales plataformas existentes en el mercado.

A continuación se detallan algunas características con las que se cuentan y podrán ser implementadas en la compañía objeto de investigación.

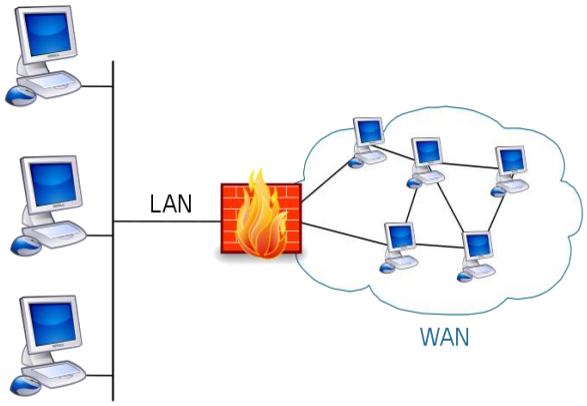

Figura 2.1 Esquema de un firewall

Firewall

Un **cortafuego** (***firewall*** en inglés) es una parte de un sistema o una red que está diseñada para bloquear o denegar el acceso a personas no autorizadas a una pc, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets.

Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuego, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

También es frecuente conectar al cortafuego a una tercera red, llamada: Zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuego correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente.

La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

Tipos de cortafuegos

Nivel de aplicación de Gateway

Aplica mecanismos de seguridad para aplicaciones específicas, tales como servidores FTP[9] y Telnet. Esto es muy eficaz, pero puede imponer una degradación del rendimiento.

Circuito a nivel de Gateway

Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Una vez que la conexión se ha hecho, los paquetes pueden fluir entre los anfitriones sin más control. Permite el establecimiento de una sesión que se origine desde una zona de mayor seguridad hacia una zona de menor seguridad.

Cortafuegos de capa de red o de filtrado de paquetes

Funciona a nivel de red (capa 3 del modelo OSI, capa 2 del stack de protocolos TCP/IP) como filtro de paquetes IP.

[9] File Transfer Protocol usado en internet. Permite transferir archivos locales hacia un servidor web

A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (capa 3 TCP/IP, capa 4 Modelo OSI), como el puerto origen y destino, o a nivel de enlace de datos (no existe en TCP/IP, capa 2 Modelo OSI) como la dirección MAC.

Cortafuegos de capa de aplicación

Trabaja en el nivel de aplicación (capa 7 del modelo OSI), de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP, se pueden realizar filtrados según la URL a la que se está intentando acceder.

Un cortafuego a nivel 7 de tráfico HTTP suele denominarse proxy, y permite que los computadores de una organización entren a Internet de una forma controlada. Un proxy oculta de manera eficaz las verdaderas direcciones de red.

Cortafuego personal

Es un caso particular de cortafuegos que se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red. Se usa por tanto, a nivel personal.

Políticas del cortafuego

Hay dos políticas básicas en la configuración de un cortafuego que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

- **Política restrictiva**: Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuego obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten. Esta aproximación es la que suelen utilizar las empresas y organismos gubernamentales.

- **Política permisiva**: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado. Esta aproximación la suelen utilizar universidades, centros de investigación y servicios públicos de acceso a internet.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por omisión.

DMZ[10]

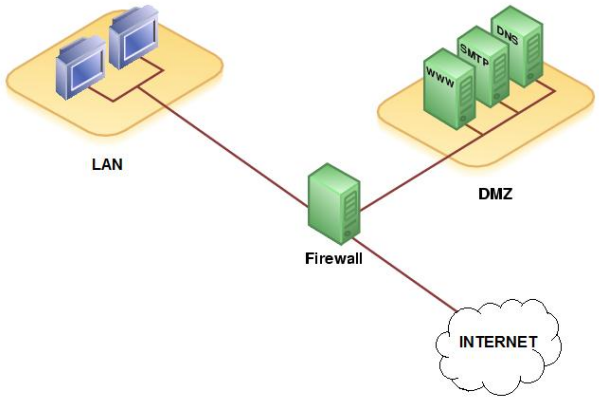

Figura 2.2 Diagrama de una red típica que usa una DMZ

Red perimetral o DMZ, es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

[10] (Demilitarized zone) Zona desmilitarizada

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, Web y DNS.

Las conexiones que se realizan desde la red externa hacia la DMZ se controlan generalmente utilizando port address translation (PAT).

Una DMZ se crea a menudo a través de las opciones de configuración del cortafuego, donde cada red se conecta a un puerto distinto de éste. Esta configuración se llama cortafuegos en trípode (three-legged firewall).

Un planteamiento más seguro es usar dos cortafuegos, donde la DMZ se sitúa en medio y se conecta a ambos cortafuegos, uno conectado a la red interna y el otro a la red externa. Esta configuración ayuda a prevenir configuraciones erróneas accidentales que permitan el acceso desde la red externa a la interna. Este tipo de configuración también es llamado cortafuegos de subred monitoreada (screened-subnet firewall).

Servidor Proxy

Un proxy es un programa o dispositivo que realiza una tarea acceso a Internet en lugar de otro ordenador. Un proxy es un punto intermedio entre un ordenador conectado a Internet y el servidor al que está accediendo. Cuando navegamos a través de un proxy, nosotros en realidad no estamos accediendo directamente

al servidor, sino que realizamos una solicitud sobre el proxy y es éste quien se conecta con el servidor que queremos acceder y nos devuelve el resultado de la solicitud.

Figura 2.3 Diagrama de un servidor Proxy

Servidor HTTP

Este tipo de servidor opera en la Capa de aplicación de TCP/IP. El puerto de comunicación de entrada debe ser 80/http según IANA. Aunque generalmente suelen utilizar otros puertos de comunicación como el 3128, 8080 o el 8085.

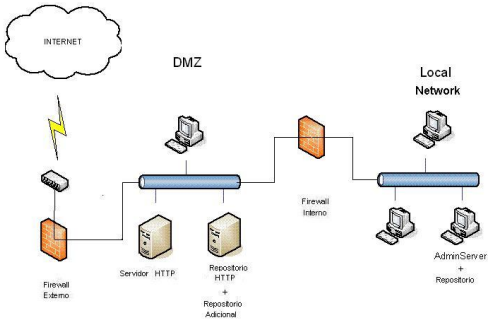

Figura 2.4 Diagrama de un servidor HTTP

Servidor HTTPS

Este tipo de servidor opera en la Capa de aplicación de TCP/IP. A diferencia de un Servidor HTTP, funciona bajo tecnologías de cifrado como SSL/TLS[11] que proporcionan mayor seguridad y anonimato. El puerto utilizado varía, aunque debe ser 443/https.

Servicio Proxy o Proxy Web

Su funcionamiento se basa en el del Proxy HTTP y HTTPs, pero la diferencia fundamental es que la petición se realiza mediante una aplicación Web embebida en un servidor HTTP al que se accede mediante una dirección DNS, esto es, una página web que permite estos servicios.

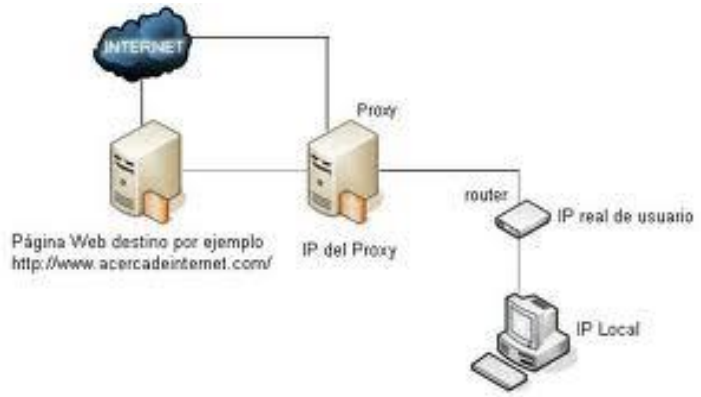

Figura 2.5 diagrama de servicio proxy

[11] (*Secure Sockets Layer)* capa de conexión segura
(*Transport Layer Security)* seguridad de la capa de transporte

Características

El uso más común es el de **servidor proxy**, que es un ordenador que intercepta las conexiones de red que un cliente hace a un servidor de destino.

De ellos, el más famoso es el **servidor proxy web** (comúnmente conocido solamente como «**proxy**»). Intercepta la navegación de los clientes por páginas web, por varios motivos posibles: seguridad, rendimiento, anonimato, etc.

Ventajas

- **Control**: sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al proxy.
- **Ahorro**. Por tanto, sólo *uno* de los usuarios (el proxy) ha de estar equipado para hacer el trabajo real.
- **Velocidad**. Si varios clientes van a pedir el mismo recurso, el proxy puede hacer caché: guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.
- **Filtrado**. El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.
- **Modificación**. Como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.

- **Anonimato**. Si todos lo usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos.

  Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.

Proxy Caché

Su método de funcionamiento es similar al de un proxy HTTP o HTTPs. Su función es precargar el contenido web solicitado por el usuario para acelerar la respuesta Web en futuras peticiones de la misma información de la misma máquina u otras

Proxies transparentes

Combina un servidor proxy con NAT[12] de manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia. Este es el tipo de proxy que utilizan los proveedores de servicios de internet (ISP).

Reverse Proxy / Proxy inverso

Es un servidor proxy instalado en el domicilio de uno o más servidores web. Todo el tráfico entrante de Internet y con el destino de uno de esos servidores

[12] (Network Address Translation) Traducción de dirección de red

web pasa a través del servidor proxy. Hay varias razones para instalar un "reverse proxy":

- Seguridad: el servidor proxy es una capa adicional de defensa y por lo tanto protege los servidores web.
- Cifrado / Aceleración SSL: cuando se crea un sitio web seguro, habitualmente el cifrado SSL no lo hace el mismo servidor web, sino que es realizado por el "reverse proxy", el cual está equipado con un hardware de aceleración SSL.
- Distribución de Carga: el "reverse proxy" puede distribuir la carga entre varios servidores web. En ese caso, el "reverse proxy" puede necesitar rescribir las URL de cada página web (traducción de la URL externa a la URL interna correspondiente, según en qué servidor se encuentre la información solicitada).
- Caché de contenido estático: Un "reverse proxy" puede descargar los servidores web almacenando contenido estático como imágenes u otro contenido gráfico.

Proxy NAT / Enmascaramiento

Otro mecanismo para hacer de intermediario en una red es el NAT.

La traducción de direcciones de red (NAT, Network Address Translation) también es conocida como enmascaramiento de IPs.

Es una técnica mediante la cual las direcciones fuente o destino de los paquetes IP son rescritas, sustituidas por otras (de ahí el "enmascaramiento").

Esto es lo que ocurre cuando varios usuarios comparten una única conexión a Internet. Se dispone de una única dirección IP pública, que tiene que ser compartida.

Dentro de la red de área local (LAN) los equipos emplean direcciones IP reservadas para uso privado y será el proxy el encargado de traducir las direcciones privadas a esa única dirección pública para realizar las peticiones, así como de distribuir las páginas recibidas a aquel usuario interno que la solicitó. Estas direcciones privadas se suelen elegir en rangos prohibidos para su uso en Internet como 192.168.x.x, 10.x.x.x, 172.16.x.x y 172.31.x.x

Esta situación es muy común en empresas y domicilios con varios ordenadores en red y un acceso externo a Internet. El acceso a Internet mediante NAT proporciona una cierta seguridad, puesto que en realidad no hay conexión directa entre el exterior y la red privada, y así nuestros equipos no están expuestos a ataques directos desde el exterior.

Mediante NAT también se puede permitir un acceso limitado desde el exterior, y hacer que las peticiones que llegan al proxy sean dirigidas a una máquina concreta que haya sido determinada para tal fin en el propio proxy.

La función de NAT reside en los Cortafuegos y resulta muy cómoda porque no necesita de ninguna configuración especial en los equipos de la red privada que pueden acceder a través de él

Proxy abierto

Este tipo de proxy es el que acepta peticiones desde cualquier ordenador, esté o no conectado a su red.

En esta configuración el proxy ejecutará cualquier petición de cualquier ordenador que pueda conectarse a él, realizándola como si fuera una petición del proxy. Por lo que permite que este tipo de proxy se use como pasarela para el envío masivo de correos de spam[13]. Un proxy se usa, normalmente, para almacenar y redirigir servicios como el DNS o la navegación Web, mediante el cacheo de peticiones en el servidor proxy, lo que mejora la velocidad general de los usuarios. Este uso es muy beneficioso, pero al aplicarle una configuración "abierta" a todo internet, se convierte en una herramienta para su uso indebido.

[13] Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido

Debido a lo anterior, muchos servidores, como los de IRC[14], o correo electrónicos, deniegan el acceso a estos proxys a sus servicios, usando normalmente listas negras ("BlackList").

Sistema de Prevención de Intrusos (IPS)

Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de *Prevención de Intrusos* es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.

Los IPS fueron inventados de forma independiente por Jed Haile y Vern Paxon para resolver ambigüedades en el monitoreo pasivo de redes de computadoras, al situar sistemas de detecciones en la vía del tráfico. Los IPS presentan una mejora importante sobre las tecnologías de cortafuegos tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos. También es importante destacar que los IPS pueden actuar al nivel de equipo, para combatir actividades potencialmente maliciosas.

[14] *(Internet Relay Chat*) es un protocolo de comunicación en tiempo real basado en texto

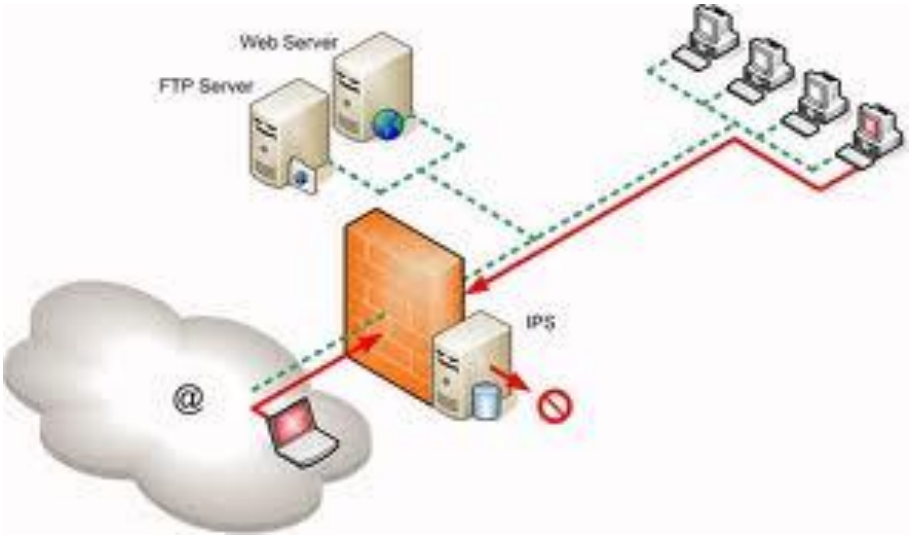

Figura 2.6 Diagrama de sistema de prevención de intrusos

Funcionamiento

Un Sistema de Prevención de Intrusos, al igual que un Sistema de Detección de Intrusos, funciona por medio de módulos, pero la diferencia es que este último alerta al administrador ante la detección de un posible intruso (usuario que activó algún Sensor), mientras que un Sistema de Prevención de Intrusos establece políticas de seguridad para proteger el equipo o la red de un ataque; se podría decir que un IPS protege al equipo proactivamente y un IDS lo protege reactivamente.

Los IPS se categorizan en la forma que detectan el tráfico malicioso:

- Detección Basada en Firmas
- Detección Basada en Políticas
- Detección Basada en Anomalías
- Detección Honey Pot (Jarra de Miel)

Detección Basada en Firmas

Una firma tiene la capacidad de reconocer una determinada cadena de bytes en cierto contexto, y entonces lanza un alerta. Por ejemplo, los ataques contra los servidores Web generalmente toman la forma de URLs[15]. Por lo tanto se puede buscar utilizando un cierto patrón de cadenas que pueda identificar ataques al servidor Web. Sin embargo, como este tipo de detección funciona parecido a un antivirus, el administrador debe verificar que las firmas estén constantemente actualizadas.

Detección Basada en Políticas

En este tipo de detección, el IPS requiere que se declaren muy específicamente las políticas de seguridad. Por ejemplo, determinar que hosts[16] pueden tener

[15] (*uniform resource locato*r) se usa para nombrar recursos en Internet para su localización o identificación.

[16] El término ***host*** es usado en informática para referirse a las computadoras conectadas a una red

comunicación con determinadas redes. El IPS reconoce el tráfico fuera del perfil permitido y lo descarta.

Detección Basada en Anomalías

Este tipo de detección tiende a generar muchos falsos positivos, ya que es sumamente difícil determinar y medir una condición 'normal'.

En este tipo de detección tenemos dos opciones:

1. Detección Estadística de Anormalidades: El IPS analiza el tráfico de red por un determinado periodo de tiempo y crea una línea base de comparación. Cuando el tráfico varía demasiado con respecto a la línea base de comportamiento, se genera una alarma.
2. Detección no estadística de anormalidades: En este tipo de detección, es el administrador quien define el patrón 'normal' de tráfico. Sin embargo, debido a que con este enfoque no se realiza un análisis dinámico y real del uso de la red, es susceptible a generar muchos falsos positivos.

Sistemas pasivos y sistemas reactivos

En un sistema pasivo, el sensor detecta una posible intrusión, almacena la información y manda una señal de alerta que se almacena en una base de datos. En un sistema reactivo, el IDS responde a la actividad sospechosa

reprogramando el cortafuego para que bloquee tráfico que proviene de la red del atacante.

Un sistema que reacciona ante el ataque previniendo que este continúe, se denomina IPS por sus siglas en ingles de "Intrusion prevention system".

Comparación con Cortafuegos

Si bien ambos están relacionados con seguridad en redes de información, un IDS, difiere de un cortafuego, en que este último generalmente examina exteriormente por intrusiones para evitar que estas ocurran. Un cortafuego limita el acceso entre redes, para prevenir una intrusión, pero no determina un ataque que pueda estar ocurriendo internamente en la red. Un IDS, evalúa una intrusión cuando esta toma lugar, y genera una alarma.

Un IDS además observa ataques que se originan dentro del sistema. Este normalmente se consigue examinando comunicaciones, e identificando mediante heurística, o patrones (conocidos como firmas), ataques comunes ya clasificados, y toma una acción para alertar a un operador.

Mecanismos de detección de un ataque

Un IDS, usa alguna de las dos siguientes técnicas para determinar que un ataque se encuentra en curso:

Heurística

Un IDS basado en heurística, determina actividad normal de red, como el orden de ancho de banda usado, protocolos, puertos y dispositivos que generalmente se interconectan, y alerta a un administrador o usuario cuando este varía de aquel considerado como normal, clasificándolo como anómalo.

Patrón

Un IDS basado en patrones, analiza paquetes en la red, y los compara con patrones de ataques conocidos, y pre configurados. Estos patrones se denominan firmas. Debido a esta técnica, existe un periodo de tiempo entre el descubrimiento del ataque y su patrón, hasta que este es finalmente configurado en un IDS. Durante este tiempo, el IDS será incapaz de identificar el ataque.

QoS[17]

Son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (throughput). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.

[17] **(**Quality of Service) Calidad de Servicio

DHCP[18]

Es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Antivirus

Son programas cuyo objetivo es detectar y/o eliminar virus informáticos

Anti Phishing

Phishing es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

Monitoreo

Es la realización del estudio del estado de los recursos. Las funciones del monitoreo de red se llevan a cabo por agentes que realizan el seguimiento y

[18] (Dynamic Host Configuration Protocol) Protocolo de configuración dinámica de host

registro de la actividad de red, la detección de eventos y la comunicación de alertas.

El monitoreo de una red abarca 4 fases[19]:

- Definición de la información de administración que se monitorea.
- Acceso a la información
- Diseño de políticas de administración.
- Procesamiento de la información.

Los tipos de monitoreo son:

- Local.
- Remoto.
- Automático.
- Manual.

Los elementos monitoreados pueden ser:

- En su totalidad.
- En segmentos.

[19] Según las políticas de seguridad que posea la empresa o el departamento de TI, el monitoreo tendrá un resultado deseado.

El monitoreo puede ser realizado en forma:

- Continua.
- Eventual.

Objetivos del monitoreo

- Identificar la información a monitorear
- Diseñar mecanismos para obtener la información necesaria
- Utilizar la información obtenida dentro de las distintas áreas funcionales de administración de red
- Tomar nuevas medidas sobre aspectos de los protocolos, colisiones, fallas, paquetes, etc.
- Almacenar la información obtenida en bases de información de gestión para su posterior análisis.
- Del análisis, obtener conclusiones para resolver problemas concretos o bien para optimizar la utilización de la red.

Dentro del monitoreo de la actividad de la red, los eventos típicos que son monitoreados suelen ser:

- Ejecución de tareas como la realización de copias de seguridad.

- Registro del estado de finalización de los procesos que se ejecutan en la red.
- Registro de las entradas y salidas de los usuarios en la red.
- Registro de arranque de determinadas aplicaciones.
- Errores en el arranque de las aplicaciones, etc.

En función de la prioridad que tengan asignados los eventos y de la necesidad de intervención, se pueden utilizar diferentes métodos de notificación o alerta tales como:

- Mensajes en la consola: método en el que se suele codificar en función de su importancia.
- Mensajes por correo electrónico: mediante el cual se envía contenido el nivel de prioridad y el nombre del evento ocurrido.
- Mensajes a móviles: método utilizado cuando el evento necesita intervención inmediata del administrador de red.

2.2.3 Red y sus servicios.

La finalidad de una red es que los usurarios de los sistemas informáticos de una organización puedan hacer un mejor uso de los mismos mejorando de este modo el rendimiento global de la organización, así las organizaciones obtienen

una serie de ventajas del uso de las redes en sus entornos de trabajo, como pueden ser:

- Mayor facilidad de comunicación.
- Mejora de la competitividad.
- Mejora de la dinámica de grupo.
- Reducción del presupuesto para proceso de datos.
- Reducción de los costos de proceso por usuario.
- Mejoras en la administración de los programas.
- Mejoras en la integridad de los datos.
- Mejora en los tiempos de respuesta.
- Flexibilidad en el proceso de datos.
- Mayor variedad de programas.
- Mayor facilidad de uso.
- Mejor seguridad.

Para que todo esto sea posible, la red debe prestar una serie de servicios a sus usuarios, como son:

- Acceso.
- Ficheros.
- Impresión.
- Correo.
- Información.

Para la prestación de los servicios de red se requiere que existan sistemas en la red con capacidad para actuar como servidores.

Los servidores y servicios de red se basan en los sistemas operativos de red. Un sistema operativo de red es un conjunto de programas que permiten y controlan el uso de dispositivos de red por múltiples usuarios.

Estos programas interceptan las peticiones de servicio de los usuarios y las dirigen a los equipos servidores adecuados. Por ello, el sistema operativo de red, le permite a ésta ofrecer capacidades de multiproceso[20] y multiusuario[21]. Según la forma de interacción de los programas en la red, existen dos formas de arquitectura lógica:

[20] Es el uso de múltiples procesos concurrentes en un sistema en lugar de un único proceso en un instante determinado.

[21] característica de un sistema operativo o programa que permite proveer servicio y procesamiento a múltiples usuarios simultáneamente.

Cliente-servidor.

Este es un modelo de proceso en el que las tareas se reparten entre programas que se ejecutan en el servidor y otros en la estación de trabajo del usuario. En una red cualquier equipo puede ser el servidor o el cliente.

El cliente es la entidad que solicita la realización de una tarea, el servidor es quien la realiza en nombre del cliente. Este es el caso de aplicaciones de acceso a bases de datos, en las cuales las estaciones ejecutan las tareas del interfaz de usuario (pantallas de entrada de datos o consultas, listados, etc.) y el servidor realiza las actualizaciones y recuperaciones de datos en la base. En este tipo de redes, las estaciones no se comunican entre sí. Las ventajas de este modelo incluyen:

- Incremento en la productividad.
- Control o reducción de costos al compartir recursos.
- Facilidad de administración, al concentrarse el trabajo en los servidores.
- Facilidad de adaptación.

2.2.4 Pyme

Las Pequeñas y Medianas Empresas (Pymes) constituyen más del 90% de las empresas en la mayoría de los países del mundo. Las Pymes son la fuerza impulsora de gran número de innovaciones y contribuyen al crecimiento de la

economía nacional mediante la creación de empleo, las inversiones y las exportaciones.

A pesar de la importancia que tienen las Pymes para la vida económica y de las posibilidades que ofrece el sistema de P.I.[22] Para el fomento de su competitividad, a menudo las Pymes no saben aprovechar debidamente ese sistema.

Las Pymes en El Salvador, al igual que en todos los países del mundo, emplean un buen porcentaje de la población económicamente activa, lo cual ha llevado a nivel internacional ha promover el aumento de la competitividad individual para aumentar la competitividad empresarial y la de cada país en su conjunto, y una de las maneras más eficientes de lograr esto es con la implantación de Sistemas de Calidad que permitan a las Pymes mejorar de forma integral y consistente aquellos productos y servicios que brindan, mediante la optimización de los recursos invertidos en procesos debidamente controlados y bajo una dirección visionaria, dinámica y comprometida con la calidad y su mantenimiento en el tiempo.

La importancia de las Pymes en la economía se basa en:

[22] propiedad intelectual

- Asegurar el mercado de trabajo mediante la descentralización de la mano de obra cumple un papel esencial en el correcto funcionamiento del mercado laboral.
- Tener efectos socioeconómicos importantes ya que permite la concentración de la renta y la capacidad productiva desde un número reducido de empresas hacia uno mayor.
- Reduce las relaciones sociales a términos personales más estrechos entre el empleador y el empleado favoreciendo la conexión laboral ya que, en general, sus orígenes son unidades familiares.
- Presenta mayor adaptabilidad tecnológica y menor costo de infraestructura.
- Obtiene economía de escala a través de la cooperación inter-empresaria, sin tener que reunir la inversión en una sola firma.

2.3 Diseño de la solución

En capítulos anteriores se determinó las deficiencias con las cuales cuenta la compañía cuenta en la actualidad, previo a cualquier propuesta de solución a implementar se realizó un análisis exhaustivo para tener una mejor perspectiva de las topologías físicas y lógicas con las cuales se cuenta actualmente.

En esta parte se plantea como encajaran las tecnologías propuestas en la red local y como resolverá las deficiencias existentes

2.3.1 Topologías

Topología[23] física

Muestra el esquema de interconexión de cada uno de los componentes de la infraestructura de la red, a través de los centros de distribución y el cableado estructurado, y el cuarto principal a donde están los equipos centrales de infraestructura y fácilmente puede ser integrado el equipo de administración de seguridad como intermediario entre el segmento de LAN interna e Internet.

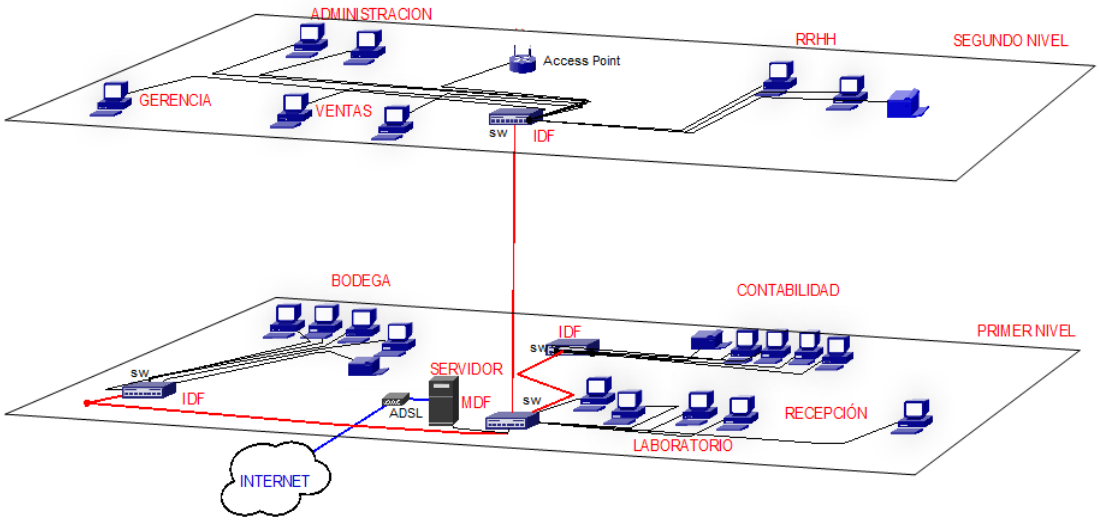

Figura 2.7 Diagrama de topología física de Droguería Universal S.A de C.V

[23] Cadena de comunicación usada por los nodos que conforman una red para comunicarse.

Topología lógica

En general describe como está constituida la red a nivel de infraestructura lógica, la topología es en estrella extendida y el direccionamiento, el cual es una red de clase C con mascara por defecto: ID de RED 192.168.1.0 MASCARA 255.255.255.0.

Los equipos cuentan con direccionamiento estático y pertenecen a un dominio de directorio Activo de Microsoft (Active Directory) en cual tiene como sufijo DNS, droguería local.

El servidor principal tiene como sistema operativo Windows Server 2008 R2, el cual ejecuta el rol de ADSL[24], y tiene un sistema de control de inventarios de productos, y cuenta con una base de datos en el servidor.

Adicionalmente a esto se le suma el rol de enrutador hacia internet ya que el segmento de la red interna 192.168.1.0 /24 tiene como Gateway una interfaz de red del servidor con direccionamiento 192.168.1.11 /24.

El servidor se encarga de hacer la traducción de direcciones internas hacia la interfaz del segmento WAN que está conectada con el modem ADSL, el proveedor de servicios es CTE Claro direccionamiento 192.168.2.1 /24.

[24] permite conectar al mismo uno o varios equipos o incluso una o varias redes de área local.

La red no cuenta con un mecanismo de seguridad que permita mantener un nivel de seguridad adecuado para la red y los servicios.

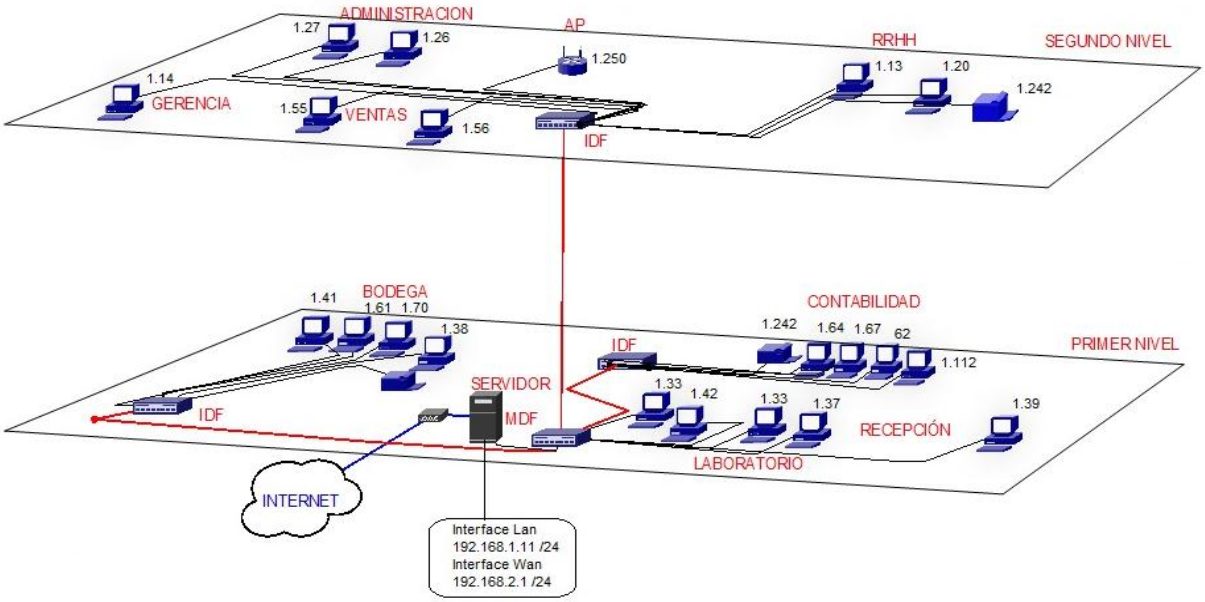

Figura 2.8 Diagrama de topología lógica de Droguería Universal S.A de C.V

2.3.2 Herramientas sujetas a evaluación.

A continuación se listan algunas herramientas posibles para la propuesta de solución, tomando en cuenta que las pequeñas y medianas empresas pueden no contar con un presupuesto adecuado para adquirir herramientas de seguridad de nivel Empresarial por ser de un alto costo.

Instalando alguna herramienta de seguridad Open Source, las pymes pueden mejorar la fiabilidad y seguridad de sus redes informáticas y reducir las inversiones TIC[25] y costes operativos.

Figura 2.9 Logotipo de herramienta Zentyal

Zentyal (anteriormente conocido como eBox Platform) es un servidor de red unificada de código abierto (o una plataforma de red unificada) para las Pymes. Zentyal puede actuar gestionando la infraestructura de red, como puerta de enlace a Internet (Gateway), gestionando las amenazas de seguridad (UTM), como servidor de oficina, como servidor de comunicaciones unificadas o una combinación de estas. Además, Zentyal incluye un marco de desarrollo (un framework[26]) para facilitar el desarrollo de nuevos servicios basados en Unix.

El código fuente del proyecto está disponible bajo los términos de la licencia pública general de GNU, así como bajo varias licencias privativas. La empresa española eBox Technologies S.L. es el propietario y patrocinador de Zentyal y posee el copyright del código fuente.

[25] Tecnologías de la información y la comunicación.

[26] infraestructura digital, es una estructura conceptual y tecnológica de soporte definido

Zentyal (eBox Platform) empezó como un proyecto colaborativo entre dos empresas y fue publicado como un proyecto de código abierto por primera vez en 2005. El 16 de noviembre de 2006 Zentyal (eBox Platform) fue oficialmente aprobado como proyecto NEOTEC[27], recibiendo fondos públicos del CDTI[28] para completar el desarrollo de la versión 1.0. Zentyal (eBox Platform) fue incluido por primera vez en Ubuntu en 2007, en el Gutsy Gibbon Tribe 3(la tercera versión alfa de Ubuntu 7.10). La primera versión candidata a definitiva de Zentyal (eBox Platform 1.0), fue publicada en 2008.

Características

Zentyal 2.0 (publicado en septiembre 2010) dispone de las siguientes características:

- **Gestión de redes**
    - Cortafuegos y encaminamiento
        - Filtrado de tráfico
        - NAT y redirección de puertos
        - VLAN 802.1Q
        - Soporte para múltiples puertas de enlace PPPoE y DHCP

[27] Tiene como objetivo el apoyo a la creación y consolidación de nuevas empresas de base tecnológica en España.

[28] Organización pública española bajo el ministerio de industria, comercio y turismo.

        - Reglas para múltiples puertas de enlace, balanceo de carga y auto-adaptación ante la pérdida de conectividad
        - Moldeado de tráfico (soportando filtrado a nivel de aplicación)
        - Monitorización gráfico de tráfico
        - Sistema de detección de intrusos en la red
        - Cliente dinámico DNS
    - Infraestructura de red
        - Servidor DHCP
        - Servidor NTP
        - Servidor DNS
            - Actualizaciones dinámicos mediante DHCP
        - Servidor RADIUS
    - Soporte de redes privadas virtuales
        - Autoconfiguración de rutas dinámicas
    - Proxy HTTP
        - Caché
        - Autenticación de usuarios
        - Filtrado de contenido
        - Antivirus transparente
        - Delay pools

- Sistema de detección de intrusos
- Servidor de correo
  - Dominios virtuales
  - Quotas
  - Soporte para SIEVE
  - Recuperación de cuentas externas
  - POP3 e IMAP con SSL/TLS
  - Filtro de Spam y Antivirus
    - Listas blancas, negras y grises
  - Filtro transparente de POP3
  - Catch-all[29] account

- **Webmail**
- **Servidor web**
  - Dominios virtuales
- **Autoridad de Certificación**
- **Trabajo en grupo**
  - Gestión centralizada de usuarios y grupos
    - Soporte maestro/esclavo
    - Sincronización con un controlador de dominio Windows Active Directory

[29] Un buzón de correo de un dominio en el cual se recoge todo.

- Controlador Primario de Dominio (PDC) de Windows
  - Política de contraseña
  - Soporte para clientes de Windows 7
- Compartición de recursos
  - Servidor de archivos
    - Antivirus
    - Papelera
  - Servidor de impresión
- Groupware: Compartición de calendarios, agendas, web mail, wiki, etc.
- Servidor VozIP
  - Buzón de voz
  - Salas de conferencias
  - Llamadas a través de un proveedor externo
  - Transferencia de llamadas
  - Aparcamiento de llamadas
  - Música de espera
  - Colas
  - Registros

- **Servidor Jabber/XMMP**
  - Salas de conferencias

- **Rincón del Usuario de Zentyal**
- **Informes y monitorización**
    - Dashboard[30] para centralizar la información de los servicios
    - Monitorización del CPU, carga, espacio del disco, temperatura, memoria
    - Estado del RAID por software e información del uso de disco duro
    - Informes completos y resumidos de sistemas
    - Notificación de eventos vía correo, subscripción de noticias (RSS) o Jabber/XMPP
- **Actualizaciones de software**
- **Copias de seguridad (backup de configuración y remoto de datos)**

Figura 2.10 Logotipo de herramienta ClearOS

ClearOS (Antes nombrado ClarkConnect) es una distribución de Linux , basado en CentOS y Red Hat Enterprise Linux , diseñado para uso en pequeñas y medianas empresas como una puerta de acceso de red y servidor de red con

[30] Barra de tareas.

una interfaz de administración basada en web Se está diseñado para ser una alternativa a Windows Small Business Server .

El software fue construido por ClearFoundation, y el soporte se puede adquirir en ClearCenter. A partir de la versión ClearOS 6.1, la distribución será un sistema operativo completo para servidores y estaciones construidas a partir de los paquetes fuente para Red Hat Enterprise Linux.

Características

ClearOS Enterprise Directory Features

- Integrated LDAP for User and Group Management
- User Security Certificate Manager

ClearOS Enterprise Network Features

- Multi-WAN
- VPN - PPTP, IPsec, OpenVPN
- DMZ and 1-to-1 NAT
- Stateful Firewall
- Local DHCP and DNS Servers

ClearOS Enterprise Gateway Features

- Antimalware - Antivirus, Antiphishing, Antispyware

- Antispam
- Bandwidth[31] Management
- Intrusion Protection, Intrusion Prevention, Intrusion Detection
- Protocol Filtering including Peer-to-Peer[32] Detection
- Content Filter
- Web Proxy
- Access Control

ClearOS Enterprise Network Features

- Windows Networking with PDC Support
- File and Print Services
- Flexshares
- Groupware with Outlook Connector
- Mail Server - POP, IMAP, SMTP, Webmail, Retrieval
- Mail Filtering - Antispam, Antimalware, Greylisting, Quarantine
- Mail Archiving
- Database with MySQL
- Web Server with PHP Support

[31] Ancho de banda

[32] Es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos

Figura 2.11 Logotipo de herramienta IPCop

IPCop es una distribución Linux que implementa un cortafuego y proporciona una simple interfaz web de administración basándose en una computadora personal.

Originalmente nació como una extensión (fork) de la distribución SmoothWall cuyo desarrollo había estado congelado bastante tiempo. Tiene como objetivos ser un cortafuego sencillo, con pocos requerimientos hardware orientado a usuarios domésticos o a pequeñas empresas, administrado a través de una interfaz web, con funcionalidades básicas y avanzadas, yendo (a manera de ejemplo) desde el simple filtrado de paquetes hasta la asignación de ancho de banda fijo a cada puesto de trabajo o la configuración de redes virtuales VPN. Se actualiza desde la Interfaz Web de manera muy sencilla, incluyendo actualizaciones del Kernel[33].

[33] Núcleo de un sistema operativo.

Algunas de las características impresionantes IPCops base de instalación incluyen: seguro https Web GUI de administración, servidor DHCP, proxy (Squid), DNS proxy DNS, dinámicos, en el Servidor, Traffic Shaping, Tráfico / Sistemas / Firewall / IDS gráfica, detección de intrusiones (Snort), dispositivo de ISDN / ADSL apoyo y la funcionalidad de VPN (IPSec / PPTP).

Como si estas características de base no eran lo suficientemente asombrosa uno hay decenas de complementos que además puede ampliar la funcionalidad de su IPCop desde la Web Filtering para escaneo anti-virus

CAPITULO III
Propuesta de la solución

3.1 Propuesta de solución

La realización del estudio de los recursos informáticos en la empresa Droguería Universal S.A de C.V, demuestra que hay deficiencias en varias áreas, para ayudar a solventar esos problemas se le hace una propuesta de solución innovadora a bajo costo.

Utilizando un sistema operativo de código abierto que permita utilizarlo como: Antivirus, filtro de contenidos, proxy web, firewall, detector de intrusos entre otros recursos de administración de red.

A fin de brindar una alternativa a la problemática planteada, se propone utilizar ClearOS, que permite utilizarlo como firewall y filtro de contenidos en la red ya existente.

El escenario de prueba para la implementación se realiza en un entorno virtual[34], que permite observar la seguridad y administración en los recursos de red.

El ClearOs se instala en un ordenador en el cuarto de servidores como una puerta de acceso de red con una interfaz de administración basada en web.

Esta propuesta permite seguridad, escalabilidad y mejor administración de los recursos de red en el departamento TI, como también a los usuarios mejor control en la entrada y salida de información.

3.1.1 Planteamiento del proyecto

Cada una de las fases planteadas en este capítulo permite conocer paso a paso el desarrollo del proyecto.

Se realiza mediante cuatro fases que darán por cumplido y finalizado la propuesta de solución unificada, las cuales son:

Fase 1: Investigación.

[34]Es un espacio de enseñanza, aprendizaje y de comunicación.

Como primer punto se debe profundizar en las necesidades en el área de informática de la empresa.

Para ello se realizan visitas constantes a la institución, que permitan recolectar la información necesaria para realizar una propuesta de solución, que ayude a la administración de los recursos tecnológicos.

Por lo que se debe conocer la topología de red utilizada[35], el direccionamiento de red implementado, los equipos con que cuenta la empresa, y el software.

Se reúne la información necesaria mediante un diagnostico de red, basados en las necesidades de seguridad y administración, con los datos adquiridos se puede elegir que alternativa ofrecer para integrarla a la compañía.

Fase 2: Diseño

Con los requerimientos obtenidos de la fase anterior se busca diseñar una alternativa de solución que permita mejorar la seguridad y la administración de la red.

El diseño contempla la selección de la tecnología de código abierto compatible a la infraestructura de red actual, la selección del direccionamiento IP para el servidor y políticas de seguridad de acceso para los usuarios.

[35] Información brindada por el administrador de TI.

Se realiza el diseño físico y el diseño lógico de la propuesta de solución unificada utilizando Open Source.

En el diseño físico se coloca el ClearOs en un área estratégica para que el administrador[36] de TI tenga acceso a él, y ese lugar es en el cuarto de servidores, una vez determinada la ubicación del sistema operativo de código abierto se dan las indicaciones a la persona encargada de administrarlo.

En el diseñó lógico se configura ClearOS como puerta de acceso y servidor de red con una interfaz de administración basada en web.

Ya que es muy fácil de administrar y por su amigable entorno gráfico, en el que es posible configurar los elementos necesarios de acuerdo a las necesidades.

Fase 3: Instalación y configuración

Según el diseño físico se instala el ClearOS en un ordenador robusto, con el hardware necesario para su buena administración y funcionamiento.

Las siguientes son las directrices del hardware adecuado para el sistema.

En la Configuración de dicho software se implementaran las herramientas:

- Firewall

[36]La persona encargada de las redes informáticas.

- DMZ
- Antivirus
- Proxy web
- QoS
- DHCP
- Filtro de contenido
- IPS
- IDS

Teniendo en cuenta que hay mas servicios que se pueden configurar en el software.

Fase 4: Pruebas

Para dar por finalizado la propuesta de solución unificada con Open Source, se realiza una serie de pruebas que permitirán diagnosticar alguna falla y corregirla en caso de encontrase alguna, las pruebas consisten en verificar el buen funcionamiento del prototipo, analizando los servicios configurados.

Pruebas a realizar.

- Conectividad de IP.
- Conectividad entre servidor y clientes.
- Establecimiento de políticas de seguridad.
- Verificación de seguridad en la información.

3.1.2 Cronograma de actividades

Tabla 3.1 Cronograma de actividades # 1

# De actividad	Actividad	Duración en horas	Calendario
Actividad # 1	Investigación	08:00 – 11:00	16/04/12 - 20/04/12
Actividad # 2	Diseño	08:00 – 17:00	26/04/12 - 27/04/12
Actividad # 3	Instalación y configuración	08:00 – 12:00	30/04/12 - 09/05/12
Actividad # 4	Pruebas	08:00 – 12:00	10/05/12 - 11/05/12

Tabla 3.2 cronograma de actividades #2

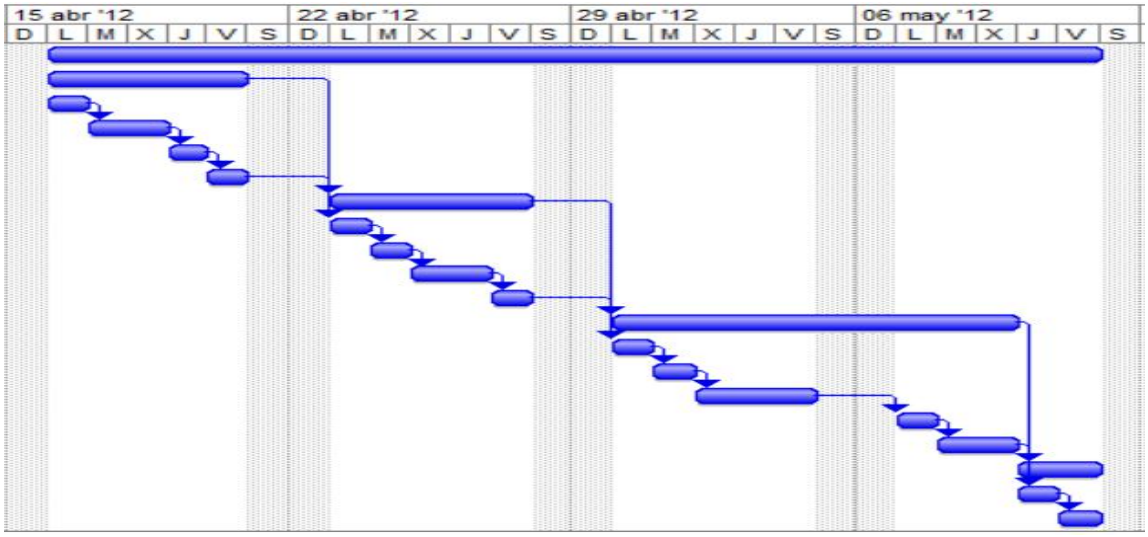

Tabla 3.3 cronograma de actividades #2

Id	Nombre de tarea	Duración	Comienzo	Fin
1	Proyecto	20 días	lun 16/04/12	vie 11/05/12
2	Investigacion	5 días	lun 16/04/12	vie 20/04/12
3	Runion de grupo	1 día	lun 16/04/12	lun 16/04/12
4	Recoleccion de informacion	2 días	mar 17/04/12	mié 18/04/12
5	Revision de informacion	1 día	jue 19/04/12	jue 19/04/12
6	Informe final de la face de diagnostico	1 día	vie 20/04/12	vie 20/04/12
7	Diseño	5 días	lun 23/04/12	vie 27/04/12
8	Evaluar la informacion	1 día	lun 23/04/12	lun 23/04/12
9	Eleccion del modelo de red	1 día	mar 24/04/12	mar 24/04/12
10	Diseño del prototipo	2 días	mié 25/04/12	jue 26/04/12
11	Eleccion del software	1 día	vie 27/04/12	vie 27/04/12
12	Instalacion y configuracion	8 días	lun 30/04/12	mié 09/05/12
13	Ubicación del servidor	1 día	lun 30/04/12	lun 30/04/12
14	Instalacion y configuracion del ClearOS	1 día	mar 01/05/12	mar 01/05/12
15	Configuracion de los servicios ClearOS	3 días	mié 02/05/12	vie 04/05/12
16	Configuracion de políticas de seguridad	1 día	lun 07/05/12	lun 07/05/12
17	Configuracion de equipos de red	2 días	mar 08/05/12	mié 09/05/12
18	Pruebas	2 días	jue 10/05/12	vie 11/05/12
19	Conectividad	1 día	jue 10/05/12	jue 10/05/12
20	Establecimiento de políticas	1 día	vie 11/05/12	vie 11/05/12

3.1.3 Tecnologías y recursos seleccionados

Figura 3.1 Logotipo de ClearOS

Realizando el estudio sobre la herramienta de seguridad que más se adecue se llegó a la conclusión de proponer ClearOS Comunity que es una distribución de Linux, de código abierto basado en CentOS y Red Hat Enterprise Linux

Diseñado para uso en pequeñas y medianas empresas como puerta de enlace de acceso de red y servidor de red con administración web.

Está diseñado para proveer servicios básicos de red y seguridad, el software fue construido por ClearFoundation.

La distribución provee un alto grado de facilidad de implementación y administración de políticas de seguridad, demás fue galardonado con ciertos reconocimientos, y por su nivel de aceptación y reconocimientos.

Awards and recognition

- Agosto 2009: ClearCenter gano el 'Best New Product' en CompTIA Breakaway.
- Agosto 2010: ClearCenter repite al ganar el 'Best New Product' en CompTIA Breakaway

Características de la versión 5.2

ClearOS Enterprise Directory Features

- Integrated LDAP for User and Group Management
- User Security Certificate Manager

ClearOS Enterprise Network Features

- Multi-WAN
- VPN - PPTP, IPsec, OpenVPN
- DMZ and 1-to-1 NAT
- Stateful Firewall
- Local DHCP and DNS Servers

ClearOS Enterprise Gateway Features

- Antimalware - Antivirus, Antiphishing, Antispyware
- Antispam
- Bandwidth Management

- Intrusion Protection, Intrusion Prevention, Intrusion Detection
- Protocol Filtering including Peer-to-Peer Detection
- Content Filter
- Web Proxy
- Access Control

ClearOS Enterprise Network Features

- Windows Networking with PDC Support
- File and PrintServices
- Flexshares
- Groupware with Outlook Connector
- Mail Server - POP, IMAP, SMTP, Webmail, Retrieval
- Mail Filtering - Antispam, Antimalware, Greylisting, Quarantine
- Mail Archiving
- Database with MySQL
- Web Server with PHP Support

ClearOS soporta muchas tecnologías pero solo se pondrá énfasis en algunas, las cuales se adecuan a las necesidades corporativas y forman parte de los mecanismos de seguridad y algunos servicios básicos de red, dentro de los cuales podemos destacar:

Tabla 3.4 Tabla de servicios de ClearOS

ClearOS	
Network Features	• DMZ • Cortafuego de Stateful • Servidor de DHCP
Gateway Features	• Antimalware • Antivirus, • Antiphishing, • Antispyware • Administración de ancho de banda • IDS,IPS • Filtro de protocolos • Filtro de contenido • Control de acceso
Gestión de servidor	• Filtración del correo - Antispam, Antimalware, Greylisting, cuarentena

3.1.4 Diseño de la Topología

El diseño de la implementación del equipo de seguridad unificada se establecerá de una forma estratégica que garantice un buen funcionamiento del equipo basado en estándares y reglas ya establecidas para implementación de firewalls.

El esquema de implementación:

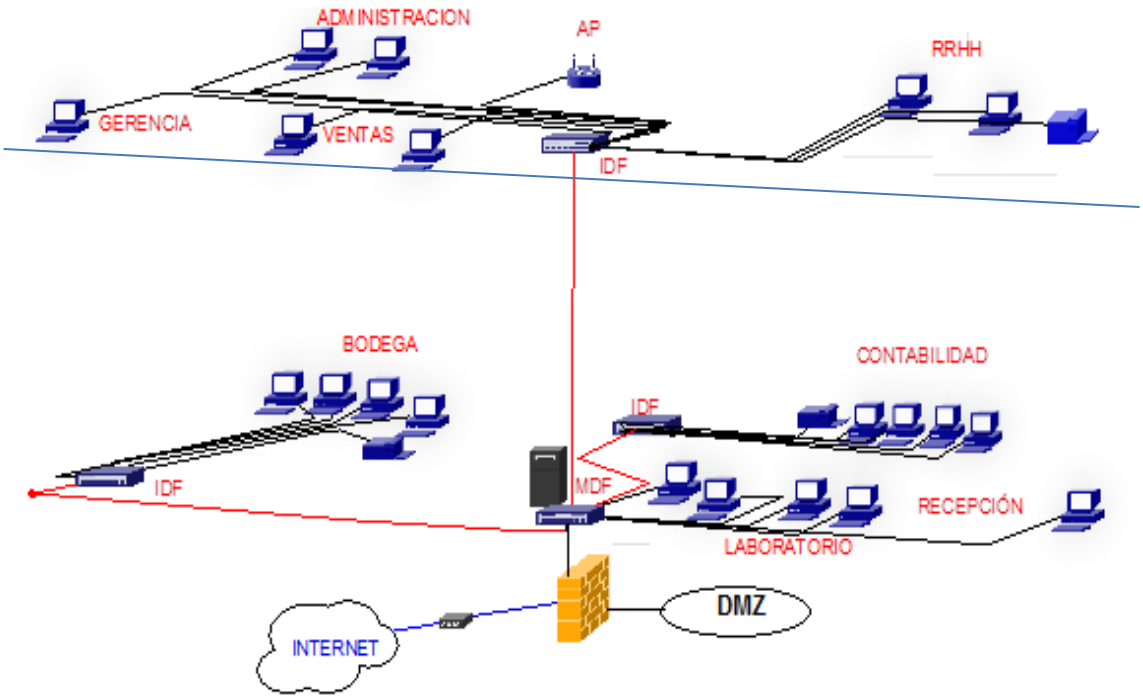

Figura 3.2 Esquema de implementación de ClearOS

Implementación de Gateway

La implementación del Gateway y cortafuego es indispensable ya que de está diseñada para bloquear o denegar el acceso a personas no autorizadas a la red corporativa y permitirá al mismo tiempo comunicaciones autorizadas.

El cortafuego será en base a software instalado en un equipo designado únicamente para este propósito.

El equipo cumple las características de las categorías de filtrado las cuales son las siguientes

Circuito a nivel de Gateway

Aplicara mecanismos de seguridad cuando una conexión TCP o UDP es establecida.

Una vez que la conexión se entable, los paquetes podrán fluir entre los anfitriones Permitiendo el establecimiento de una sesión que se origine desde una zona de mayor seguridad hacia una zona de menor seguridad.

Cortafuegos de capa de red o de filtrado de paquetes

La implementación de este permitirá controlar del tráfico que fluye a través del firewall estableciendo reglas de filtrado a nivel de capa de 3 y capa 4 del modelo de referencia OSI, estableciendo que redes puertos y protocolos son permisibles desde la red interna hacia afuera o viceversa garantizando que el tráfico no permitido sea bloqueado no importando origen ni destino.

Cortafuegos de capa de aplicación

Trabaja en el nivel de aplicación (capa 7 del modelo OSI), de manera que los filtrados se podrán adaptar a características propias de los protocolos de este nivel.

Esquema de Cortafuego

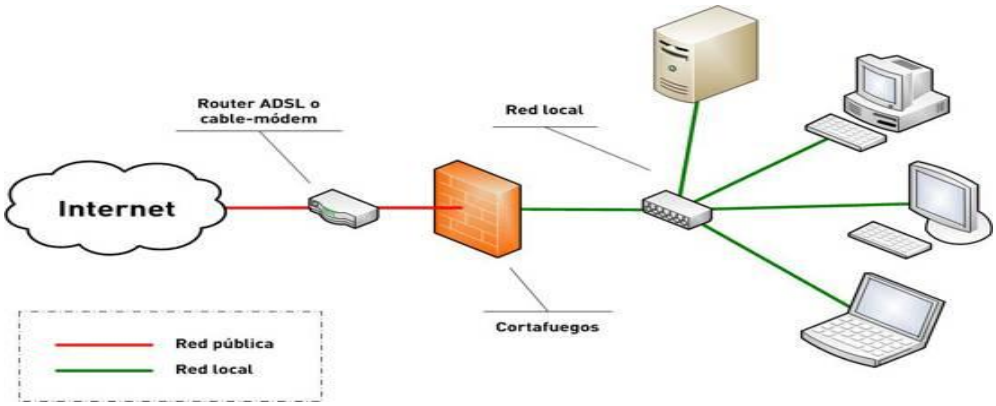

Figura 3.3 Esquema de cortafuego

Configuración de la DMZ

Se implementara una red perimetral La cual provee de capas de seguridad protegiendo servidores de acceso público no autorizado aislándolos en una ubicación llamada zona Desmitarilizada, en la cual se publican los servicios mientras que también se protege a la red interna de accesos no autorizados desde el exterior en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada.Donde cada red se conecta a un puerto distinto de éste. Esta configuración se llama cortafuegos en trípode (three-legged firewall).

Aunque en la actualidad la compañía no cuenta con servicios que se estén publicando hacia el exterior se prevé a futuro desarrollo empresarial que se tenga y se incrementara las necesidades de servicios públicos por lo cual se dejara la implementación adecuadas para las futuras necesidades.

Configuración perimetral de tres patas (three-legged)

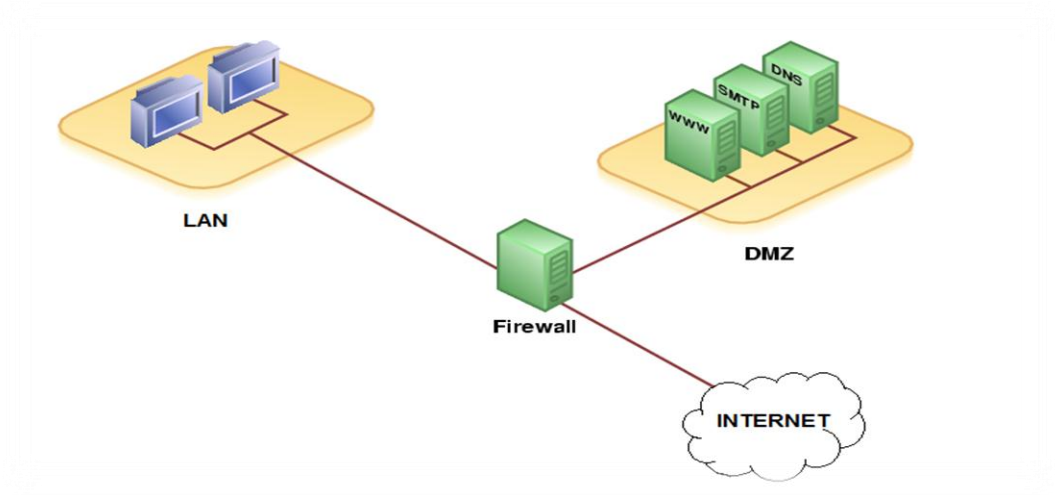

Figura 3.4 Esquema de tres patas

Configuración del filtrado de contenido.

El filtrado de contenido web es otra característica la cual se implementara para evitar que los usuarios de la compañía tengan acceso a sitios web inapropiados o contenidos, o como una medida de seguridad preventiva para evitar virus y malware en los equipos, el filtro de contenido trabaja en conjunto con el servicio proxy el cual es intermediario entre la red interna e Internet y este evaluara si la solicitud es permitida o denegado de acuerdo a los perfiles de filtrado,el motor de filtro de contenido utiliza una variedad de métodos, incluyendo la concordancia de frases, filtro url, Listas Blancas y listas negras, adicionalmente

a esto ayudara a optimizar el tráfico, bloqueando cierto contenido que consuma mayor ancho de banda y dificulte la realización de las actividades laborales.

.El filtrado de contenidos también quedara configurado para filtrar el spam. Y este definirá si se acepta o rechaza el mensaje de correo electrónico

Filtro de Contenido

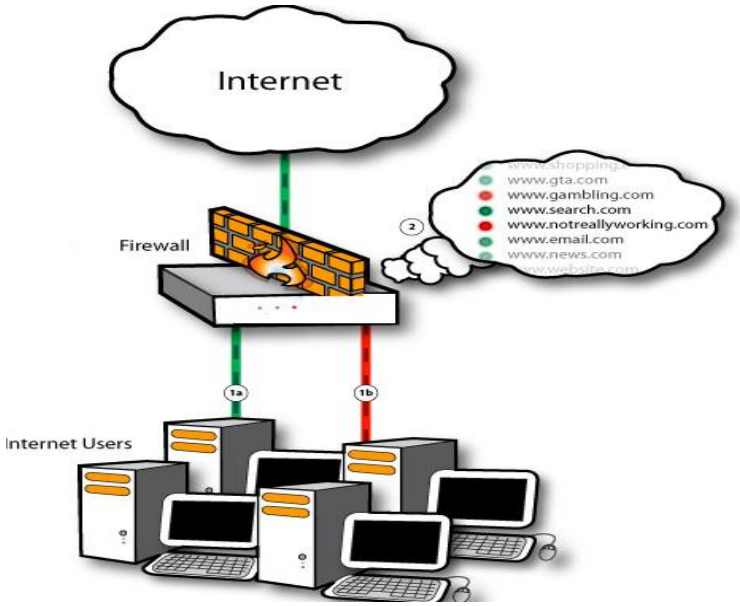

Figura 3.5 Esquema de filtro de contenido

Servidor Proxy Web, Proxy Cache

El servicio proxy realiza la tarea acceso a Internet en lugar de los ordenadores de la red local directamente, actúa como un punto intermedio entre un ordenador conectado a internet y el servidor al que está accediendo, cuando los

equipos naveguen a través de un proxy, en realidad no estarán accediendo directamente al servidor en internet, sino que realizan una solicitud sobre el proxy quien se conectará con el servidor enmascarando la dirección local de nuestro equipo y nos devolverá el resultado de la solicitud,el proxy cache permitirá mejorar la velocidad de acceso a Internet almacenado localmente las páginas más consultadas por los usuarios de la empresa, evitando las conexiones directas con los servidores remotos, así como la utilización innecesaria de ancho de banda.

Figura 3.6 Esquema de proxy

Implementación de IPS e IDS

Para poner en funcionamiento el sistema de detección de intrusos se optara por una solución de software que viene incluida con la distribución de Linux ClearOS, y esta, es SNORT herramienta de código abierto que detectara los

registros de firmas y las bases de datos con los posibles ataques, mantendrá un control exhaustivo para la prevención de intrusos bloqueando cualquier intento de intrusión a la red interna.

El IPS protegerá a la red proactivamente y el IDS lo protegerá reactivamente de esta forma se realizara un monitoreo continuo del tráfico que atraviesa nuestro firewall

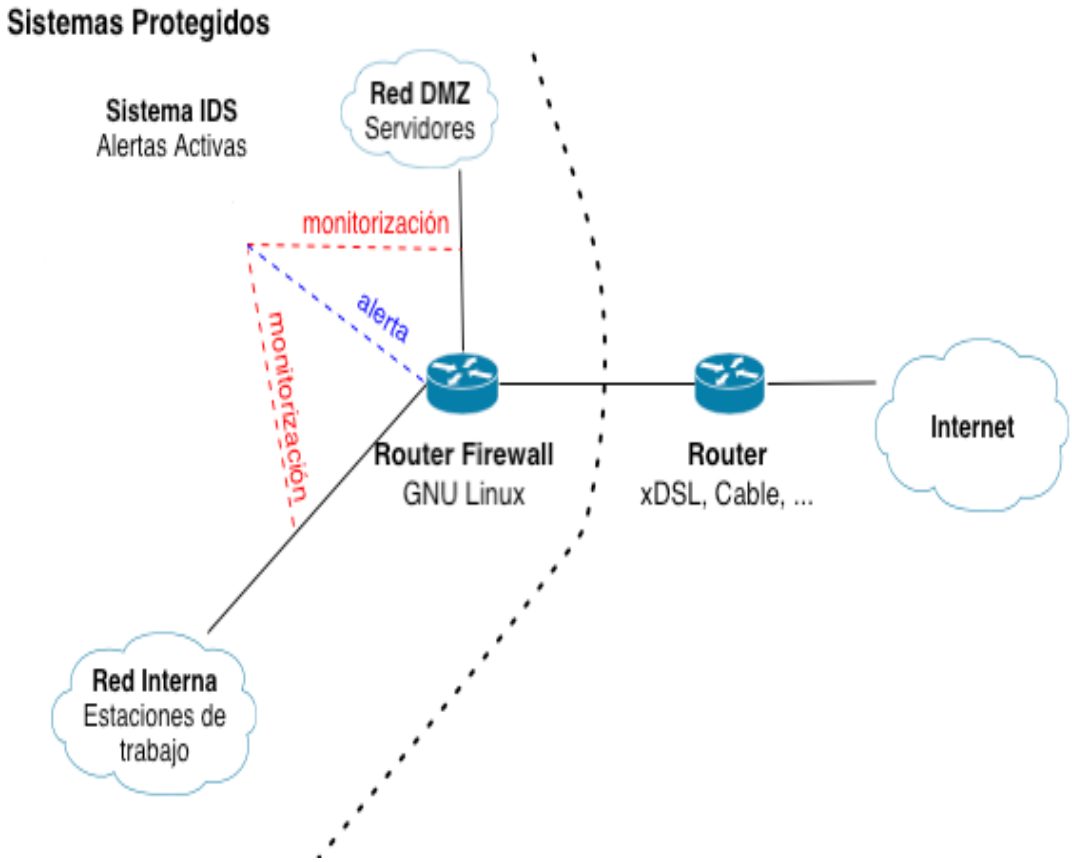

Figura 3.7 Esquema de IPS e IDS

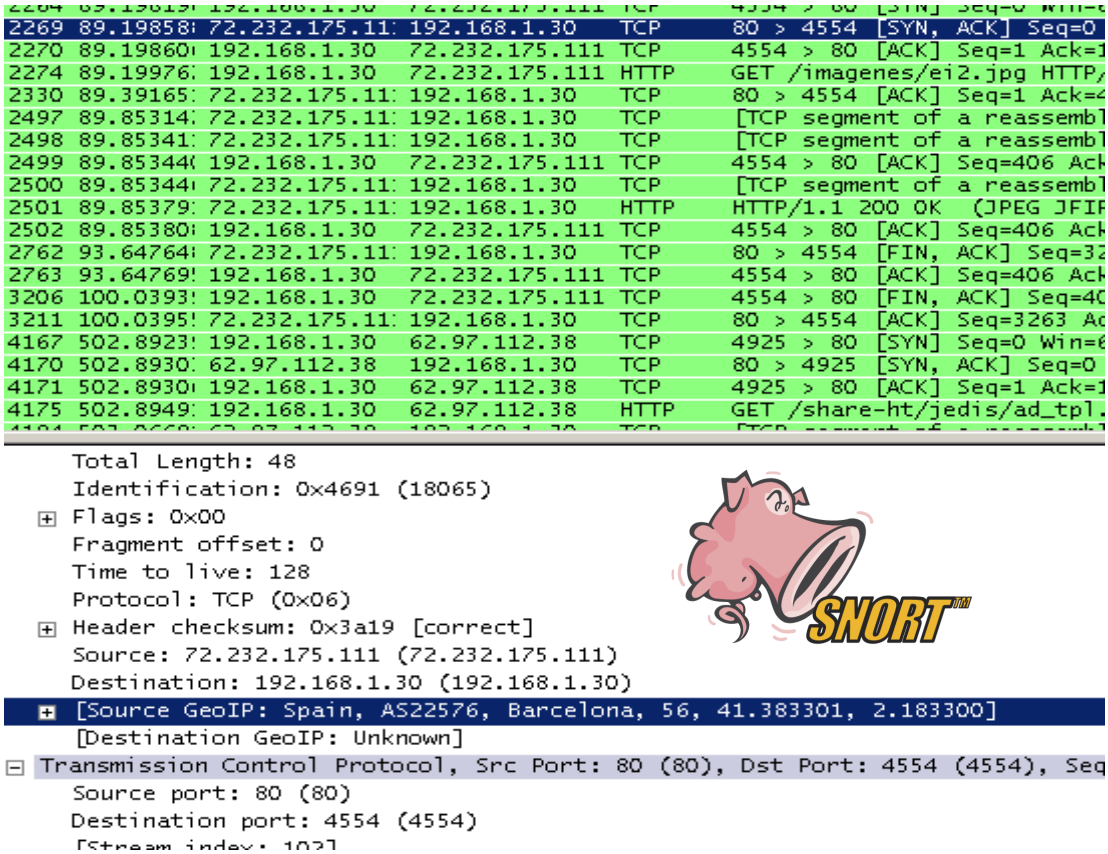

Figura 3.8 Imagen de Monitoreo con ClearOS

Antivirus

La función del módulo de Antivirus protegerá la red de Virus y troyanos, y el motor de búsqueda de código malicioso está integrado en varias características de ClearOS, dentro de las cuales destacan:

- Filtro de Contenido

- Antimalware de Correo
- Escaneo de Archivos

Antiphishing

La función de antiphishing protege a los usuarios de la suplantación de identidad.

Los mensajes fraudulentos que intentan obtener información confidencial, como números de tarjetas de crédito, contraseña se información personal o de la compañía.

Bandwidth Management

El administrador de ancho de banda se utilizara para dar forma o priorizar el tráfico de red entrante y saliente limitar el ancho de banda y priorizar según la dirección IP, rangos de direcciones IP y puertos.

Al habilitarlo el modulo se garantizara la transmisión de cierta cantidad de información en un tiempo dado (throughput) ya que es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.

Figura 3.9 Imagen de monitoreo de ancho de banda

Servidor DHCP

El servicio (DHCP) permitirá a los hosts de la red solicitar asignar direcciones IP. Este servicio eliminara la necesidad de configurar manualmente los equipos en la red evitando la tarea de establecer direcciones manualmente a los equipos y administrando las concesiones asignadas de forma centralizada.

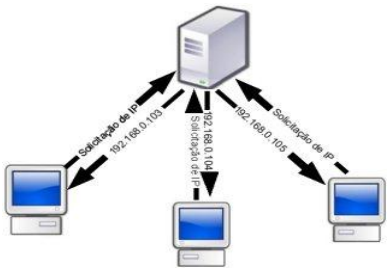

Figura 3.10 Esquema de DHCP

3.1.5 Implementación de la propuesta

La implementación de la propuesta fue desarrollada previamente en un escenario virtual para realizar pruebas de funcionamiento rendimiento y corrección de fallas para luego ser implementadas en producción en la red.

Implementación

Las siguientes son pautas para estimar el hardware adecuado para el sistema. Teniendo en cuenta que el hardware necesario depende de cómo utilizara el software.

Tabla 3.5 Pautas para estimar hardware

RAM y CPU	5 usuarios	5-10 usuarios	10-50 usuarios	50-200 usuarios
Procesador / CPU	500 MHz	De 1 GHz	2 GHz	3 GHz.
Memoria / RAM	512 MB	1 GB	1,5 GB	2 GB
Disco Duro	La instalación y los log requieren 1 GB adicional de espacio			
RAID	Recomendado para sistemas de misión crítica			

En el servidor es que se instalo la propuesta estaba dañado y la empresa lo mando a reparar para reutilizarlo para la implementación, solo tenia dañada una fuente.

Características de servidor para implementación

Características de Servidor IBM XSeries 206	
Factor Forma	**Torre**
Procesador	**Intel Pentium 4 3.00GHz**
Cache interna L2	**2MB**
Memoria RAM	**2GB**
Discos instalados	**3x 73.40GB HotSwap SAS**
Capacidad máx. de almacenamiento	**1 TB**
Fuente	**400W**

1. instalación del sistema

Al iniciar la instalación, aparece un asistente de instalación en el cual nos guiara para realizar la configuración básica que se requieren para instalar ClearOS.

Al iniciar con el CD de instalación nos mostrara la siguiente ventana, presionamos **Enter** para iniciar el asistente de instalación

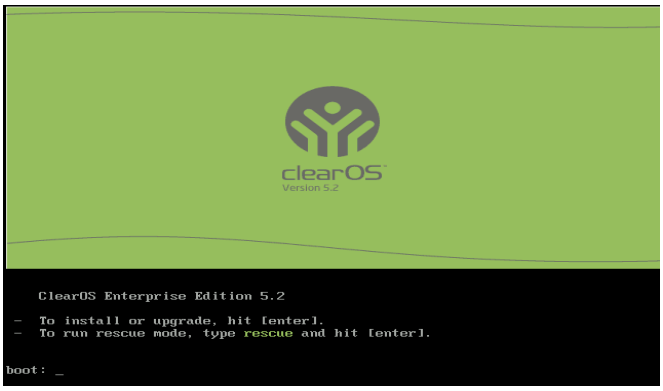

Figura 3.11 Imagen de instalacion de ClearOS

2. El asistente solicita el lenguaje a utilizar durante la instalación.

Figura 3.12 Selección de idioma

3. Seleccionamos tipo de teclado a utilizar

Figura 3.13 selección de teclado

4. Seleccionamos la media de instalación (**Local CDROM)**

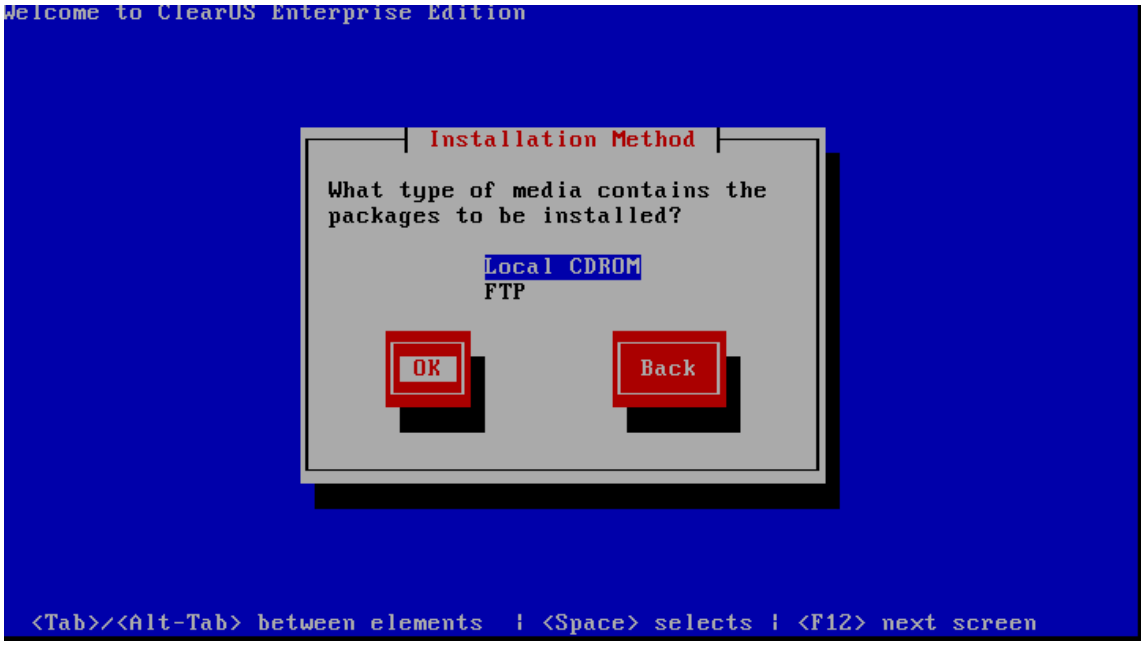

Figura 3.14 selección de medio de instalación

5. Si está instalando ClearOS por primera vez, deje **Install** seleccionada y pulse Aceptar

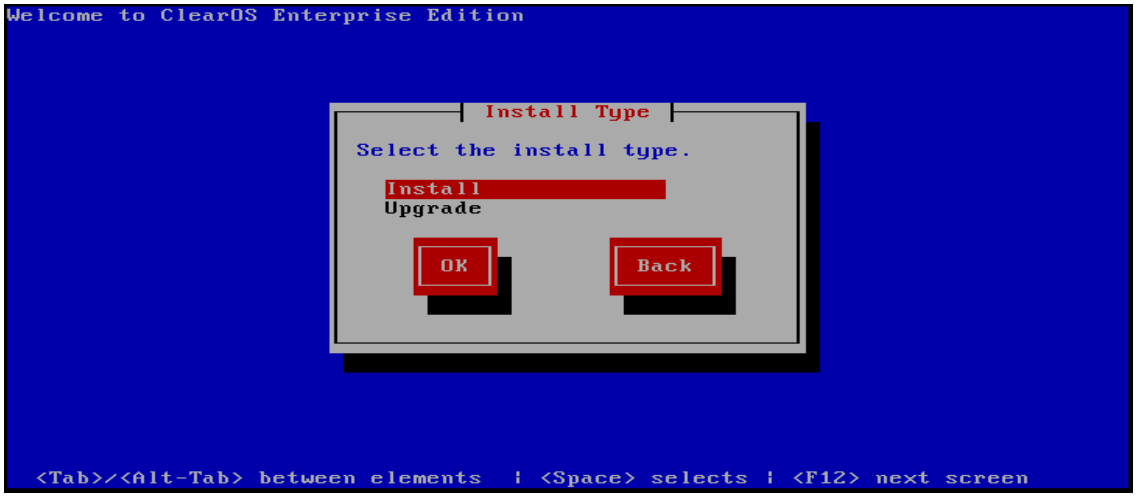

Figura 3.15 selección de tipo de instalación

6. En el proceso de instalación se eliminarán todos los datos conectados al servidor (incluyendo USB y Firewire). Para continuar con la instalación digitamos **ClearOS**, las mayúsculas son importantes

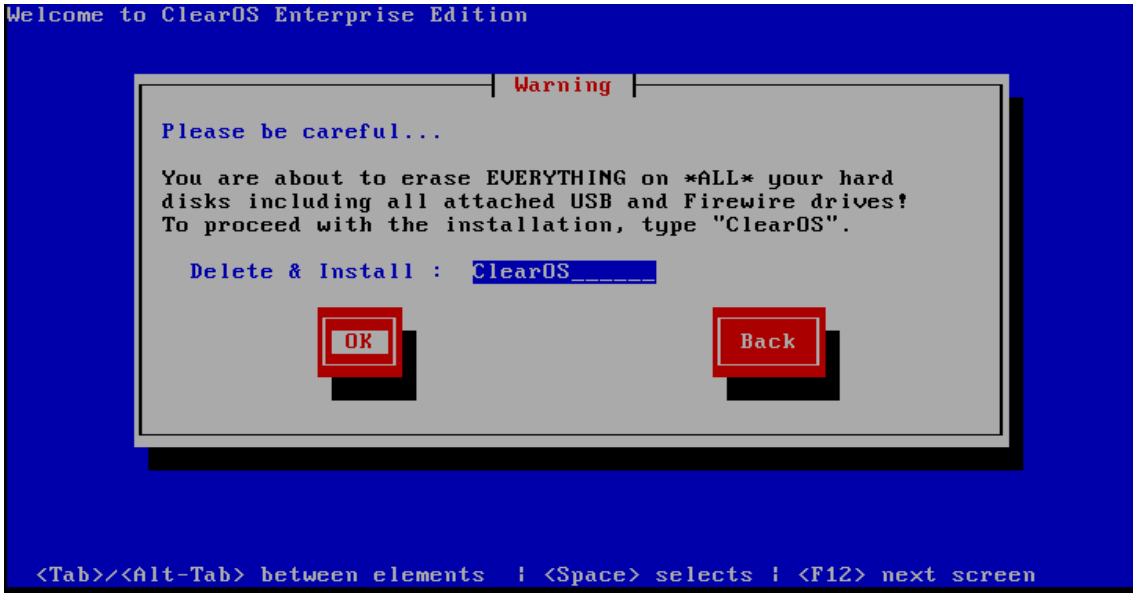

Figura 3.16 verificación de instalación

7. ClearOS soporta servidor modo Gateway y servidor modo Standalone.

7.1. **Modo Standalone:** Se utiliza para crear un servidor en una red de área local (detrás de un cortafuego existente). Sólo una tarjeta de red.

7.2. **Modo Gateway:** permite que su sistema sea utilizado como un Firewall, Gateway y servidor de su red local. Por lo menos dos tarjetas de red son necesarias

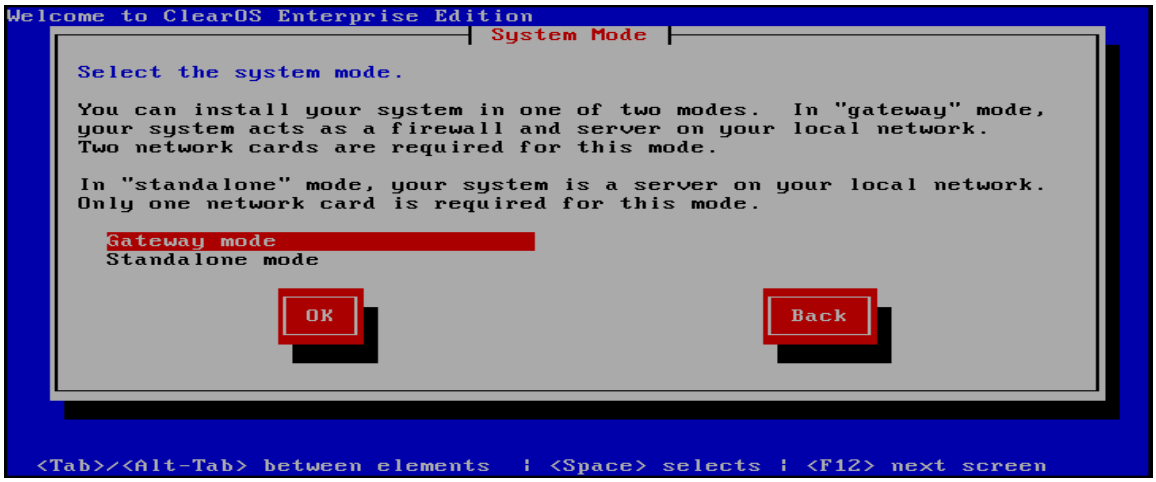

Figura 3.17 selección de modo de instalación

8. Seleccionamos tipo de conexión a Internet, es este caso será **Ethernet**

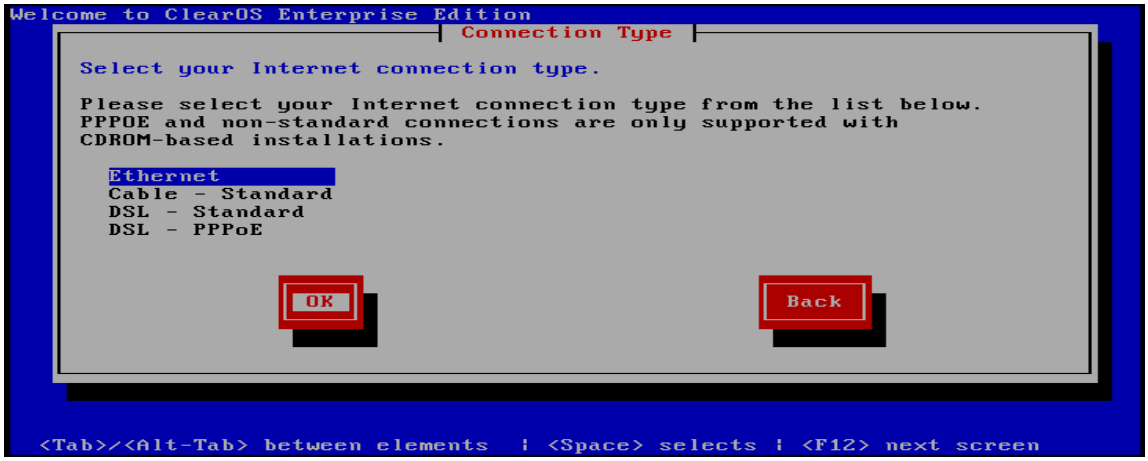

Figura 3.18 selección de conexión.

9. Especificamos que la configuración de la interfaz del segmento de Red WAN de se hará por DHCP

Figura 3.19 especificación de interfaz con DHCP

10. Dejamos en blanco el campo de Nameserver ip

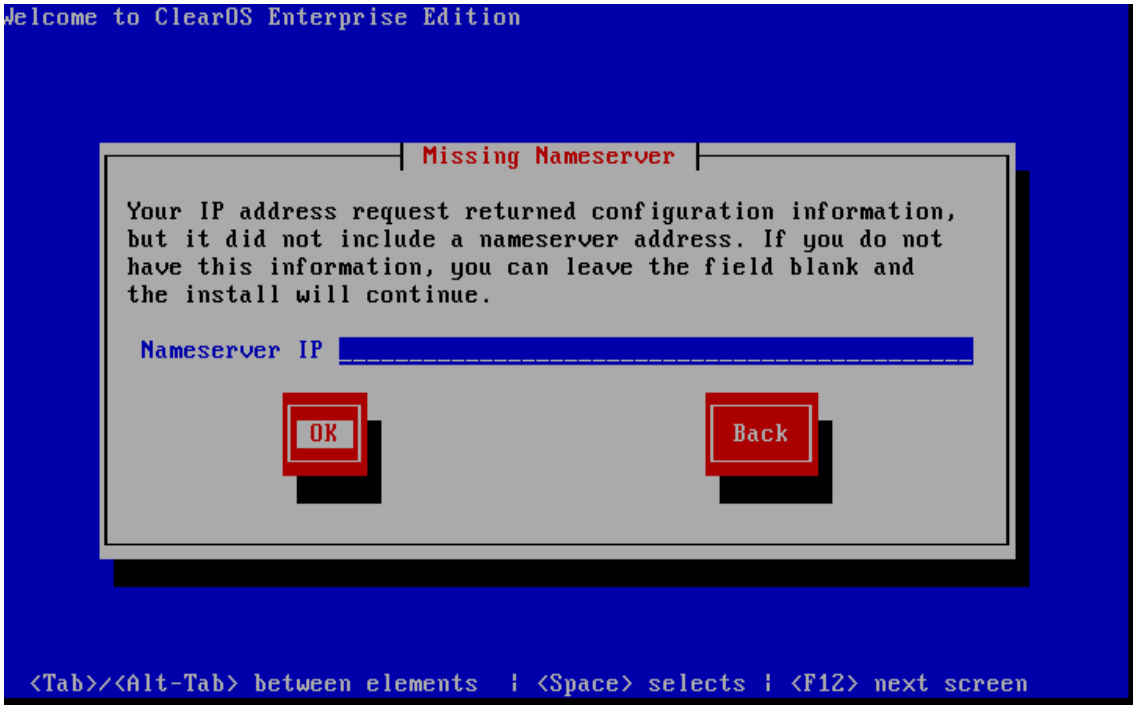

Figura 3.20 nombre del servidor

11. En esta parte de la instalación asignamos la IP que tendrá el servidor dentro de la red LAN, para este caso asignaremos la IP: 192.168.1.254 con mascara 255.255.255.0

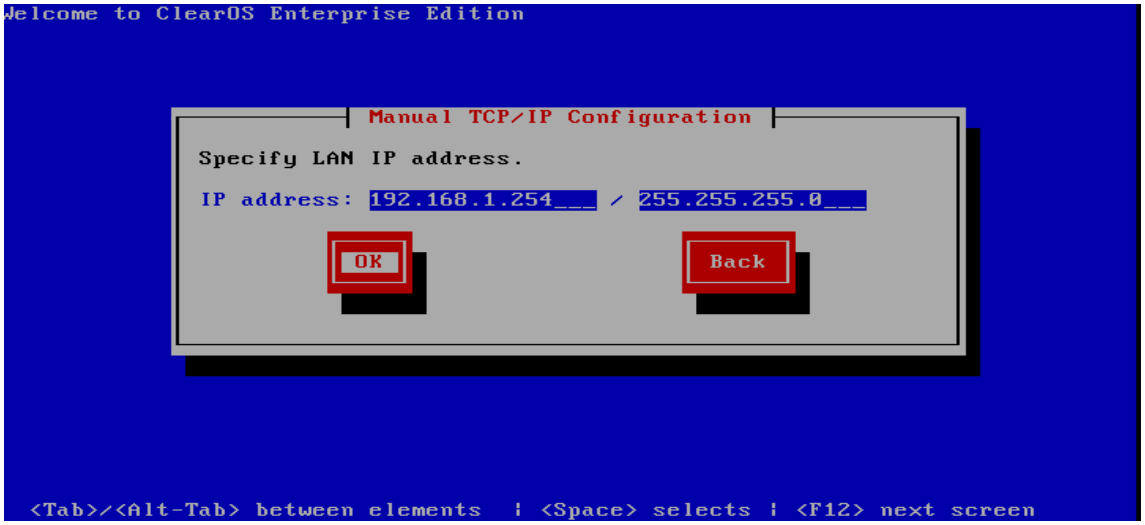

Figura 3.21 asignación de IP

12. Configuramos la contraseña que tendrá el usuario **Root** que es el administrador de Sistema,

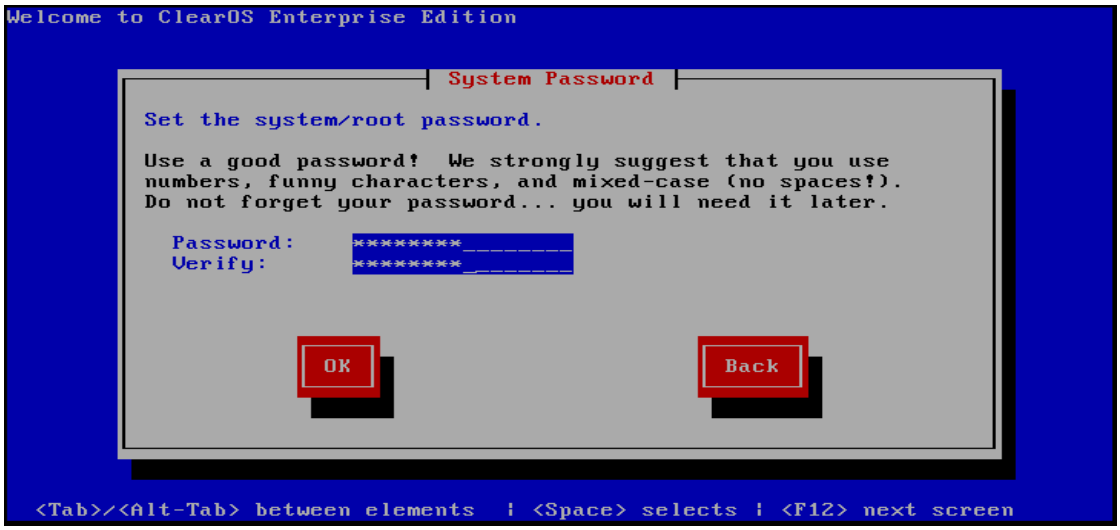

Figura 3.22 asignación de contraseña

13. El Asistente solicita el esquema de particiones que utilizaremos, seleccionamos: **Use default**

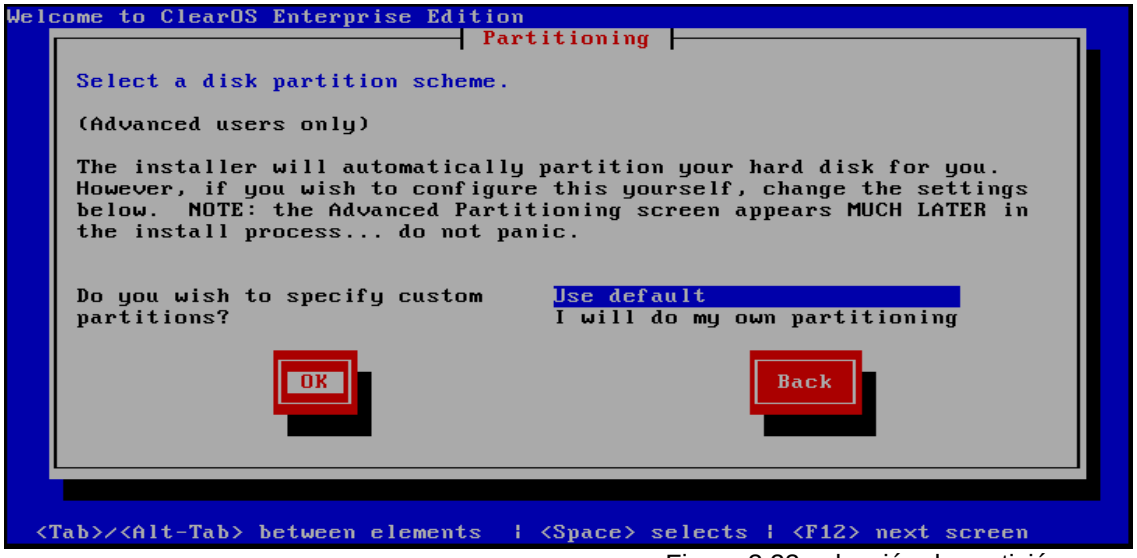

Figura 3.23 selección de partición

14. Posteriormente seleccionaremos los módulos que administraremos desde el servidor

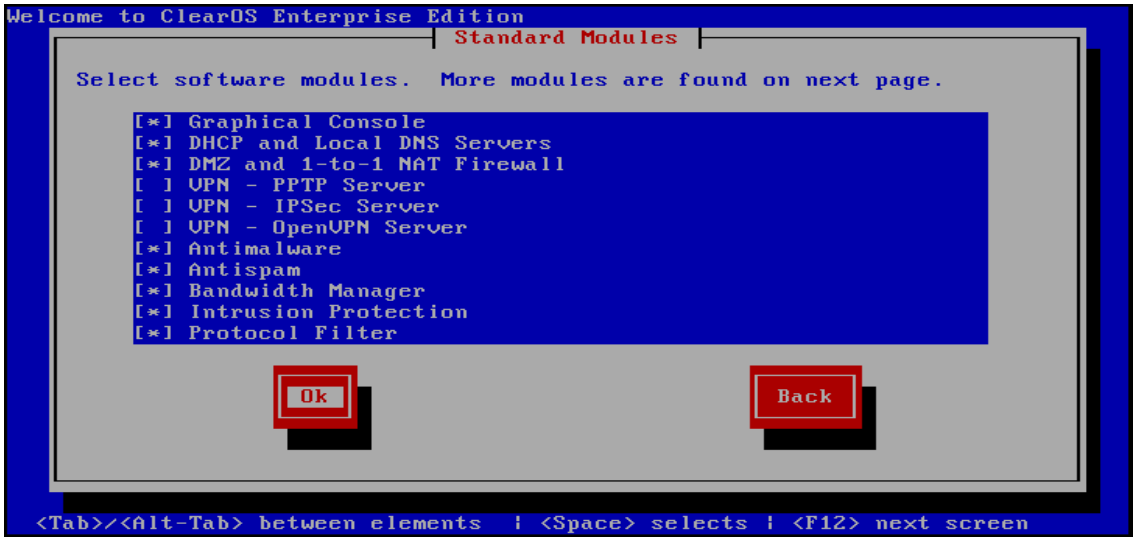

Figura 3.24 selección de módulos

.

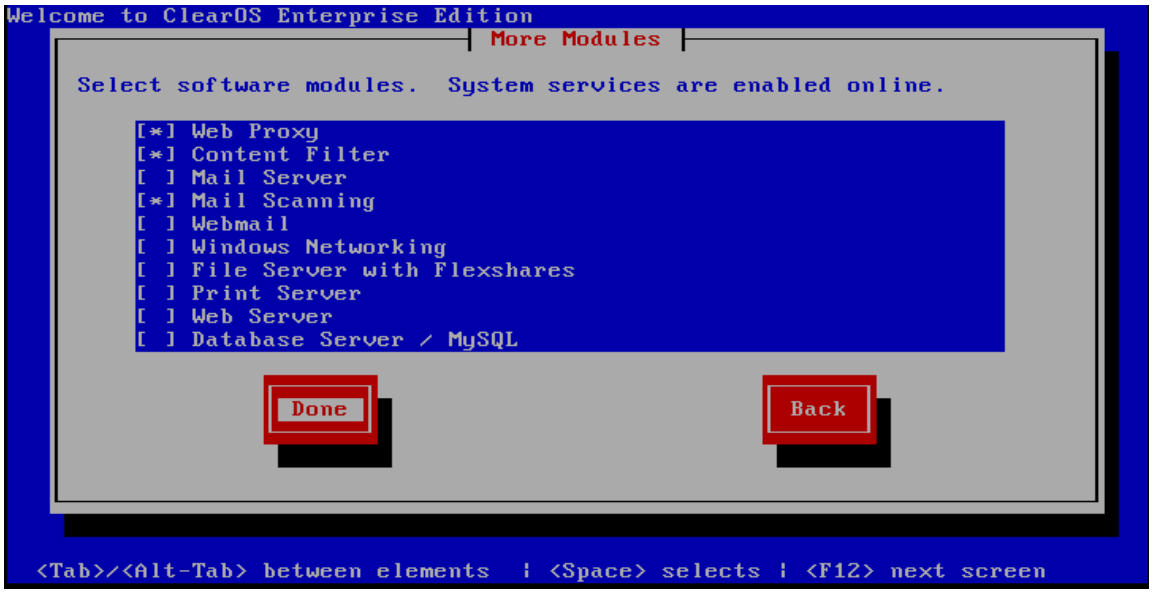

Figura 3.25 confirmación de selección de módulos15.

15. Luego veremos una advertencia en la cual nos pregunta si esta correcta la configuración, seleccionamos **Done**

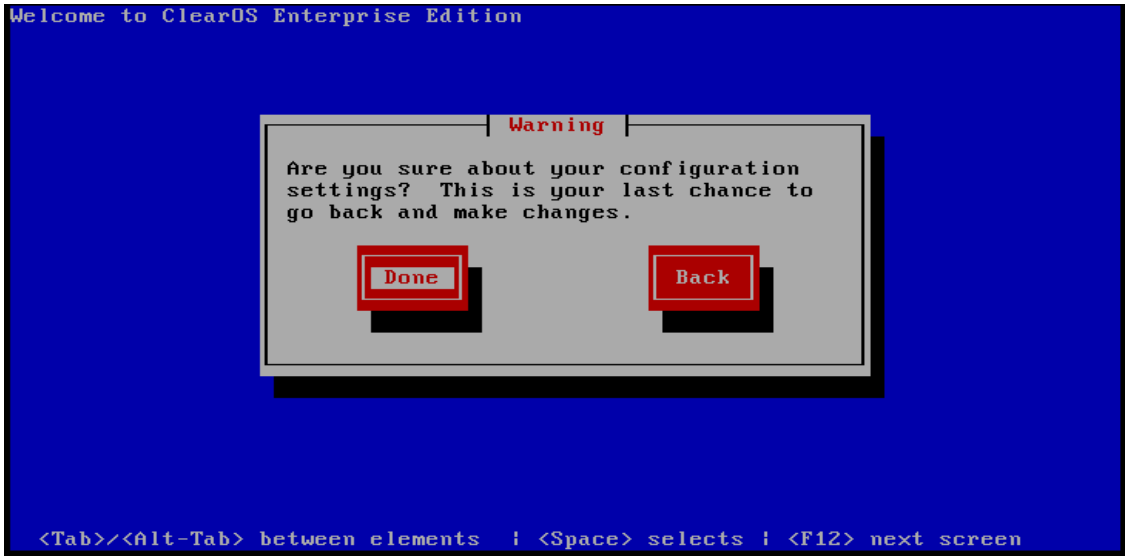

Figura 3.26 Confirmación

16.aparece una venta en la cual nos muestra el proceso de la instalación de los paquetes

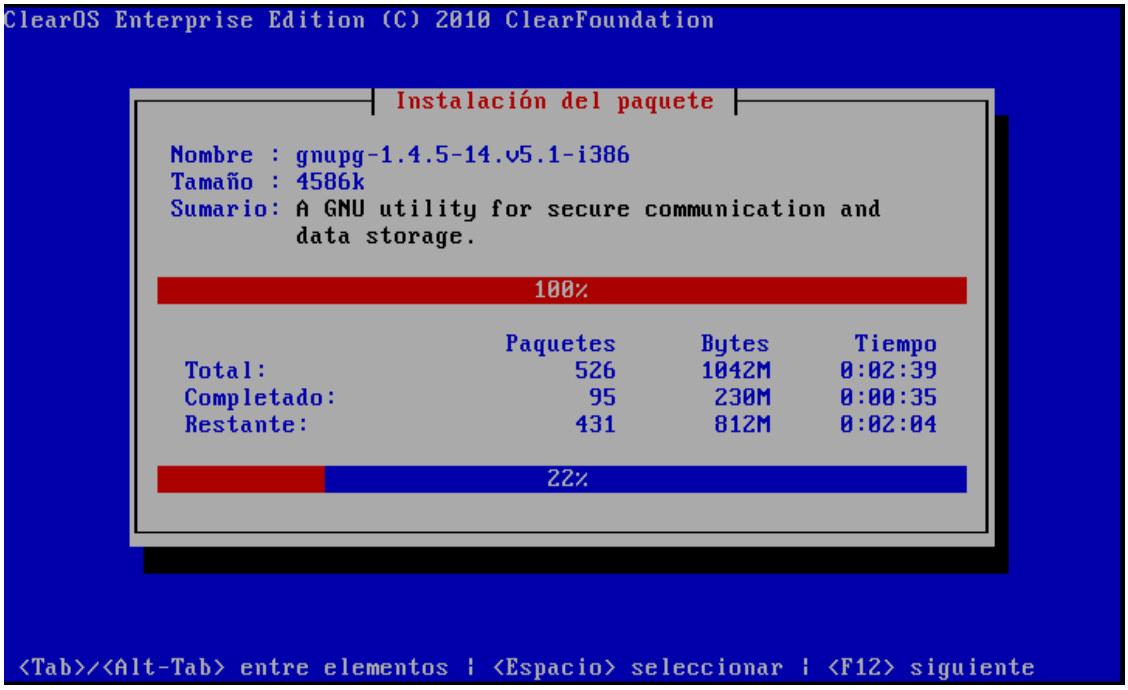

Figura 3.27 proceso de instalación

17. Al finalizar nos muestra la una ventana en la cual nos dice que la Instalación a finalizado y que reiniciara el Sistema, previamente retiramos el CD de ClearOS

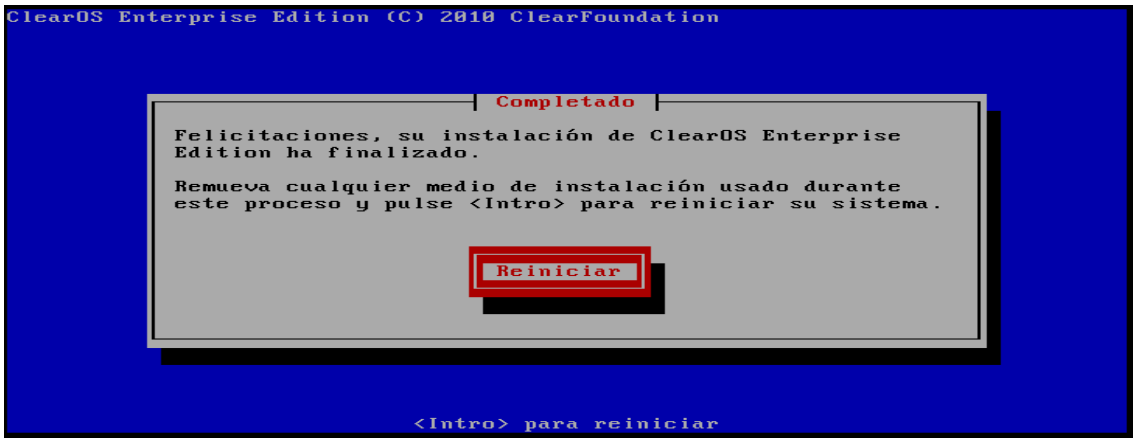

Figura 3.28 reinicio para finalizar instalación

18. Reinicio del Sistema

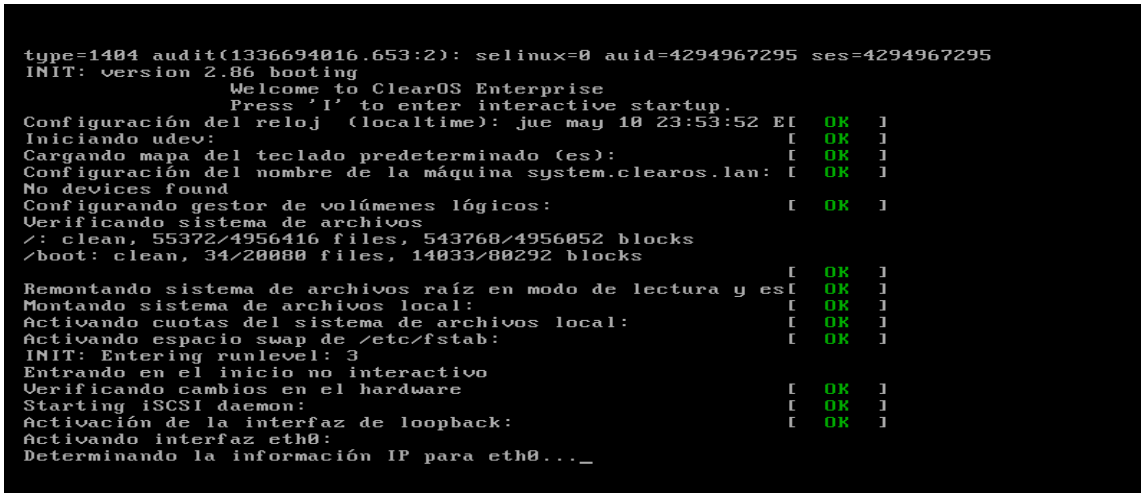

Figura 3.29 reinicio del sistema

2. Configuración inicial

Al reiniciar el Sistema iniciamos sesión con el usuario **Root** y la contraseña previamente establecida.

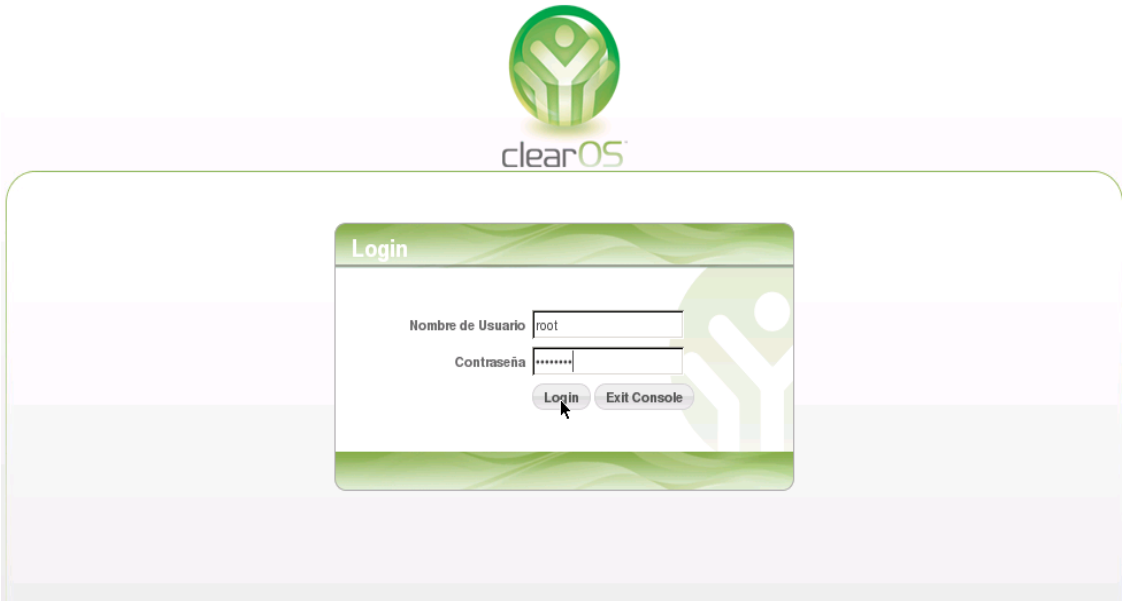

Figura 3.30 inicio de sesión

3.1.6 Presentación de la propuesta

En un acuerdo con la decisión del encargado de TI, se opto por utilizar la herramienta ClearOS en base a la tabla comparativa de herramientas propuestas y a la experiencia que él tiene con utilización de herramientas de Open Source para seguridad informática.

Oferta Económica

Cotización : 000001
Fecha: 23 de Abril de 2012

Sres.: Droguería Universal S.A de C.V
Dirección: Alameda Roosevelt 32736, San Salvador
Teléfono: (503) 2352 – 1000

Cantidad	Descripción	Precio Unitario	Total
1	ClearOS 5.2 Community Edition Open source	$0.00	$0.00
La herramienta no tiene costo alguno por ser Open Source			$0.00

Oferta Técnica

Cotización : 000001
Fecha: 23 de Abril de 2012

Sres.: Droguería Universal S.A de C.V
Dirección: Alameda Roosevelt 32736, San Salvador
Teléfono: (503) 2352 – 1000

Cantidad	Descripción	Precio Unitario	Total
1	Instalación y Configuración de ClearOS 5.2	$0.00	$0.00
1	Capacitación de Personal Técnico	$0.00	$0.00
1	Visitas de Soporte durante el proyecto de Graduación	$0.00	$0.00
La oferta técnica no tiene costo alguno por ser proyecto de Tesis en beneficio de la Compañía			$0.00

Tabla comparativa de Herramientas propuestas

Evaluación técnica de herramientas Open Source Sera considerado como aprobado si alcanza una ponderación mínima del 80%									
Características		Parámetro o valoración requerida	Peso	Operaciones a evaluar					
				ZENTIAL		IPCOP		CLEAROS	
				Calificación	Puntaje	Calificación	Puntaje	Calificación	Puntaje
1	Facilidad de instalación y administración	Indispensable	20%	2	20	1	15	2	20
2	Módulos integrados de Seguridad	Indispensable	15%	2	15	1	10	2	15
3	Servicios integrados básicos de una LAN	Indispensable	10%	1	5	1	5	2	10
4	Soporte comunitario	Indispensable	25%	1	15	2	25	2	25
5	Estabilidad	Indispensable	20%	2	20	2	20	2	20
6	Compatibilidad e integración con otros sistemas	Indispensable	10%	2	10	1	5	2	10
Totales			100%		85				
Ponderación final					85 %		80%		100%
Resultado obtenido				Aprobado		Aprobado		Aprobado	
Calificación: **(0)**, si no cumple o no especifica que cumple; **(1)**, cumple a medias sin perder la funcionalidad; **(2)**, cumple o supera lo requerido									

3.1.7 Evidencias del proyecto

1. Comenzaremos a configurar el servidor con el Asistente Inicial que consta de 6 Pasos, primero solicita el **Idioma** seleccionamos **Spanish.** Damos clic en *Siguiente.*

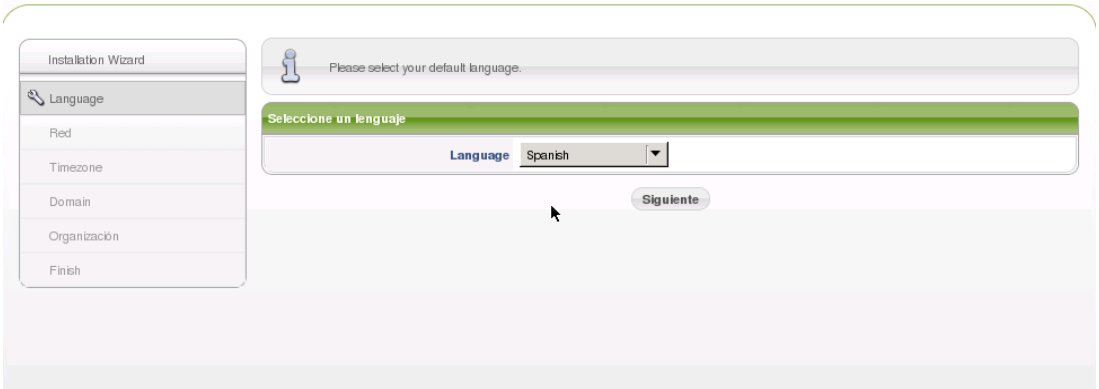

Figura 3.31 selección de idioma

2. Posteriormente veremos las interfaces de redes las cuales se pueden Editar o Eliminar. Cambiamos el nombre del servidor del DNS #1 y digitamos la IP del Servidor que sería para este caso 172.22.1.21. El DNS #2 no lo modificamos luego damos clic en *Siguiente*

Figura 3.32 asignación de nombre de servidor

3. Seleccionamos la zona horaria, configuramos **América-El Salvador.** Clic en *Siguiente*

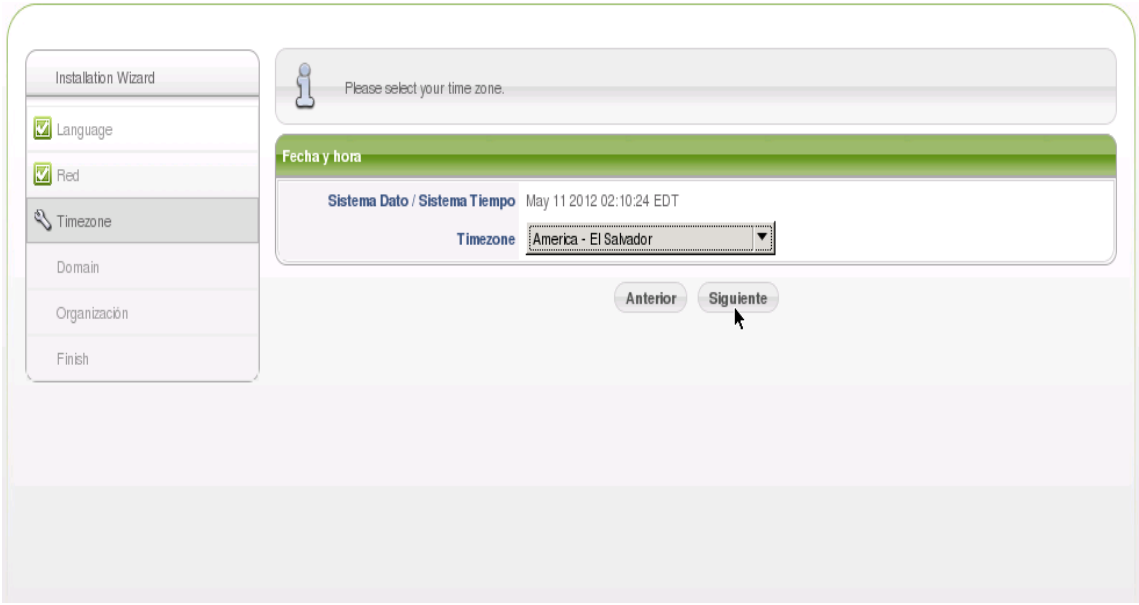

Figura 3.33 selección de zona horaria

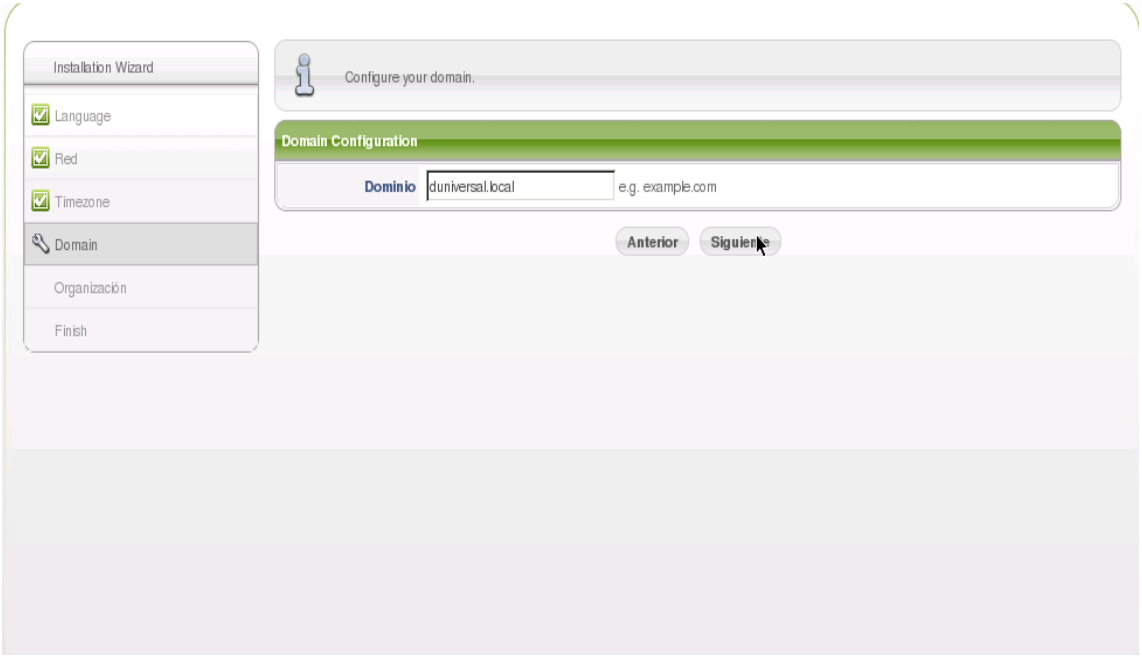

Figura 3.34 Asignación de dominio

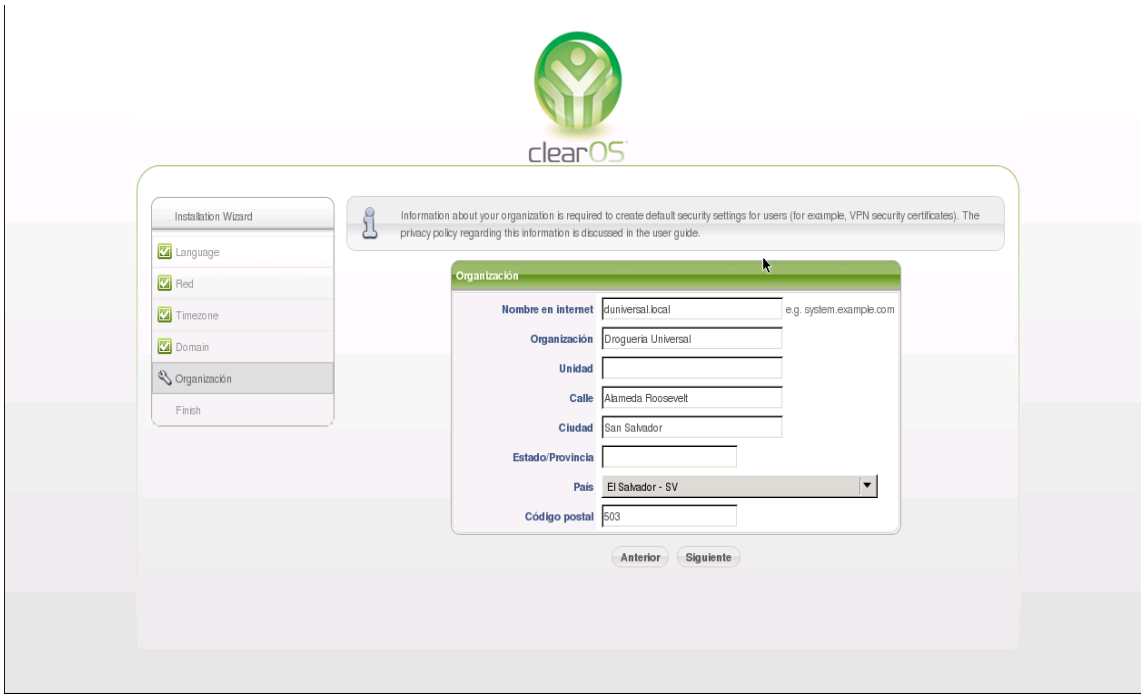

Figura 3.35 información de organización

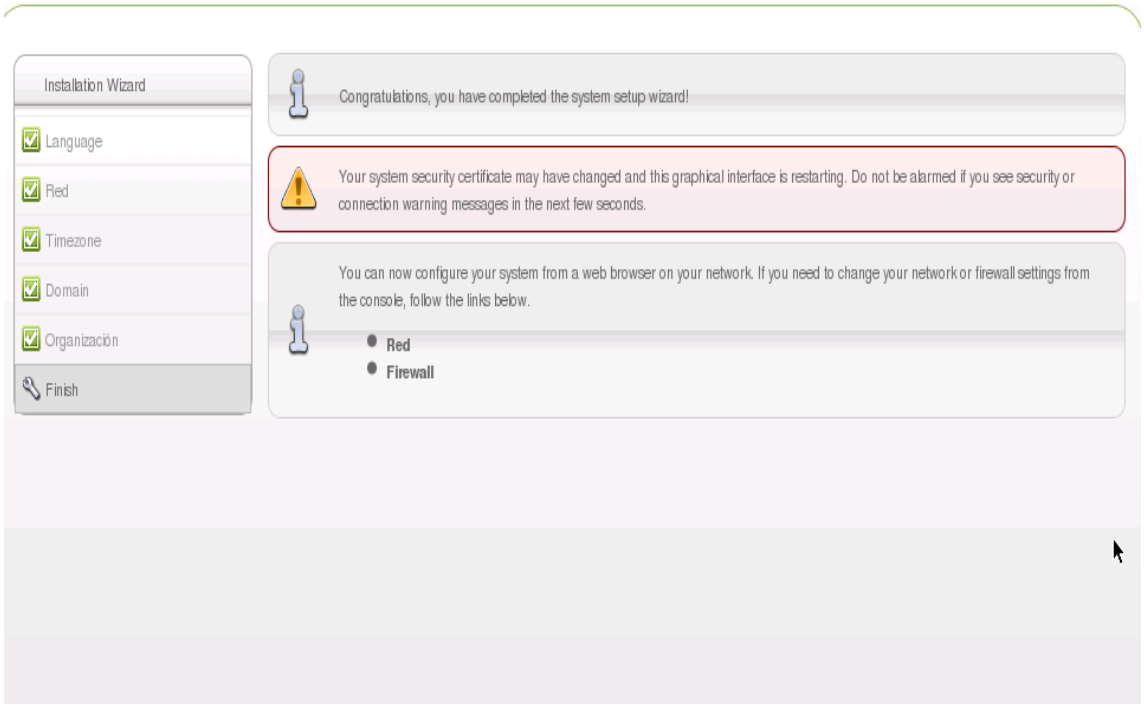

Figura 3.36 finalización de asistente de configuración

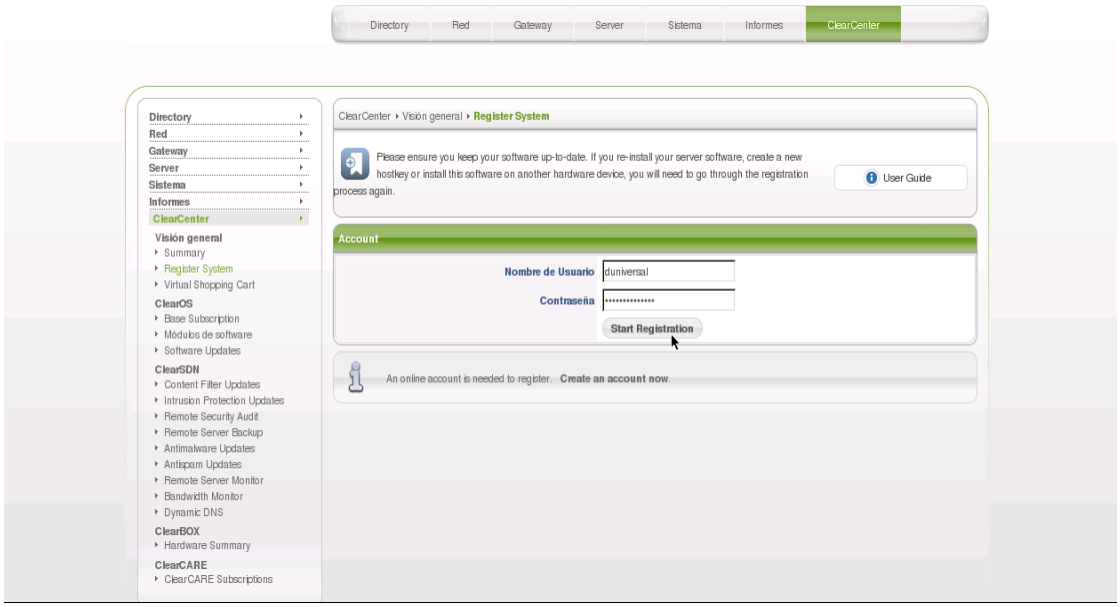

Figura 3.38 inicio de registro

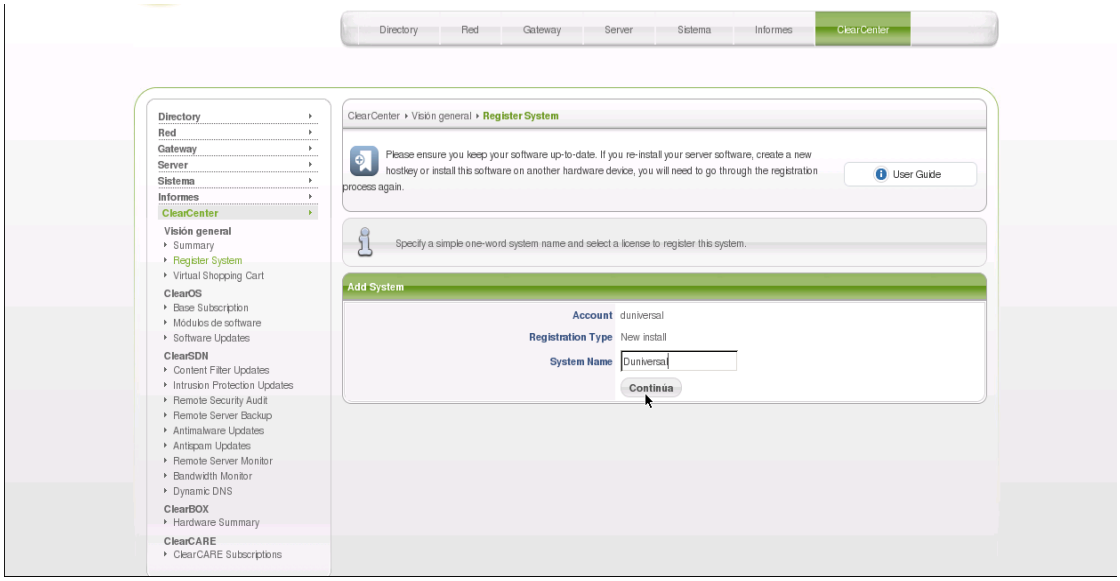

Figura 3.39 nombre del sistema

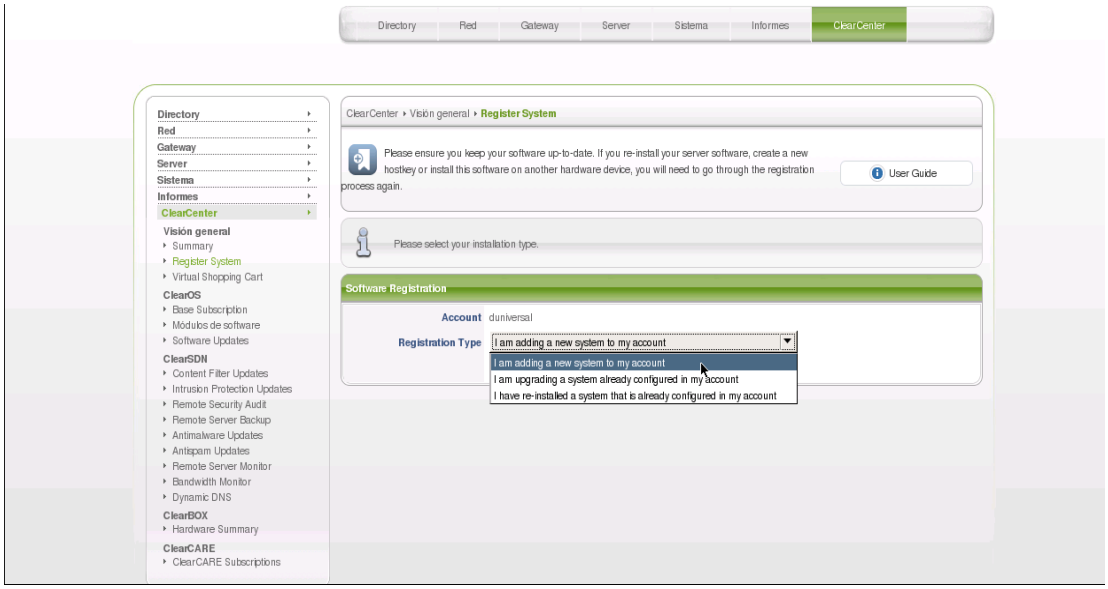

Figura 3.40 tipo de registro

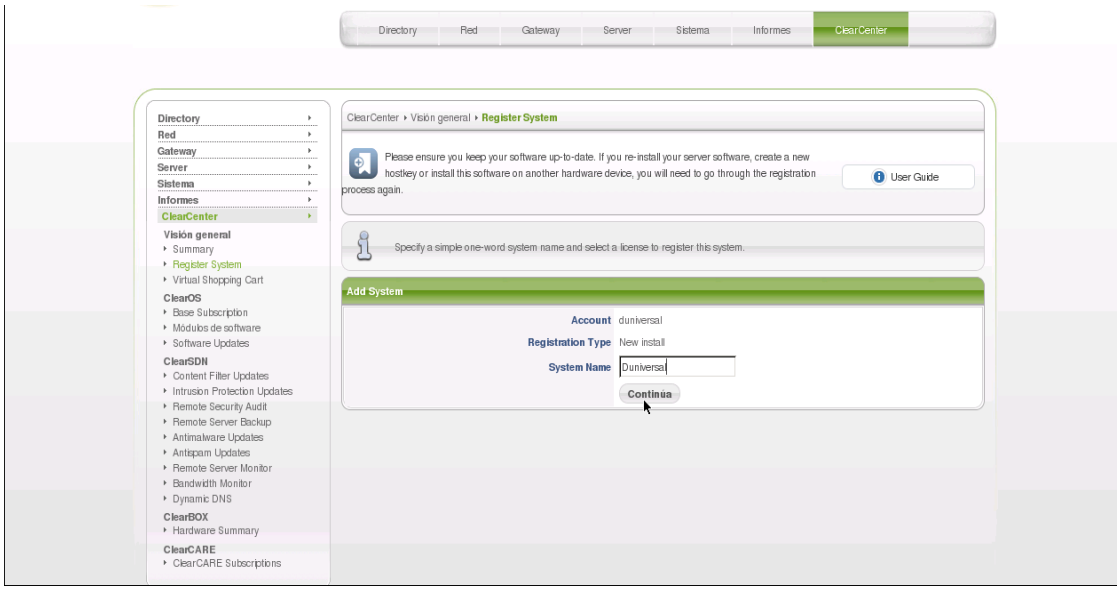

Figura 3.41 Nombre para registro

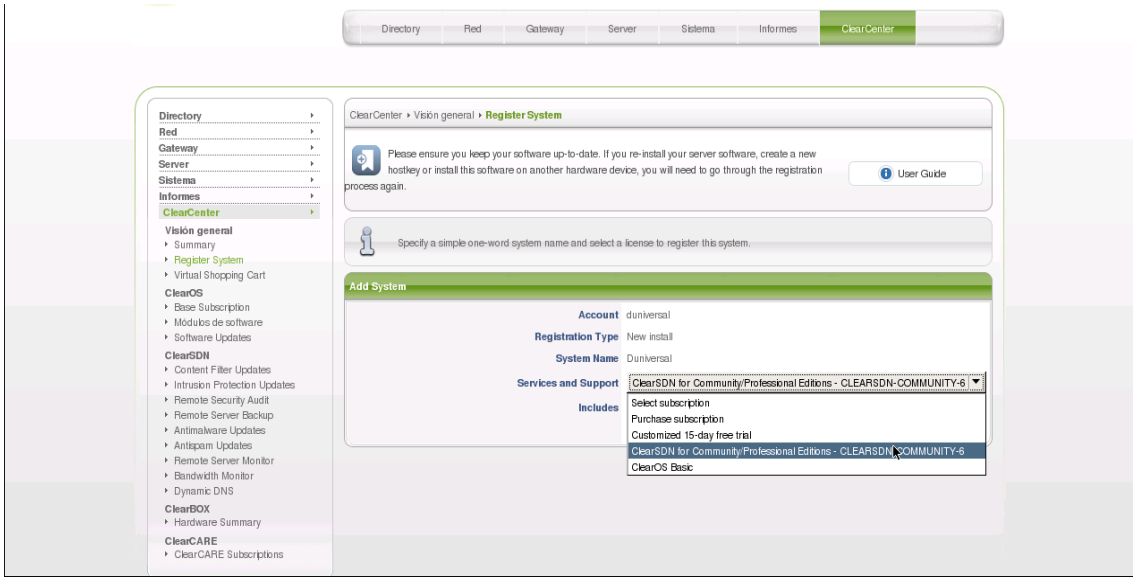

Figura 3.42 Tipo de subscripción

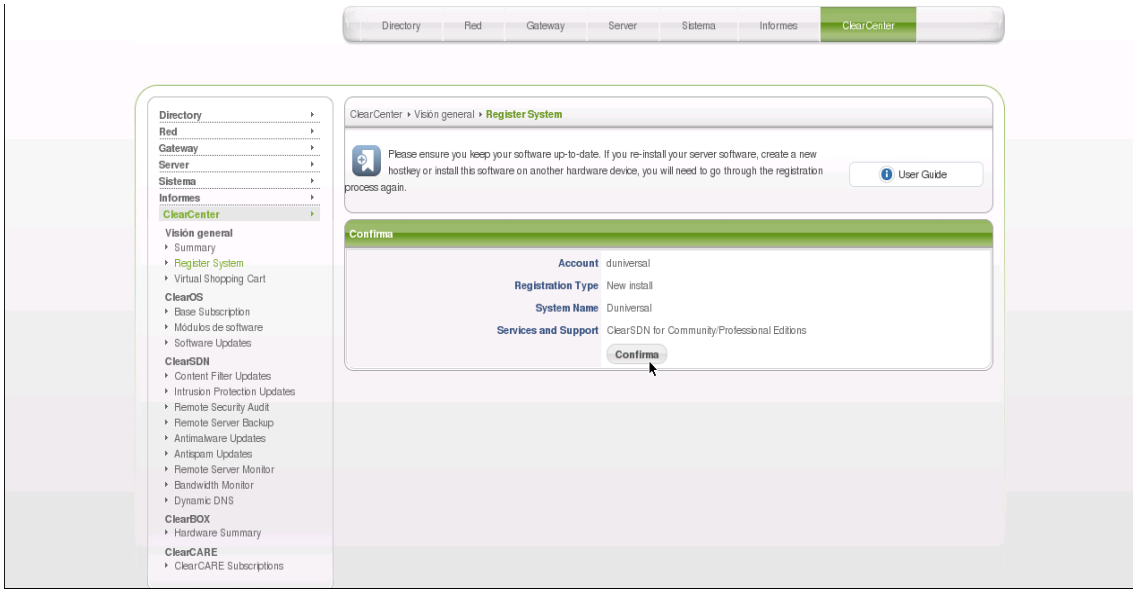

Figura 3.43 confirmación de registro de sistema

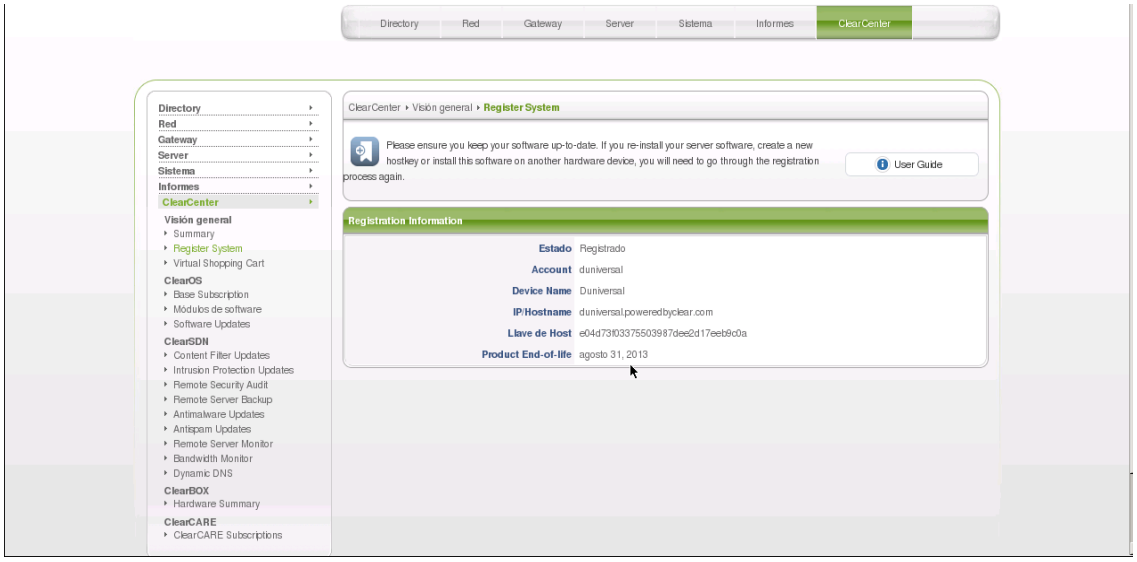

Figura 3.44 Estado de registro de sistema

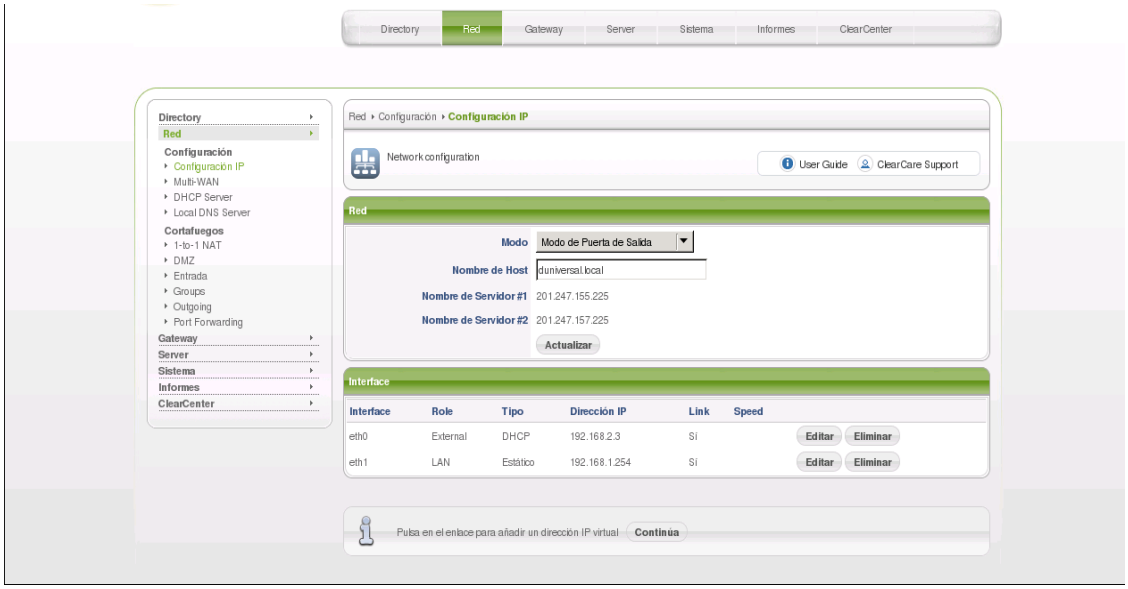

Figura 3.45 Configuración de IP

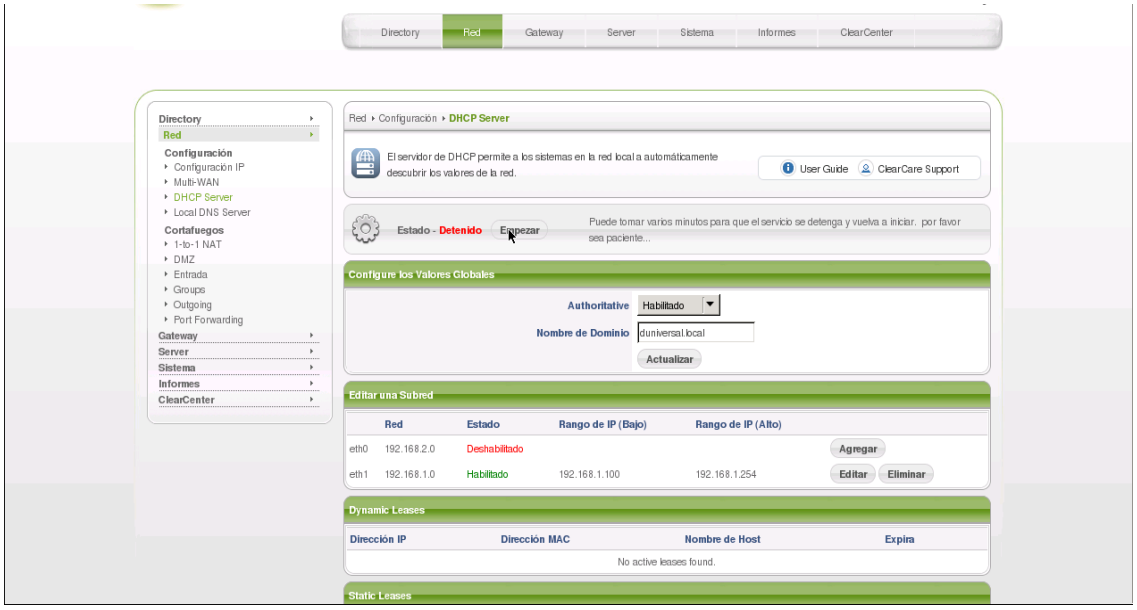

Figura 3.46 DHCP Server

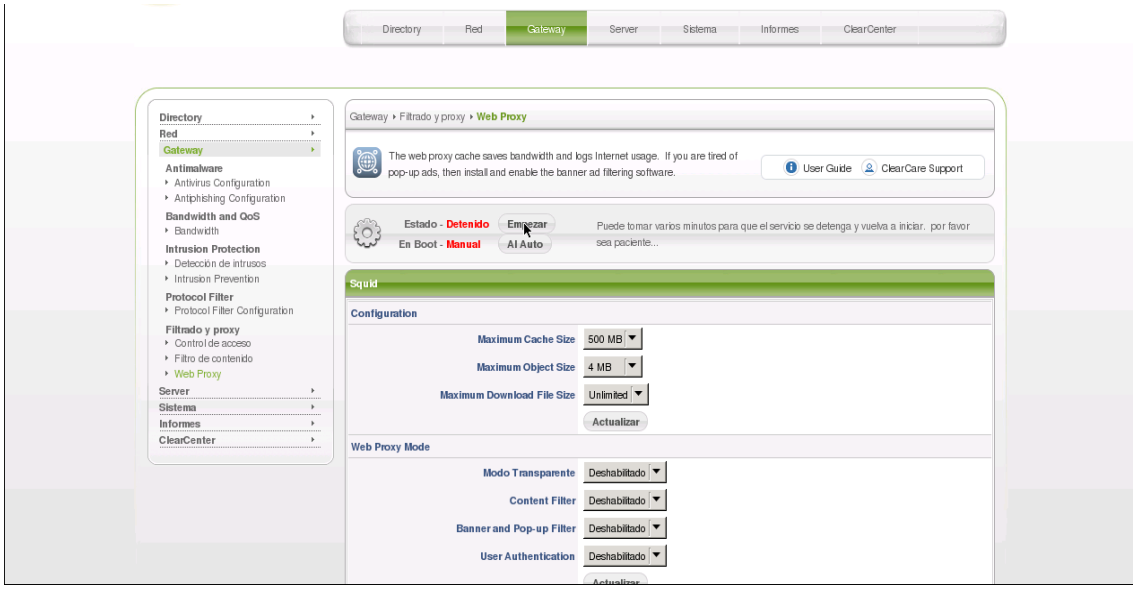

Figura 3.47 Web Proxy

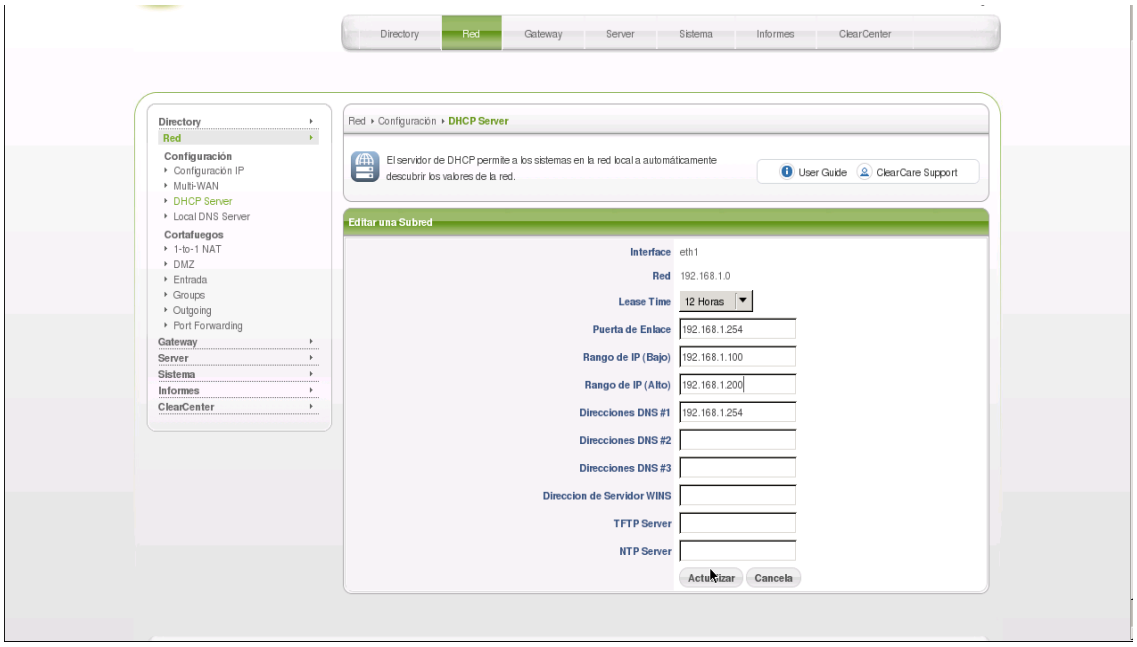

Figura 3.48 Edición de sub redes

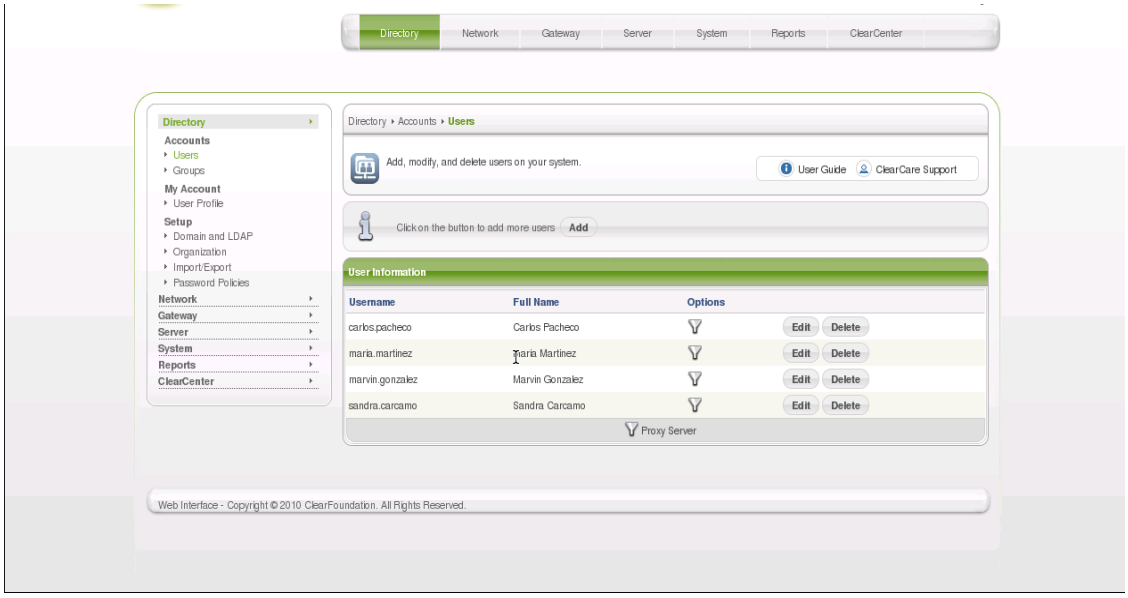

Figura 3.49 Creación de usuarios

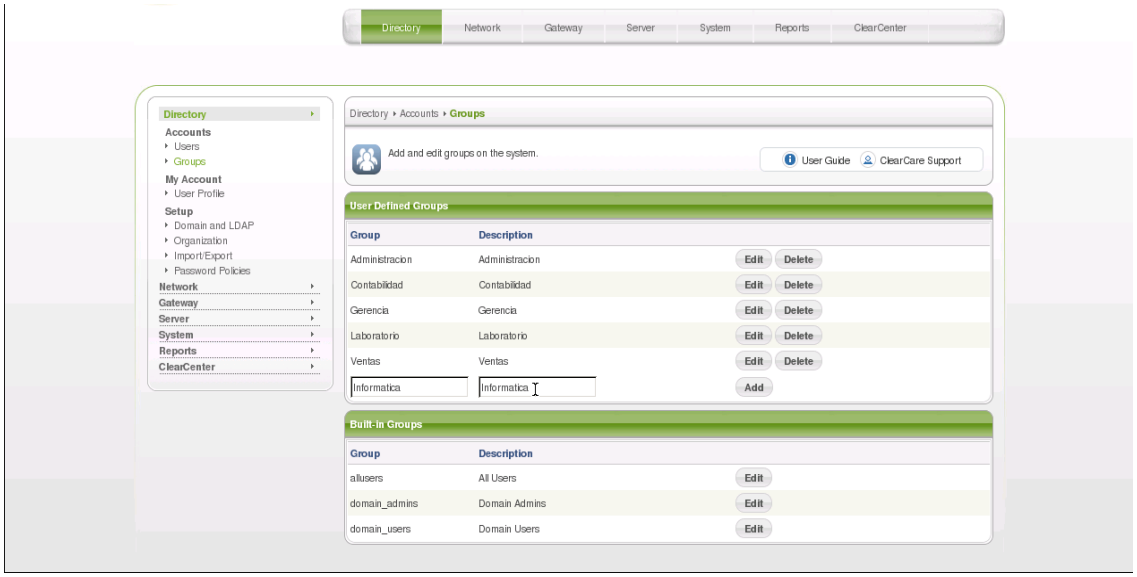

Figura 3.50 Creación de grupos

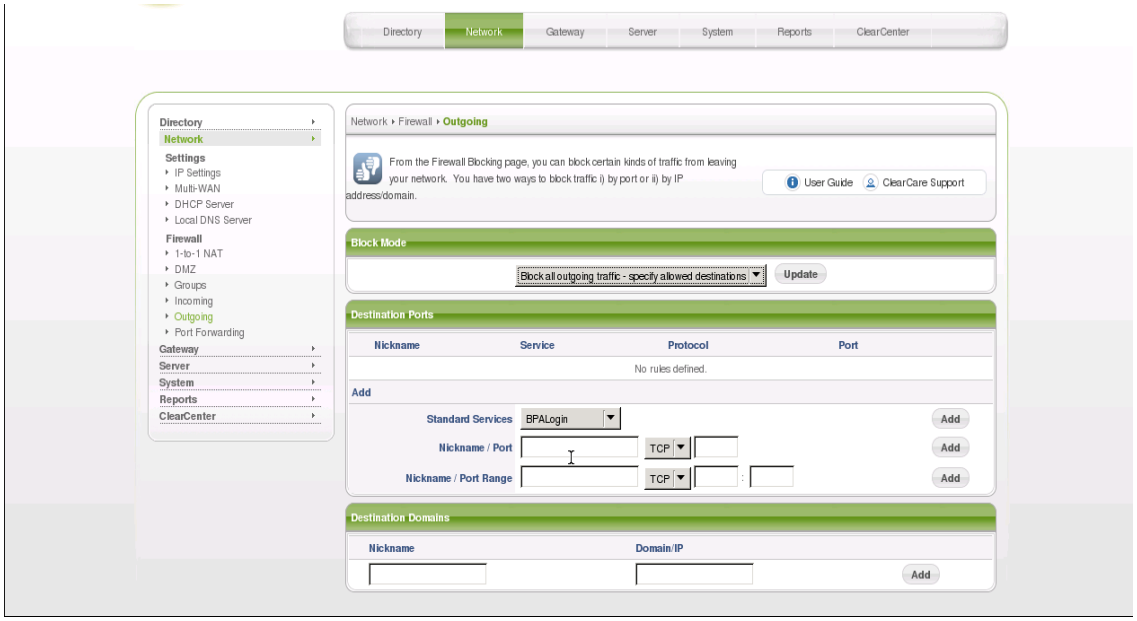

Figura 3.51 Bloqueo de trafico saliente

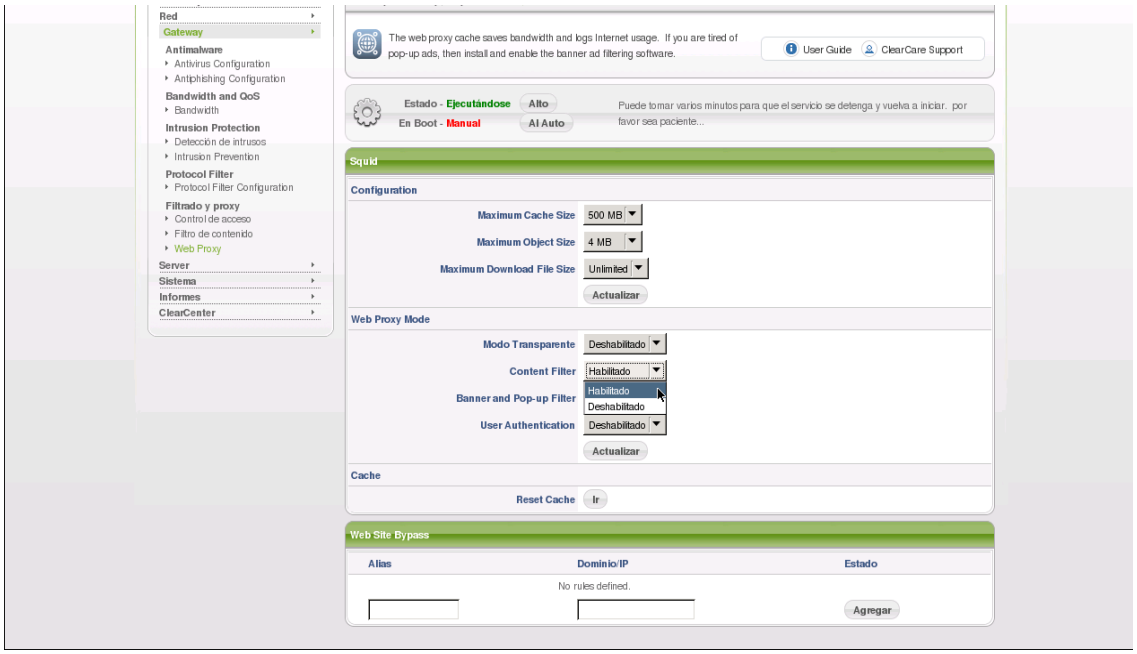

Figura 3.52 Web Proxy

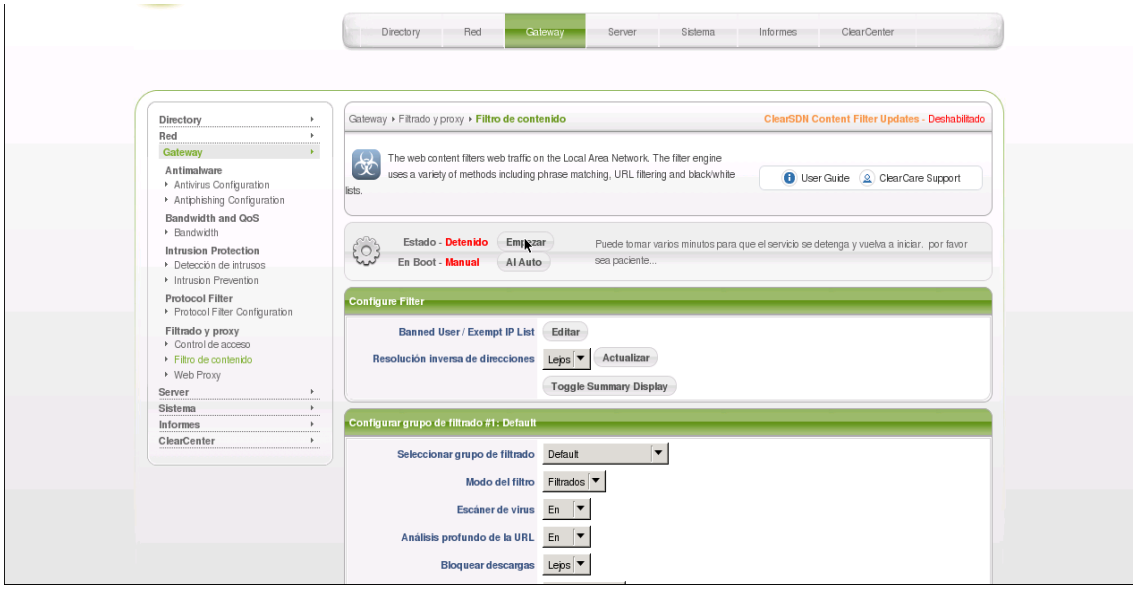

Figura 3.53 Filtro de contenido

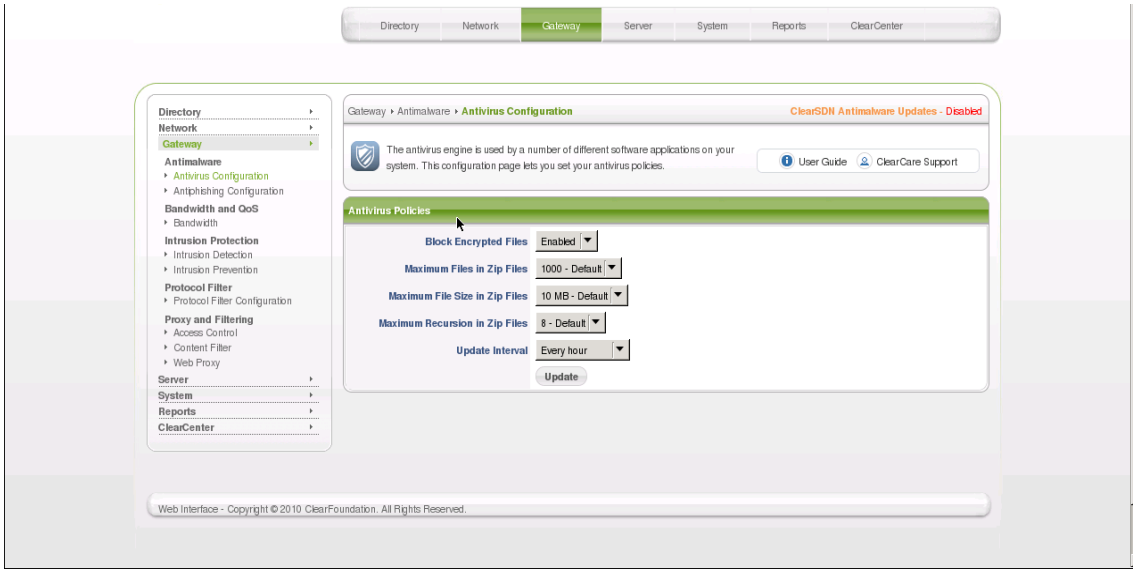

Figura 3.54 Configuración de antivirus

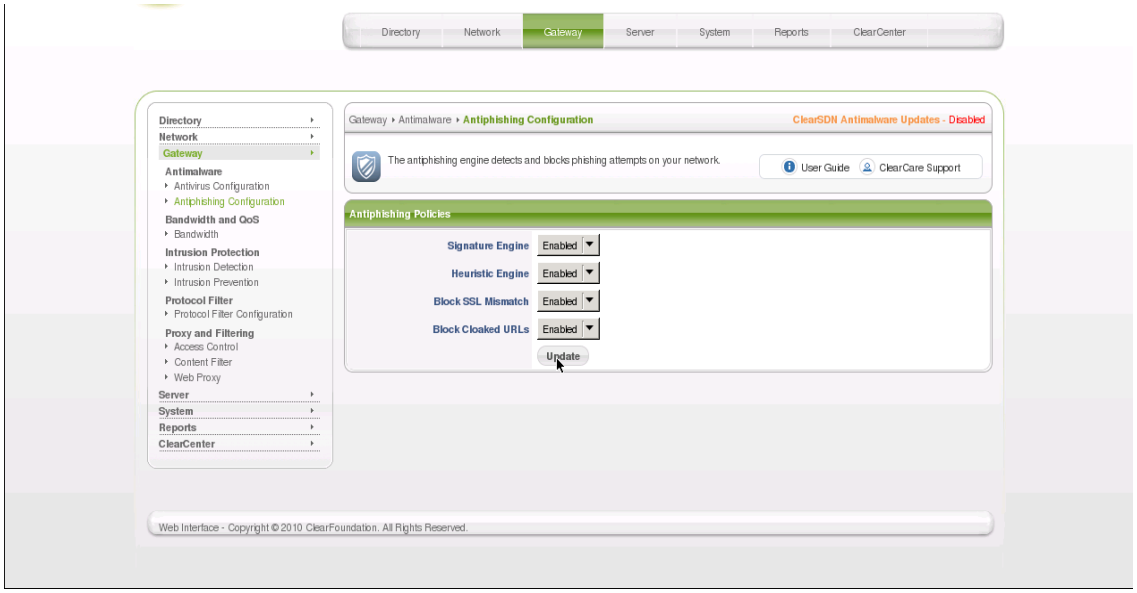

Figura 3.55 Configuración Antiphishing

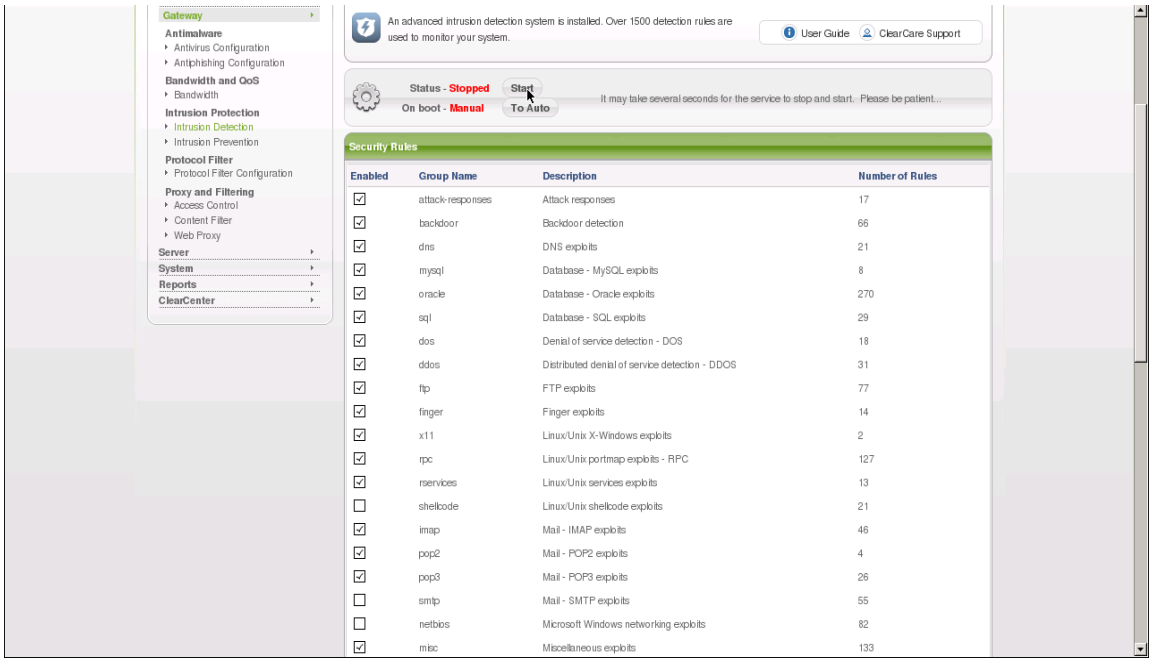

Figura 3.56 Configuración de detección de intrusos

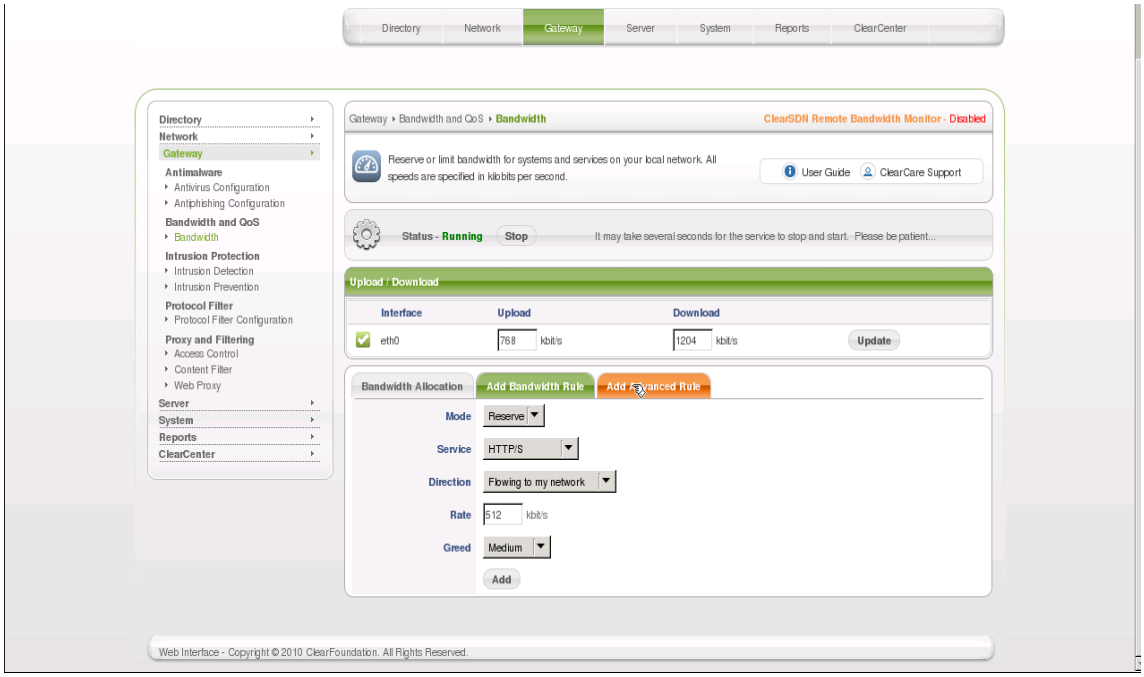

Figura 3.57 Configuración de Bandwidth

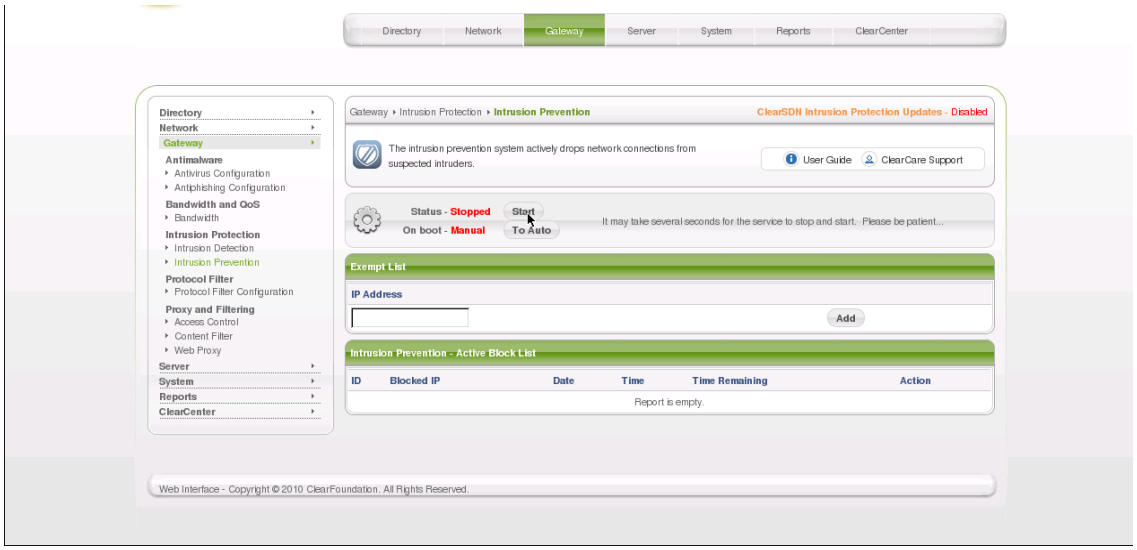

Figura 3.58 Configuración de Prevención de Intrusos

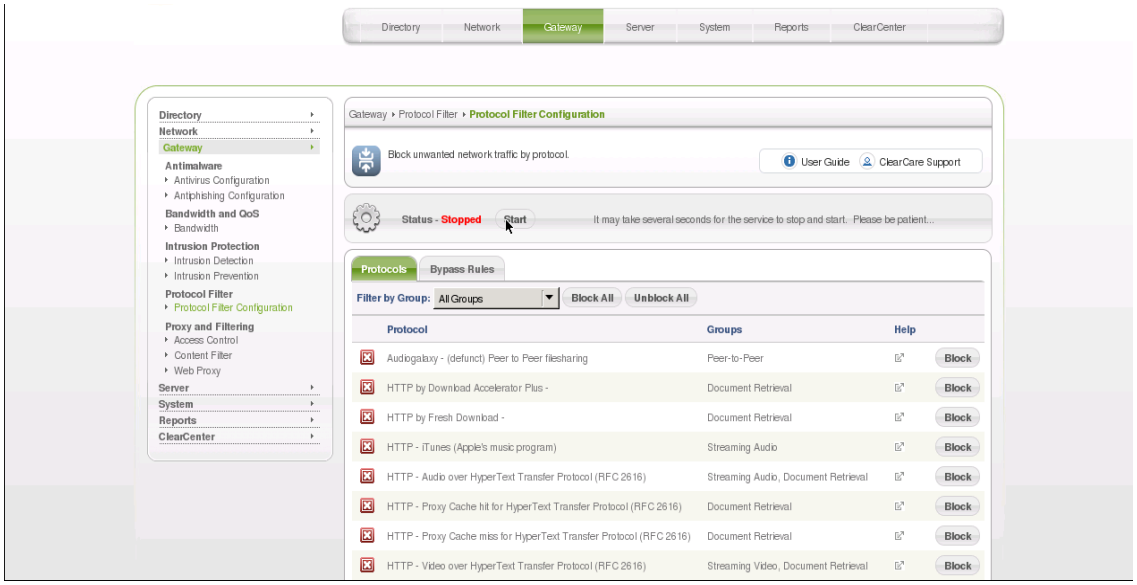

Figura 3.59 Configuración de Filtro de Protocolos

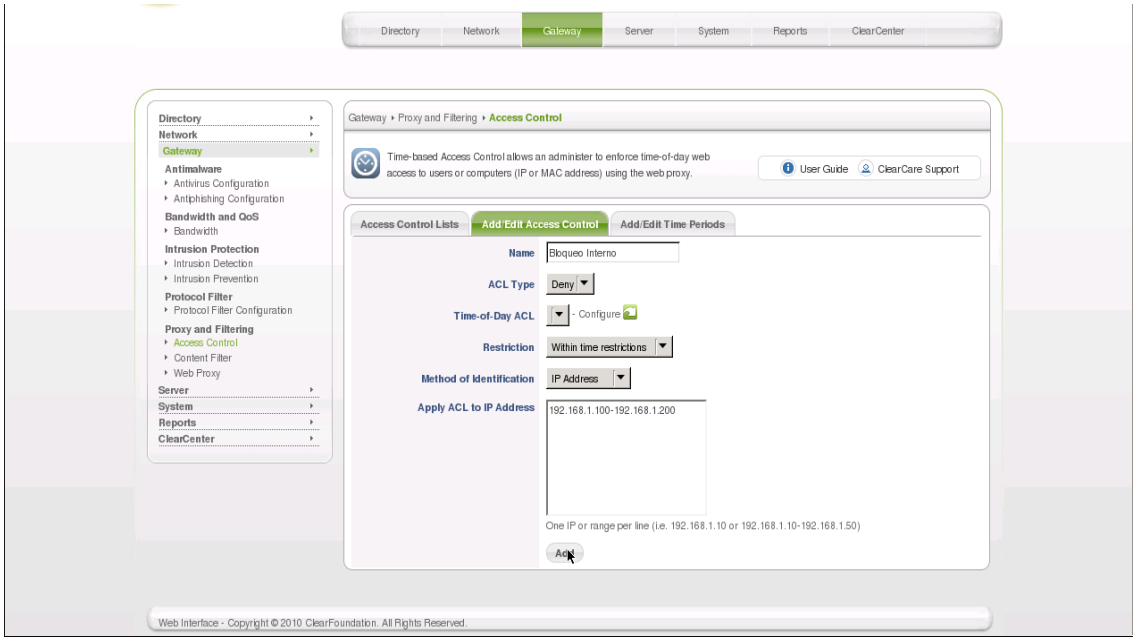

Figura 3.60 Configuración de Control de Acceso

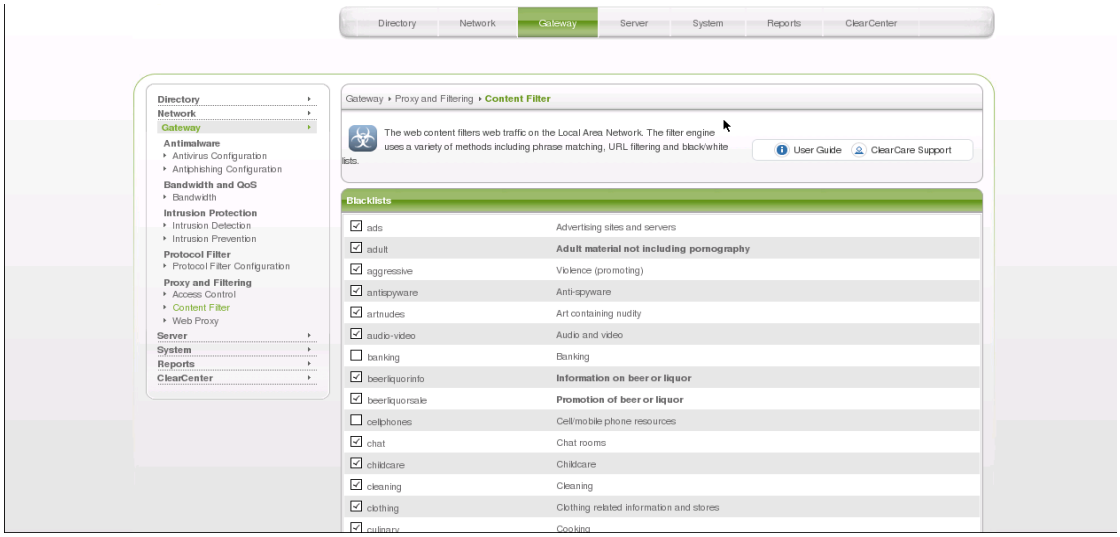

Figura 3.61 Configuración de Filtro de contenidos

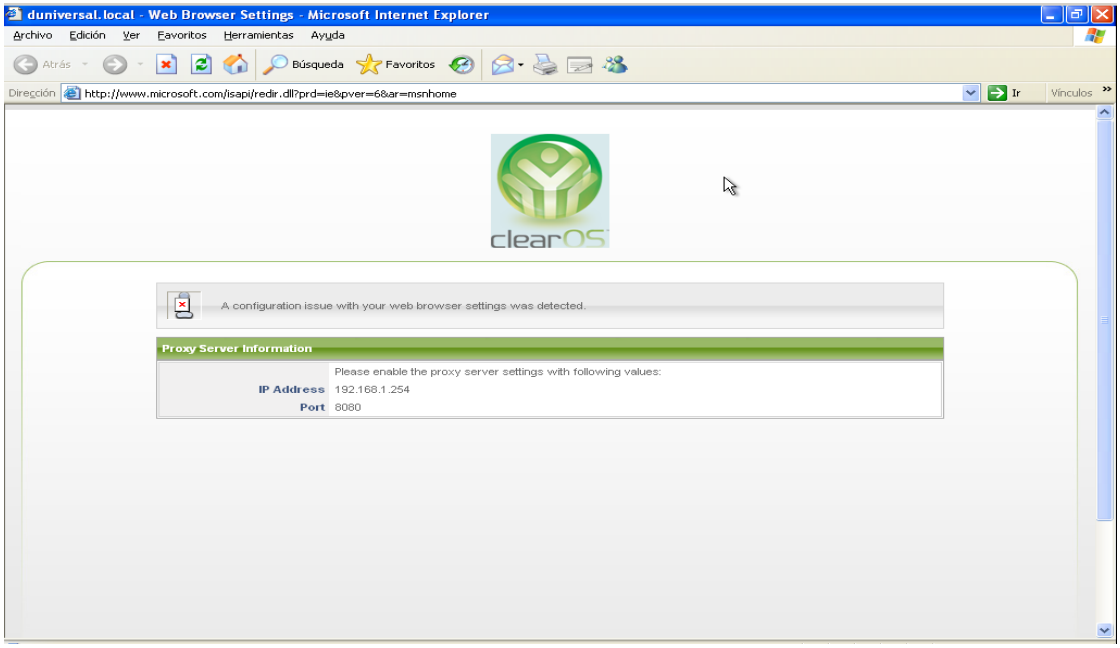

Figura 3.62 Muestra de bloqueo de Proxy

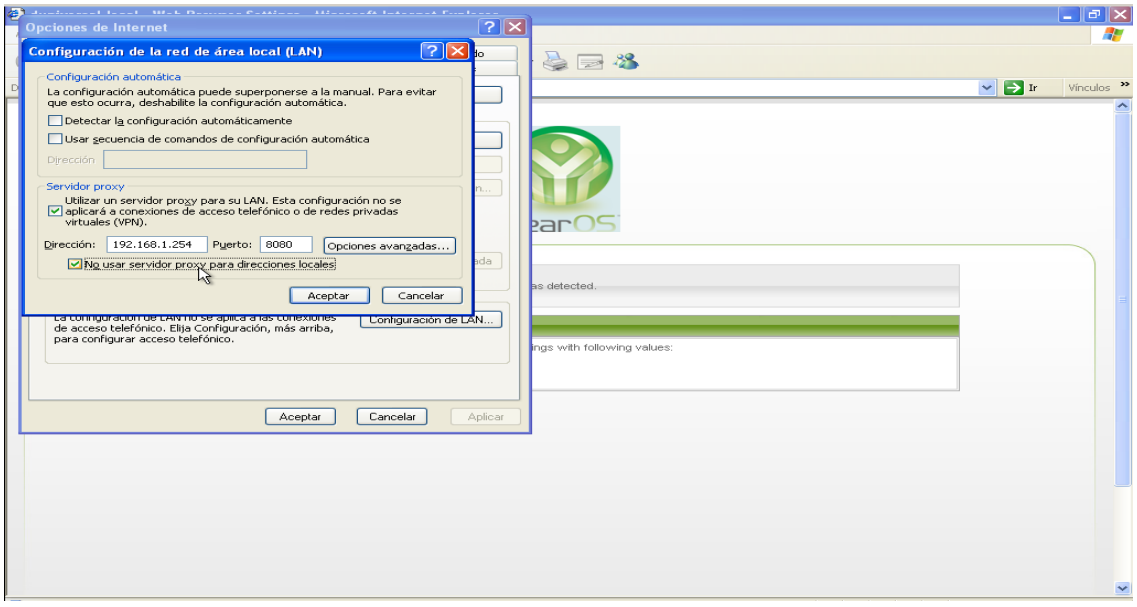

Figura 3.63 Configuración de Proxy en la red

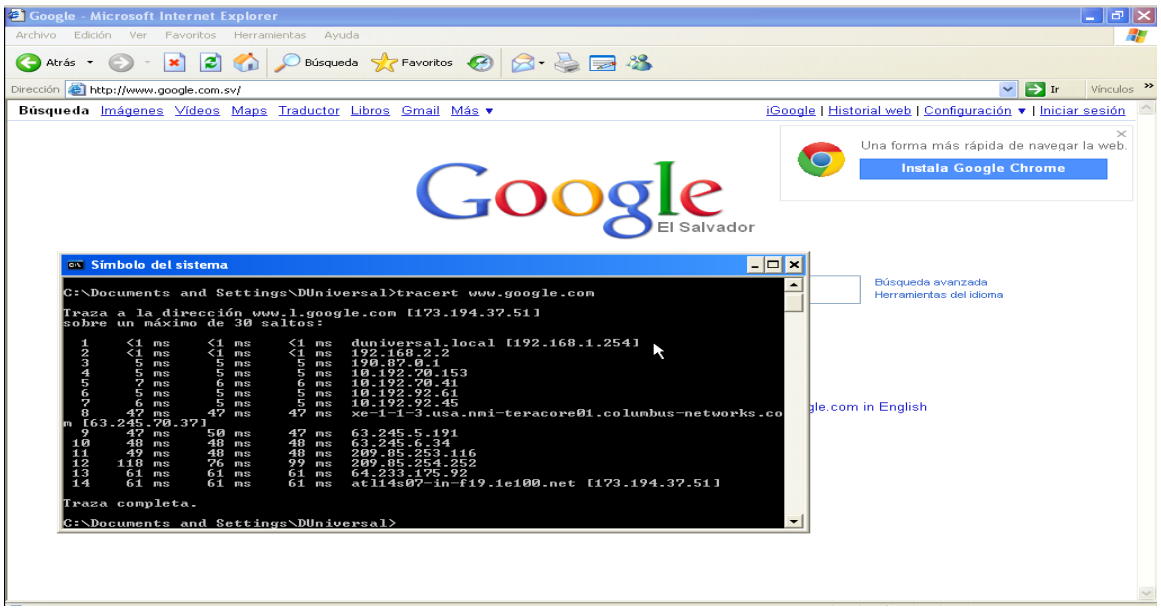

Figura 3.64 Verificación de tracert a una dirección de internet

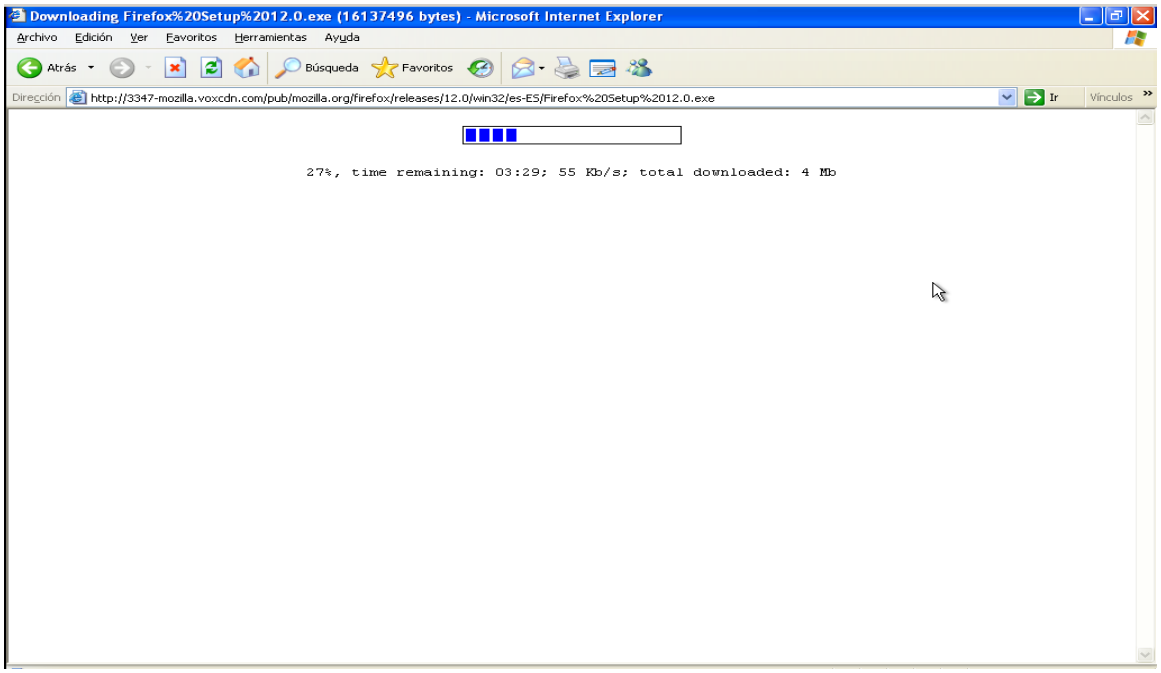

Figura 3.65 Proceso de descarga

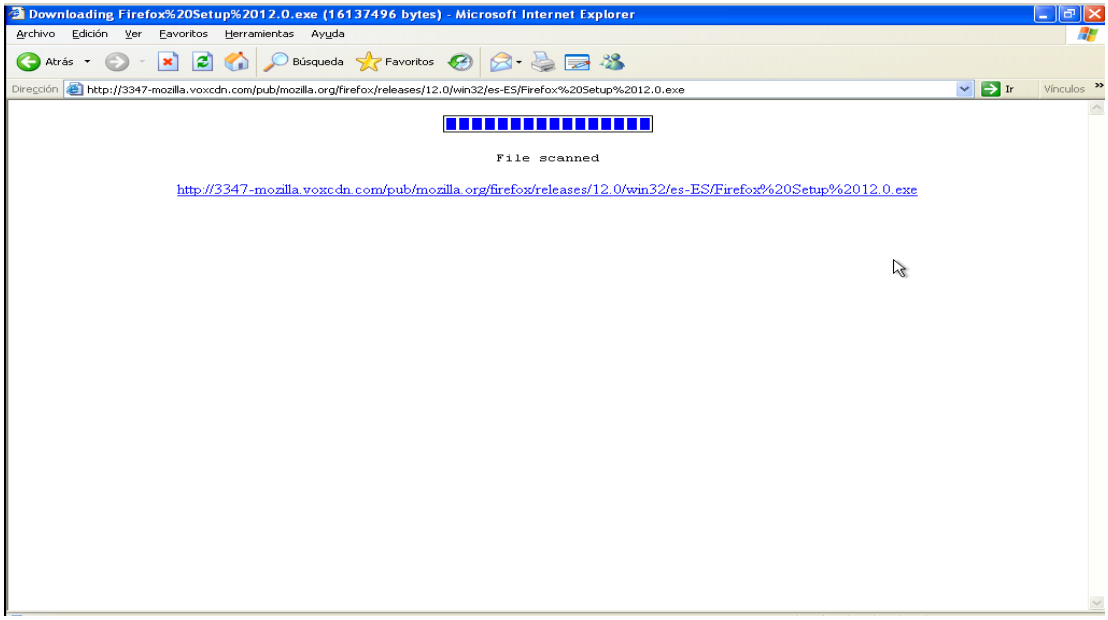

Figura 3.66 Finalización de escaneo al descargar

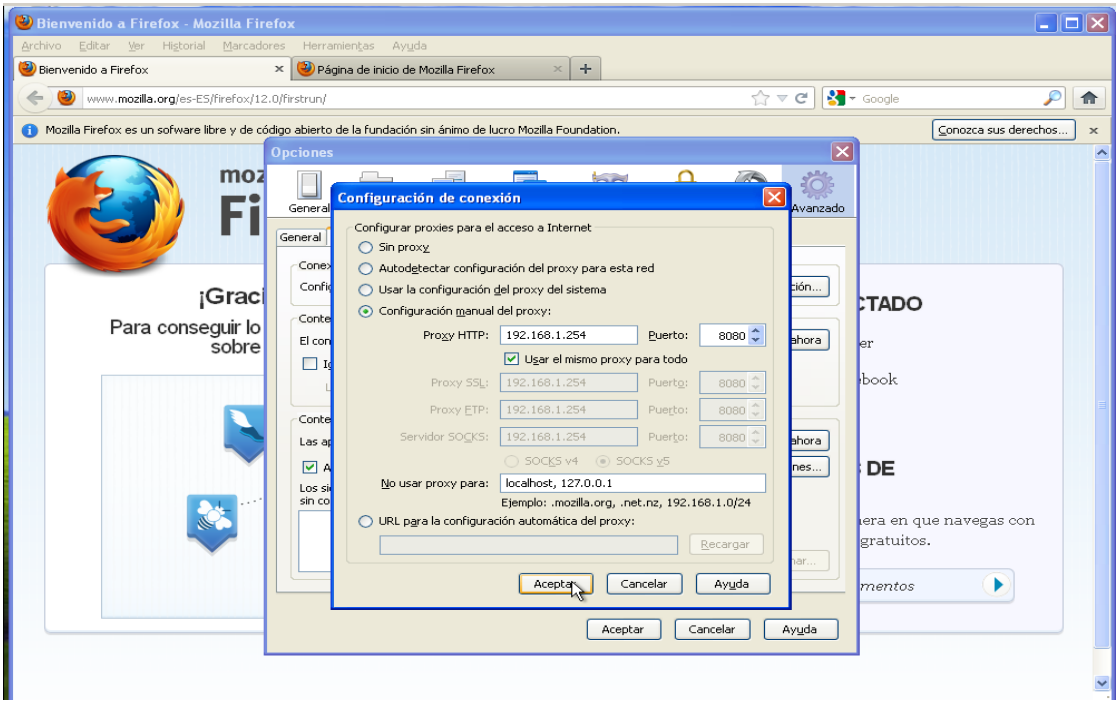

Figura 3.67 Configuración de conexión

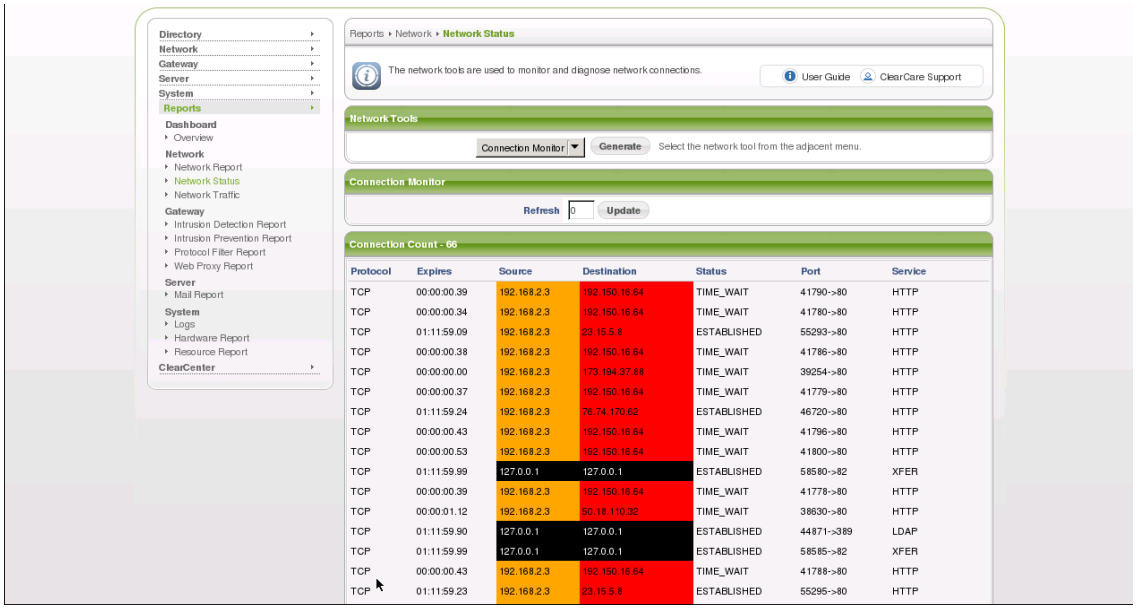

Figura 3.68 Estatus de la red

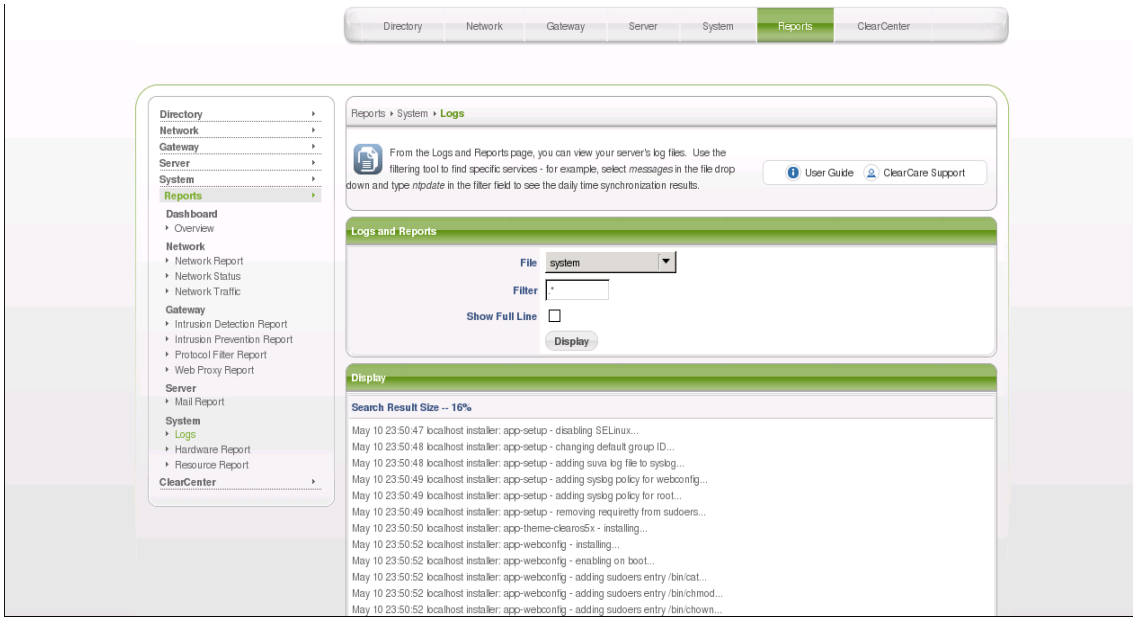

Figura 3.69 Registros

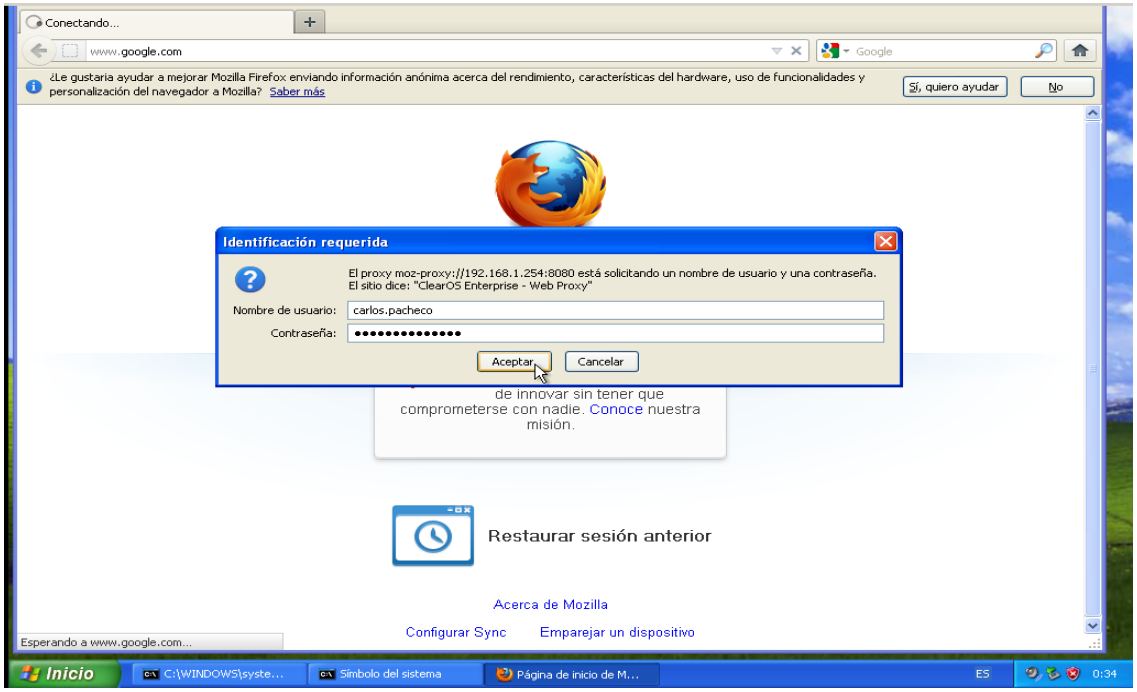

Figura 3.70 Validación de usuarios con el Proxy

Figura 3.71 instalación de server

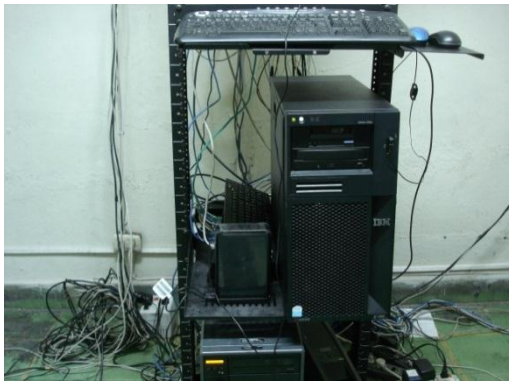

Figura 3.72 server con ClearOS

Figura 3.73 Configuración de ClearOS

Figura 3.74 Configuración de servicios

Figura 3.75 Demostración de ClearOS

Figura 3.76 Prueba de ClearOS

Conclusiones

Con el desarrollo de la investigación realizada en la compañía se pudo constatar de las necesidades tecnológicas y los problemas de seguridad informáticos los cuales hoy en día se enfrentan las PYMES e imposibilitan el crecimiento de estas.

A pesar de estar conscientes de los beneficios que las tecnologías informáticas proveen, y que día con día se han ido transformando en medios esenciales para realizar sus negocios y actividades cotidianas.

La adquisición de plataformas de seguridad o herramientas, se suele ver por las gerencias como un gasto y no como una inversión, por la falta de conocimiento sobre las herramientas Open Source, optan por trabajar sin herramientas de seguridad provocando riesgos de alta magnitud.

Ante cualquier amenaza que puede generar problemas de operación o aun peor robo o pérdida de información vital para la operación del negocio.

Ante toda esta problemática que se genera existen herramientas de código Abierto que benefician en gran medida las PYMES, ahorrando costos excesivos de licenciamiento y proveyendo múltiples soluciones para cada necesidad existente,

Por lo cual se destaca el impacto que estas herramientas generan en el desarrollo de las PYMES ayudándoles a expandirse y trabajar de una forma óptima y segura

.

Recomendaciones

- Brindar el seguimiento necesario a la implementación para mantener y administrar óptimamente la herramienta de seguridad Open Souce.

- Se recomienda monitorear periódicamente la implementación de los servicios Activos de ClearOS y establecer líneas bases que nos permitan observan cambios o saturación en el rendimiento de la red.

- Se recomienda sacar reportes semanales de las estadísticas de la negación, tráfico, detecciones del antivirus y módulos de IPS e IDS.

- Es necesario crear una bitácora de seguridad en la cual nos permita registrar todos los incidentes y cambios que se efectúen en la distribución de ClearOS.

- La persona encargada del soporte deberá mantener actualizada la distribución de ClearOS y deberá estar en constante verificación de cualquier parche o actualización para evitar cual problema de seguridad o funcionamiento.

- Se recomienda la adquisición de otro disco para crear un arreglo RAID 1 para establecer una estrategia tolerante a fallas.

- Se recomienda la implementación de una herramienta de Backup que nos permita respaldar las configuraciones de nuestro equipo

- Se recomienda asegurar físicamente el área del Data Center para evitar que personas no autorizadas puedan provocar al daño en los equipos o en las conexiones de la red,

Bibliografía

Atica.cl (2012).*Open Source, Costo Beneficio.* Recuperado de http://www.atica.cl/aticaprofesionales/Open-Source/costo-beneficio-open-source.html

Clear Fundation (2012). *Guía de usuario de clearOS 5.2.* Recuperado de http://www.clearcenter.com/support/documentation/clearos_enterprise_5.2/user_guide/start

Clear Fundation (2012). *Software ClearOS 5.2.* Recuperado de http://www.clearfoundation.com/Software/overview.html

Segu-info.com.ar (2012) *Estrategia de Seguridad.* Recuperado de http://www.segu-info.com.ar/politicas/seguridad.htm

Wikipedia (2012) *Seguridad Informática*. Recuperado de http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

Wikipedia (2012).*ClearOS.* Recuperado de http://en.wikipedia.org/wiki/ClearOS

Wikipedia (2012).*Proxy Server.* Recuperado de http://en.wikipedia.org/wiki/Proxy_server

Wikipedia (2012).*Software libre y de código abierto.* Recuperado de http://es.wikipedia.org/wiki/Software_libre_y_de_c%C3%B3digo_abierto

Anexos

Costo Beneficio del Opensource

El alto costo de las soluciones propietarias (ISVs) ha llevado a muchas empresas e instituciones, a considerar el software de código abierto (**opensource**) como una opción cada vez más viable. Hay algunos puntos que considerar en estos escenarios:

Distinciones del Opensource en el ROI

- Bajo costo de las aplicaciones opensource para comenzar proyecto.
- Opensource reduce costos promedio del proyecto al 50%
- Sin altos costos de licencia
- Se obtiene retorno en la medida que se invierte
- Puede balancear inversión, a medida que va obteniendo resultados

Algunas ventajas del Opensource

- Estabilidad de la solución: Las pruebas a las que son sometidas el opensource aseguran un alto nivel de estabilidad.
- Avance tecnológico: Las soluciones tradicionales son incapaces de incorporar tecnología a la velocidad de las opensource.
- Seguridad: Los agujeros de seguridad son detectados tempranamente, al disponer (en las soluciones opensource) del código fuente.

- Independencia de terceros: Teniendo la aplicación y el código fuente, con opensource tenemos toda la independencia que necesitamos.
- Eliminación de costos ocultos: Hay muchos costos que no aplican en las soluciones opensource, como los asociados a las licencias, soporte, códigos fuentes, etc.
- Continuidad del producto: En el mundo opensource, su aplicación no es vulnerable a las políticas de los ISVs para descontinuar productos.
- Mayor funcionalidad: La gran cantidad de programadores, permiten incorporar muchas más funcionalidades a la aplicación opensource que a una propietaria.
- Calidad, altos estándares: El gran número de testers de aplicaciones opensource, garantizan un producto altamente probado.
- Costos: Las aplicaciones open source pueden costar desde un 30% de lo que costaría un equivalente en software propietario.

Glosario

CPU: Unidad central de procesamiento, es el componente del computador y otros dispositivos programables, que interpreta las instrucciones contenidas en los programas y procesa los datos.

DHCP: Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres.

DNS: Servicio o cualquier recurso conectado a Internet o a una red privada, Esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

Firewall: Un cortafuegos (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Gateway: Dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

Hardware: Corresponde a todas las partes tangibles de un sistema informático: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos.

Host: El término host es usado en informática para referirse a las computadoras conectadas a una red.

IP: Define la manera en que los paquetes de datos, también llamados datagramas, deben ser transportados entre el origen y el destino de una red.

Protocolo: Reglas usadas por computadoras para comunicarse unas con otras a través de una red.

Red: Red de ordenadores o red informática, es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos.

Servidor: Es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes

Software: Se conoce como software al equipamiento lógico o soporte lógico de un sistema informático; comprende el conjunto de los componentes necesarios que hacen posible la realización de tareas específicas.

Web: Sistema de distribución de información basado en hipertexto accesible a través de Internet. Con un navegador web, un usuario visualiza páginas web que pueden contener texto, imágenes, videos u otros contenidos multimedia.

IDS: Un **sistema** de **detección de intrusos (IDS)** es un dispositivo o aplicación de software que monitorea las actividades de red o del sistema para actividades

maliciosas o violaciones a las políticas y produce informes a una estación de administración

IPS: Un Sistema de Prevención de Intrusos (IPS) es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de *Prevención de Intrusos* es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos

Antivirus: son programas cuyo objetivo es detectar y/o eliminar virus informáticos

Filtro de Contenido: se refiere a un programa diseñado para controlar qué contenido se permite mostrar, especialmente para restringir el acceso a ciertos materiales de la Web.

QoS o **Calidad de Servicio:** (Quality of Service, en inglés) son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (throughput). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.

ADSL: (Asymmetric Digital Subscriber Line) es un tipo de tecnología de línea DSL. Consiste en una transmisión analógica de datos digitales apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado.

ATM: Modo de Transferencia Asíncrona o Asynchronous Transfer Mode (ATM) es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.