Universidad Tecnológica de El Salvador

FACULTAD DE INFORMÁTICA Y CIENCIAS APLICADAS

TÉCNICO EN INGENIERÍA DE HARDWARE

TEMA:

Instalación y Configuración de un Sistema Operativo que Funcione como Firewall para Protección de la Red en el Colegio la Asunción de San Salvador.

TRABAJO DE GRADUACIÓN PRESENTADO POR:

Jorge Alberto Henríquez Campos

Samuel Eduardo García García

PARA OPTAR AL GRADO DE:

Técnico En Ingeniería de Hardware

SEPTIEMBRE, 2016

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

PÁGINA DE AUTORIDADES

ING. NELSON ZÁRATE SÁNCHEZ

RECTOR

LIC. JOSÉ MODESTO VENTURA

VICERRECTOR ACADEMICO

ING. FRANCISCO ARMANDO ZEPEDA

DECANO

JURADO EXAMINADOR

ING. NUMA POMPILIO SUNCÍN AYALA

PRESIDENTE

LIC. OSCAR OBDULIO CHEVEZ ULLOA

PRIMER VOCAL

TEC. CARLOS ALBERTO NARVÁEZ MORÁN

SEGUNDO VOCAL

SEPTIEMBRE, 2016

SAN SALVADOR, EL SALVADOR, CENTROAMERICA

Universidad Tecnológica de El Salvador

ACTA DE EXAMEN PROFESIONAL

HABIÉNDOSE REUNIDO EL JURADO CALIFICADOR INTEGRADO POR:
Lic. Oscar Obdulio Chevez Ulloa Tec. Carlos Alberto Narváez, Ing. Numa Pompilio Suncin Ayala, a las 6:30a.m. del día Jueves, 23 de Junio de dos mil dieciséis.

Y LUEGO DE HABER DELIBERADO SOBRE EL EXAMEN PROFESIONAL DE LOS ALUMNOS:

1-Jorge Alberto Henriquez Campos Carnet 28-3347-2011
2-Samuel Eduardo García García Carnet 28-6299-2012

QUIENES PRESENTARON DEFENSA DE SU TRABAJO DE GRADUACION TITULADO:

"Instalación y configuración de un sistema Operativo que funcione como firewall para la protección de la Red en el Colegio la Asunción de San Salvador"

PARA OPTAR AL GRADO DE:

TÉCNICO EN INGENIERIA DE HARDWARE

Y DEL CUAL TAMBIEN EVALUARON LOS CONOCIMIENTOS RELACIONADOS CON EL TEMA DEL MISMO. POR LO QUE ESTE JURADO RESUELVE DECLARAR EL EXAMEN COMO:

APROBADO

YA QUE CUMPLE CON LOS REQUISITOS ESTABLECIDOS EN EL REGLAMENTO DE GRADUACION DE LA UNIVERSIDAD.

San Salvador, 23 de Junio de dos mil dieciséis.

F. _____
PRIMER VOCAL
Lic. Oscar Obdulio Chevez Ulloa

F. _____
SEGUNDO VOCAL
Tec. Carlos Alberto Narváez

F. _____
PRESIDENTE
Ing. Numa Pompilio Suncin Ayala

Índice

Introducción

El Colegio La Asunción de San Salvador, depende cada vez es más de su propia red informática y por un problema que le afecte puede interrumpir los servicios que en dicho colegio se presten.

Debido a ello, se propone instalar un Servidor Firewall basado en sistema operativo Linux, con una unidad del sistema (CPU) con características óptimas, que con el cual se hará ver cuáles son los riesgos que corren los laboratorios de informática al no tener el control de las páginas que se visitan.

Al igual se plantea una idea, con la cual se procura tener el control, con el fin de evitar que los alumnos/as pierdan el tiempo en hora de clase, en páginas de ocio o de contenido sexual y violencia explícita. Por lo que el firewall contará con un antivirus y anti-spyware, que analizará todo el tráfico de internet para evitar que ingresen virus y contenido no deseado a la red local.

Al mismo tiempo se brindará un manual impreso que facilite y oriente al usuario para la administración de las funciones básicas del servidor firewall, basado en el sistema operativo Linux.

También, se realizará un estudio de factibilidad técnica como económica de los productos que cumplan con los requisitos necesarios para la instalación del servidor firewall.

En el capítulo dos, se agrupan los conceptos y teorías que se utilizan para formular y desarrollar la tesis, con ideas básicas que ayudan a crear los argumentos; es una investigación basada en libros, documentos, artículos de revistas, artículos de periódicos, documentos de sitios web y en páginas web.

Las teorías desarrolladas, son utilizadas con el fin de proporcionar la solución con los productos que van a poner a funcionar el proyecto. Instalar y configurar un Servidor Firewall basado en sistema operativo Linux, con una unidad del sistema (CPU) con características óptimas, que con el cual se hará ver cuáles son los riesgos y vulnerabilidades que corren laboratorios de informática del Colegio La Asunción, al no tener el control de las páginas que se visitan. Al mismo tiempo se brindará un manual impreso que facilite y oriente al usuario para la administración de las funciones básicas del servidor firewall, basado sistema operativo Linux.

Este capítulo cuenta con un glosario, en donde son definidos los conceptos más importantes de la investigación. Aquí se enumeran ciertos términos de los que puede no haberse comprendido su significado; de este modo los lectores pueden comprender una forma más amplia el texto.

Luego, se describen las características técnicas que poseen cada uno de los productos para llevar a cabo el proyecto. Son seleccionados conforme a la evaluación técnica y económica; obtenidas de la página principal del fabricante o en su defecto, la página principal del producto.

En el capítulo tres, se describe la propuesta de la solución que se realizará para resolver el problema planteado, tomando en cuenta todos los productos integrados que van a ser la solución a través del prototipo o producto final.

En el presente capítulo tres se llega a una proposición final o conclusiones, después de hacer las consideraciones de la evidencia, el servidor Firewall con sistema base Linux Endian a pesar que es gratuito, es la solución para proteger la red local del Colegio La Asunción; ya que es fácil de instalar y usar; al guiarse por las instrucciones del manual de usuario y no requiere de dispositivos de Hardware muy robustos para su funcionamiento.

Las recomendaciones realizadas, son generadas a partir de las reflexiones, conclusiones o evaluaciones de la situación; el servidor Firewall con sistema operativo Endian, necesita un mantenimiento preventivo por parte del administrador de la red de dicho colegio para que continúe con el rendimiento óptimo y pueda servirle a las futuras generaciones. Sin dejar de mencionar, que se debe de adquirir un software firewall de paga ya que cuenta con más funciones que la versión gratuita y trae la asistencia de soporte técnico, de esta manera se tiene más opciones y beneficios en el control de la red.

Por último en dicho capitulo, se hace referencia de los textos utilizados como material de consulta o bibliografía para la investigación y la elaboración de la presente tesis.

Capítulo I Situación Actual

1. Situación Problemática

Actualmente, el Colegio La Asunción de San Salvador cada vez es más dependiente de su propia red informática y por un problema, por pequeño que sea y este le afecte puede llegar a interrumpir los servicios que se presten en dicho Colegio.

Debido a que hoy en día, la herramienta del internet representa una gran fuente de información ya que se encuentra prácticamente de todo como: consultar servicios que prestan las diferentes Instituciones de Gobierno, buscar un determinado libro en las bases de datos de muchas bibliotecas, Consultar periódicos y revistas, oír la radio, webcams, ver vídeos y al mismo tiempo permite al acceso a páginas web con contenido sexual y violencia explícita; por lo que es necesario la seguridad de la red del Colegio La Asunción, que comprende el Hardware y Software de cada dispositivo, así como también, la integridad y confidencialidad de los datos como: publicación de calificaciones, pagos de colegiatura, evaluaciones docentes y actualización de antivirus entre otros, que circulan en ella.

El Colegio La Asunción, cuenta con dos laboratorios de informática con el acceso a internet restringido, es decir que los alumnos y alumnas no pueden accesar a cualquier sitio por internet, es por ello, que no logran visitar páginas de ocio, de violencia explícita y sitios web con contenido sexual, entre otras. Por contar con servicio denominado Open DNS, pero el problema es que la dirección IP es asignada por DHCP por el proveedor de internet es decir que se modifica la IP en ocasiones y se pierden las configuraciones

asignadas a la IP en el servicio Open DNS, En ese momento los estudiantes pueden accesar a cualquier tipo de información. Hasta que se actualicen las configuraciones en la nueva IP asignada por el proveedor de Internet.

Otra situación que se debe tomar en cuenta, que la red WIFI del Colegio La Asunción no puede ser controlada o no puede ser filtrado el contenido al cual pueden accesar.

Es por esto, que también dificulta la detección y corrección de muchos y variados problemas de seguridad que van surgiendo. Dentro de esta variedad, van aumentando acciones que irrespetan la privacidad y propiedad de los recursos y sistemas informáticos. Crackers, hackers, entre otros, están formando parte del vocabulario ordinario de los alumnos, alumnas y del administrador de la red cada vez más.

Es responsabilidad del administrador de la red del Colegio La Asunción, estar en la búsqueda constante de riesgos y vulnerabilidades que existan en la red de datos, y en la mayoría de casos ni siquiera sabe cómo empezar, que preguntar o que investigar.

2. Enunciado del Problema

¿Será necesario instalar y configurar un Servidor Firewall, para evitar riesgos y vulnerabilidades en la red del Colegio La Asunción?

3. Justificación

El Colegio La Asunción no cuenta con la seguridad y control necesario de la red informática, no cuenta con un filtrado o analizador web y mucho menos con un firewall que los proteja de un ataque externo, además las páginas web que se visitan dentro de los laboratorios de dicho Colegio solo son restringidas por un software llamado Open DNS con el cual se puede bloquear las páginas web por categoría, pero es poco eficiente, ya que cuando cambia la ip del proveedor de servicio pierde la configuración y las computadoras de los laboratorios del Colegio navegan libremente sin ninguna restricción por internet, solo hasta que el administrador de red vuelve a configurar el software Open DNS queda restringido nuevamente el internet.

También el servicio WIFI dentro del Colegio no está controlado, si cuenta con contraseña para poder acceder a internet, pero no se tiene control sobre ella, el administrador de la red del mencionado Colegio debe de estar pendiente de las ip asignada por los routers que brindan el servicio wifi y de esta manera bloquear las direcciones ip que no deberían de tener el acceso a internet.

Es por ello que se considera necesario, seleccionar una unidad del sistema (CPU) con características óptimas para implementar un servidor Firewall, con Sistema Operativo basado en Linux libre; que brindará políticas de seguridad para prevenir riesgos y vulnerabilidades y minimizar los mismos, en la red del Colegio la Asunción de San Salvador. El servidor firewall evitará que los alumnos y alumnas corran riesgos a la hora de navegar por internet, al visitar sitios web con contenido educativo; eso traerá

beneficios en la eficiencia de los alumnos y alumnas en el proceso de aprendizaje, y a la vez mantendrá segura la red local.

Por todo lo antes expuesto, se instalará un Servidor Firewall basado en Linux, el cual estará configurado para que las computadoras de los laboratorios de informática del Colegio la Asunción, no tengan acceso total a internet y evitar de esta manera páginas de ocio, violencia, y con contenido sexual, etcétera. Solo permitiendo el acceso a páginas de contenido educativo en internet.

Es importante mencionar, que el servidor firewall, incluye productos como: un antispyware, que protegerá a los equipos de cómputo contra spyware y otro software potencialmente no deseado; y también cuenta con antivirus, que analizará todo el tráfico de los sitios web que se visiten en internet, para evitar que ingresen virus a la red local.

Y al mismo tiempo, se brindará un manual de usuario del Servidor Firewall basado en Linux, al administrador de la red del referido Colegio, para que se le haga más sencillo detectar los riesgos y vulnerabilidades en la red local y pueda minimizar los mismos. Y a la vez, pueda controlar el tráfico de los sitios que se visiten por internet.

4. Objetivos

4.1 General:

Identificar e Instalar un sistema operativo que funcione como firewall, para la protección de la red del Colegio La Asunción de San Salvador.

4.2 Específicos:

- Seleccionar una Unidad del Sistema (CPU) con las características óptimas, que funcionará como servidor firewall.
- Utilizar y configurar un sistema operativo basado en Linux, para controlar el tráfico de los sitios que se visiten por internet, y que cuente con antivirus y anti-spyware.
- Crear un instrumento al administrador de la red del Colegio La Asunción, para la administración de funciones básicas del servidor firewall.

5. Delimitaciones

5.1 Geográfica

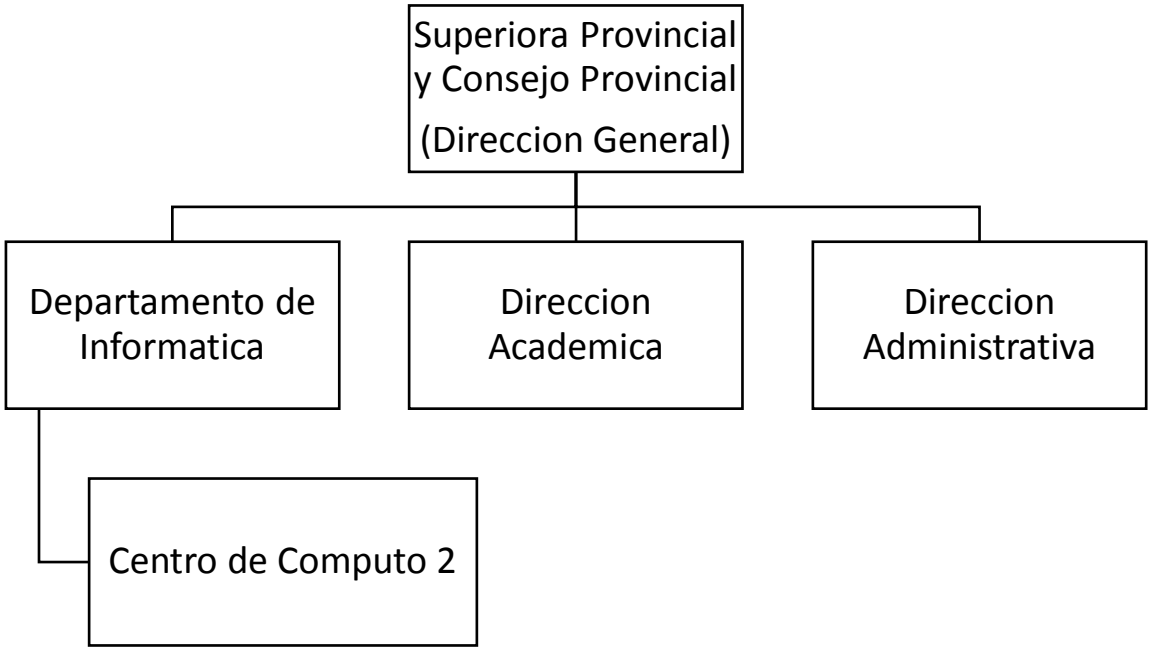
La investigación del proyecto se realizará en el Colegio La Asunción, que está sobre 21 avenida norte y 1ra calle poniente, San Salvador, El Salvador.

5.2 Temporal

El tiempo en que se realizará la investigación será de 36 días, será de la fecha 5 de marzo al 10 de junio del 2016.

5.3 Organizacional

A continuación se presenta el diagrama de la estructura organizativa donde se implementará el proyecto:



6. Alcances

Promesa	**Producto**
Una PC de características óptimas que funcionará como servidor firewall.	Una unidad del sistema (CPU), con 12GB de memoria RAM, disco duro de 500GB, 2 tarjetas de Red alámbricas, procesador Dual Core 3.2GHZ, teclado y mouse. Será de acuerdo a su análisis técnico y económico.
Utilizar y configurar un sistema operativo basado en Linux, para controlar el tráfico de los sitios que se visiten por internet, y que cuente con antivirus y anti-spyware.	Sistema operativo Endian.
Crear un instrumento al usuario para la administración de funciones básicas del servidor firewall.	Un manual impreso de la configuración básica del sistema operativo Endian.

7. Estudio de Factibilidad

7.1 Factibilidad económica

Cuadro de Evaluación Económico Producto "Motherboard"			
Nombre del Producto	Motherboard MSI H61MGV3	Motherboard BIOSTAR B85M-GR2.0	Motherboard BIOSTAR H81MLV3
Precios	$58.95	$65.00	$54.00
Análisis	Se optará por el producto H81MLV3, proveedor Tecnoservice, por ser el más económico, ya que cumple con los requisitos necesarios para la instalación del servidor firewall.		
Establecimiento	R.G NIETO	INNOVATEK	Tecnoservice

Cuadro Económico N°1

Cuadro de Evaluación Económico Producto "Disco Duro"			
Nombre del Producto	SEGATE BARRACUDA 500GB	SEGATE BARRACUDA 500GB	TOSHIBA DE 500GB
Precios	$72.75	$75.00	$54.00
Análisis	Se optará por el producto TOSHIBA DE 500GB, proveedor Tecnoservice, por tener el precio más factible, ya que cumple con los requisitos necesarios para la instalación del servidor firewall.		
Establecimiento	R.G NIETO	INNOVATEK	Tecnoservice

Cuadro Económico N°2

Cuadro de Evaluación Económico Producto "Procesadores"			
Nombre del Producto	INTEL DUAL CORE 3.2 GHz	INTEL I3-4170 CORE 3.2GHz	INTEL DUAL CORE 3.2GHZ
Precios	$81.95	$85.00	$ 73.50
Análisis	Se seleccionó el producto INTEL DUAL CORE 3.2GHZ, proveedor Tecnoservice, por tener el precio más accesible, ya que cumple con los requisitos necesarios para la instalación del servidor firewall.		
Establecimiento	R.G NIETO	INNOVATEK	Tecnoservice

Cuadro Económico N°3

Cuadro de Evaluación Económico Producto "Memoria RAM"			
Nombre del Producto	DDR3 1333 12GB Kingston	DDR3 12800 12GB Kingston	DDR3 1333 12GB Kingston
Precios	$96.00	$110.00	$87.00
Análisis	Se escogió el producto DDR3 1333 12GB Kingston, proveedor Tecnoservice, por ser más económico, ya que cumple con los requisitos necesarios para la instalación del servidor firewall.		
Establecimiento	R.G NIETO	INNOVATEK	Tecnoservice

Cuadro Económico N°4

Cuadro de Evaluación Económico Producto "Tarjeta de Red Alámbrica"			
Nombre del Producto	Nexxt 100Mbps	D-link 100Mbps	Nexxt 100Mbps
Precios	$13.00	$15.00	$10.50
Análisis	Se seleccionó el producto Nexxt 100Mbps, proveedor Tecnoservice, por ser el más económico, ya que cumple con los requisitos necesarios para la instalación del servidor firewall.		
Establecimiento	R.G NIETO	INNOVATEK	Tecnoservice

Cuadro Económico N°5

Cuadro de Evaluación Económico Producto "Software Distribuciones gratuitas"			
Producto	Smothwall	Clearos	Endian
Precios	$ -	$ -	$ -
Análisis	Se optará el producto Endian por ser gratuito, porque cumple con los requisitos necesario para la instalación del servidor firewall, Sistema basado en Linux, en el cual se hacen las configuraciones a través de una interfaz web, teniendo el servicio de firewall, antivirus, anti-spyware, usuario VPN, es la versión gratuita más completa.		
Establecimiento	http://www.smoothwall.org/download/	https://www.clearfoundation.com/#clearfoundation-overview	http://www.endian.com/community/overview/

Cuadro Económico N°6

Cuadro de Evaluación Económico Producto "Case"			
Nombre del Producto	Omega	Starview hy-28	Genérico
Precios	$32.50	$45.00	$34.50
Análisis	Se escogió el producto Omega, proveedor R.G NIETO, por tener el precio más accesible, ya que cumple con los requisitos necesarios para la instalación del servidor firewall.		
Establecimiento	R.G NIETO	INNOVATEK	Tecnoservice

Cuadro Económico N°7

7.2 Factibilidad técnica

Cuadro Técnico N°1

Cuadro de evaluación Producto "Motherboard" se requiere un nivel de calificación del 90 %							
característica técnica	**ponderación**	**H61MGV3**		**B85M-GR2.0**		**H81MLV3**	
		valor	**total**	**valor**	**total**	**valor**	**total**
soporta 12gb de RAM como mínimo	40.00%	1	40.00%	2	80.00%	2	80.00%
soporta procesador dual Core socket 1150	40.00%	1	40.00%	2	80.00%	2	80.00%
soporta discos duros SATA de 500gb mínimo	20.00%	2	40.00%	2	40.00%	1	20.00%
Total	100.00%		120.00%		200.00%		180.00%
	% Final		**60.00%**		**100.00%**		**90.00%**
Análisis	Se optará por el producto H81MLV3, proveedor Tecnoservice, porque cumple con las Características Técnicas necesarias para la instalación del servidor firewall.						

Valor 0 = No aplica.

Valor 1 = Aplica a Medias.

Valor 2 = Aplica en Totalidad.

Cuadro Técnico N°2

Cuadro de evaluación Producto "Procesadores" se requiere un nivel de calificación del 100 %							
característica técnica	**ponderación**	**INTEL DUAL CORE 3.2 GHz**		**INTEL I3-4170 CORE 3.2GHz**		**INTEL DUAL CORE 3.2GHZ**	
		valor	**total**	**valor**	**total**	**valor**	**total**
Frecuencia de Reloj 3.2Ghz como mínimo.	70.00%	2	140.00%	2	140.00%	2	140.00%
debe de ser Socket 1150	20.00%	0	0.00%	2	40.00%	2	40.00%
Procesador Intel Pentium	10.00%	2	20.00%	2	20.00%	2	20.00%
Total	100.00%		160.00%		200.00%		200.00%
	% Final		**80.00%**		**100.00%**		**100.00%**
Análisis	Se seleccionó el producto INTEL DUAL CORE 3.2GHZ, proveedor Tecnoservice, porque cumple con las Características Técnicas necesarias para la instalación del servidor firewall.						

Valor 0 = No aplica.

Valor 1 = Aplica a Medias.

Valor 2 = Aplica en Totalidad.

Cuadro Técnico N°3

Cuadro de evaluación Producto "RAM" se requiere un nivel de calificación del 80 %							
característica técnica	**ponderación**	**DDR3 1333 12GB**		**DDR3 12800 12GB**		**DDR3 1333 12GB**	
		valor	**total**	**valor**	**total**	**valor**	**total**
Velocidad de 12Gb como mínimo	75.00%	1	75.00%	2	150.00%	2	150.00%
Bus de dato de 1333, como mínimo	15.00%	2	30.00%	2	30.00%	2	30.00%
debe de ser RAM DDR3	10.00%	2	20.00%	2	20.00%	2	20.00%
Total	100.00%		125.00%		200.00%		200.00%
	% Final		**62.50%**		**100.00%**		**100.00%**
Análisis	Se escogió el producto DDR3 1333 12GB, proveedor Tecnoservice, porque cumple con las Características Técnicas necesarias para la instalación del servidor firewall.						

Valor 0 = No aplica.

Valor 1 = Aplica a Medias.

Valor 2 = Aplica en Totalidad.

Cuadro Técnico N°4

Cuadro de evaluación Producto "Disco Duro" se requiere un nivel de calificación del 70 %							
característica técnica	**ponderación**	**SEGATE BARRACUDA 500GB**		**SEGATE BARRACUDA 500GB**		**TOSHIBA DE 500GB**	
		valor	**total**	**valor**	**total**	**valor**	**total**
Capacidad de 500GB	50.00%	2	100.00%	2	100.00%	1	50.00%
velocidad de 7200 rpm	40.00%	2	80.00%	2	80.00%	2	80.00%
Interface SATA	10.00%	2	20.00%	2	20.00%	2	20.00%
Total	100.00%		200.00%		200.00%		150.00%
	% Final		**100.00%**		**100.00%**		**75.00%**
Análisis	Se optará por el producto TOSHIBA DE 500GB, proveedor Tecnoservice, porque cumple con las Características Técnicas necesarias para la instalación del servidor firewall.						

Valor 0 = No aplica.

Valor 1 = Aplica a Medias.

Valor 2 = Aplica en Totalidad.

Cuadro Técnico N°5

Cuadro de evaluación Producto "Tarjeta de Red Alámbrica" se requiere un nivel de calificación del 70 %							
característica técnica	**ponderación**	**Nexxt 100Mbps**		**D-link 100 Mbps**		**Nexxt 100Mbps**	
		valor	**total**	**valor**	**total**	**valor**	**total**
Transferencia de 100Mbps	40.00%	2	80.00%	2	80.00%	2	80.00%
Tarjeta ranura PCI	30.00%	2	60.00%	2	60.00%	2	60.00%
Compatibilidad con S.O Linux	30.00%	2	60.00%	2	60.00%	2	60.00%
Total	100.00%		200.00%		200.00%		200.00%
	% Final		**100.00%**		**100.00%**		**100.00%**
Análisis	Se eligió el producto Nexxt 150Mb/s, proveedor Tecnoservice, porque cumple con las Características Técnicas necesarias para la instalación del servidor firewall.						

Valor 0 = No aplica.

Valor 1 = Aplica a Medias.

Valor 2 = Aplica en Totalidad.

Cuadro Técnico N°6

Cuadro de evaluación Producto "Case" se requiere un nivel de calificación del 60 %							
característica técnica	**ponderación**	**Omega**		**Starview hy-28**		**Genérico**	
		valor	**total**	**valor**	**total**	**valor**	**total**
Fuente de 550 Watts	50.00%	1	50.00%	2	100.00%	1	50.00%
Puertos USB Delanteros	20.00%	0	0.00%	1	20.00%	2	40.00%
Case metálico, polarizado.	20.00%	2	40.00%	2	40.00%	2	40.00%
Total	90.00%		90.00%		160.00%		130.00%
	% Final		**45.00%**		**80.00%**		**65.00%**
Análisis	Se seleccionó el producto Omega, proveedor R.G NIETO, porque cumple con las Características Técnicas necesarias para la instalación del servidor firewall. Incluye también teclado, mouse y bocinas.						

Valor 0 = No aplica.

Valor 1 = Aplica a Medias.

Valor 2 = Aplica en Totalidad.

Cuadro Técnico N°7

Cuadro de evaluación Producto "Sistema Operativo" se requiere un nivel de calificación del 100 %							
característica técnica	**ponderación**	**Smothwall**		**Clearos**		**Endian**	
		valor	**total**	**valor**	**total**	**valor**	**Total**
Bloque de páginas Web por categorías o especificas	70.00%	1	70.00%	1	70.00%	2	140.00%
Anti-virus	15.00%	1	15.00%	1	15.00%	2	30.00%
Anti-Spyware	15.00%	0	0.00%	0	0.00%	2	30.00%
Total	100.00%		85.00%		85.00%		200.00%
	% Final		**42.50%**		**42.50%**		**100.00%**
Análisis	Se escogió el producto Endian, porque cumple con las Características Técnicas necesarias para la instalación del servidor firewall.						

Valor 0 = No aplica.

Valor 1 = Aplica a Medias.

Valor 2 = Aplica en Totalidad.

7.3 Análisis general de factibilidades

De acuerdo con el análisis realizado tanto de factibilidad económica como técnica, estos son los dispositivos recomendados para llevar a cabo dicho proyecto:

Análisis de la Factibilidad de la Motherboard:

Se ha escogido el modelo H81MLV3 BIOSTAR, por su buen precio, ya que cuenta con las características técnicas necesarias, como son: un socket 1150, que soporta procesadores Pentium i3, i5 y i7, con garantía de 12 meses y soporta 16GB de memoria RAM, lo suficiente para soportar el sistema operativo Firewall Endian.

Análisis de la Factibilidad del Procesador:

Se ha elegido el procesador Intel Dual Core 3.2GHZ, ya que es el que resulta más económico, a la vez cumple con las características técnicas demandadas, el Procesador dual Core de 3.2Ghz, de socket 1150, 3mb de memoria cache, 12 meses de garantía.

Análisis de la Factibilidad de la Memoria RAM:

Se ha optado por dos memorias RAM Kingston, por su precio más accesible, cumplen con las características técnicas demandadas, el cual será una memoria RAM de 12GB, con un bus de datos de 1333MHZ, lo suficiente para tener en óptimo funcionamiento el servidor Firewall.

Análisis de la Factibilidad del Disco Duro:

Se ha escogido el disco duro THOSIBA de 500GB, por su buen precio, cumple con las características técnicas demandadas, el disco duro es de 7200 rpm, con interfaz SATA garantía 12 meses.

Análisis de la Factibilidad del Case:

Se ha optado por uno Genérico, ya que es el que ha resultado mejor evaluado en el cuadro de factibilidad económica, cumple con las características técnicas demandadas, el case es de aluminio y cuenta con una fuente de 550W, teclado, mouse, y bocinas.

Análisis de la Factibilidad del Sistema operativo Firewall:

Se ha seleccionado el sistema operativo Endian, de distribución OpenSource, que de acuerdo a las características técnicas es el mejor evaluado, Endian es un sistema basado en Linux, en el cual se hacen las configuraciones, y se tiene el monitoreo a través de una interfaz web, Endian tiene el servicio de firewall, antivirus, anti-spyware, entre otras cosas más.

Análisis de la Factibilidad de la Tarjeta de Red Alambrica:

Nexxt Siruis 1000 con una velocidad de 150 mb/s, por su precio más accesible, de acuerdo a las características técnicas es el mejor evaluado, incorpora un módulo de chips de avanzada tecnología para facilitar su instalación y garantizar la integración fluida de todos sus componentes. Con un extenso número de controladores, la tarjeta es capaz de funcionar con los sistemas operativos mayormente utilizados en la actualidad.

Cuadro de Factibilidad General			
Nombre y Modelo Producto	**Cumple Factibilidad Económica**	**Cumple Factibilidad Técnica**	**Observaciones**
Motherboard BIOSTAR H81MLV3	Si	Si	Por su buen precio, ya que cuenta con las características técnicas necesarias, como son: un socket 1150, que soporta procesadores Pentium i3, i5 y i7, con garantía de 12 meses y soporta 16GB de memoria RAM, lo suficiente para soportar el sistema operativo Firewall Endian.
Micro Procesador Intel Dual Core 3.2GHZ	Si	Si	Ya que es el que resulta más económico, a la vez cumple con las características técnicas demandadas, el Procesador dual Core de 3.2Ghz, de socket 1150, 3mb de memoria caché, con 12 meses de garantía.
Memoria RAM Kingston 12GB	Si	Si	Por su precio más accesible, cumplen con las características técnicas demandadas, el cual será una memoria RAM de 12GB, con un bus de datos de 1333MHZ, lo suficiente para tener en óptimo funcionamiento el servidor Firewall.
Disco Duro Toshiba	Si	Si	Por su buen precio, cumple con las características técnicas demandadas, el

Barracuda de 500GB			disco duro es de 7200 rpm, con interfaz SATA garantía 12 meses.
Case Genérico	Si	Si	Ya que es el que ha resultado mejor evaluado en el cuadro de factibilidad económica, cumple con las características técnicas demandadas, el case es de aluminio y cuenta con una fuente de 550W, teclado, mouse, y bocinas.
Tarjeta Red Alámbrica Nexxt Siruis	Si	Si	Con una velocidad de 150 Mb/s, por su precio más accesible, de acuerdo a las características técnicas es el mejor evaluado, incorpora un módulo de chips de avanzada tecnología para facilitar su instalación y garantizar la integración fluida de todos sus componentes. Con un extenso número de controladores, la tarjeta es capaz de funcionar con los sistemas operativos mayormente utilizados en la actualidad.
Sistema Operativo Endian Firewall	Si	Si	Se ha seleccionado el sistema operativo Endian, de distribución OpenSource, que de acuerdo a las características técnicas es el mejor evaluado, Endian es un sistema basado en Linux, en el cual se hacen las configuraciones, y se tiene el monitoreo a través de una interfaz web, Endian tiene el servicio de firewall, antivirus, anti-spyware, entre otras cosas más.

8. Carta de Aceptación

Colegio La Asunción
San Salvador

San Salvador, 11 de marzo del 2016

A Quien Corresponda
Universidad Tecnológica de El Salvador

Por medio de la presente hacemos constar que aceptamos la realización del proyecto: **Instalación y Configuración de un equipo informático que funcione como Firewall**, que se desarrollara en nuestra institución por los estudiantes: **Samuel Eduardo García y Jorge Alberto Henríquez**; estudiantes de la carrera Técnico en Ingeniería de Hardware de la Universidad Tecnológica de El Salvador.

La Aportación de ambas partes será del 50% del costo económico de dicho proyecto. Aceptamos y a la vez agradecemos el Equipo del Proyecto que quedará dentro de nuestra institución como una donación realizada por los estudiantes antes mencionados.

A los once días del mes de marzo de dos mil dieciséis en la ciudad de San Salvador.

F._____

Madre Ethel María Saavedra Montoya
Directora General
Colegio La Asunción

CORPORACIÓN LA ASUNCIÓN

Capítulo II Documentación Técnica

1. Marco Teórico de Referencia

1.1 Breve historia del término firewall

El término "firewall / fireblock" significaba originalmente una pared para confinar un incendio o riesgo potencial de incendio en un edificio. Más adelante se usa para referirse a las estructuras similares, como la hoja de metal que separa el compartimiento del motor de un vehículo o una aeronave de la cabina. La tecnología de los cortafuegos surgió a finales de 1980, cuando Internet era una tecnología bastante nueva en cuanto a su uso global y la conectividad. Los predecesores de los cortafuegos para la seguridad de la red fueron los routers utilizados a finales de 1980, que mantenían a las redes separadas unas de otras. La visión de Internet como una comunidad relativamente pequeña de usuarios con máquinas compatibles, que valoraba la predisposición para el intercambio y la colaboración, terminó con una serie de importantes violaciones de seguridad de Internet que se produjo a finales de los 80. (Edward, 2012)

1.2 Principios de seguridad en las redes

Actualmente, las empresas cada vez son más dependientes de sus propias redes informáticas y por un problema, por pequeño que sea y les afecte puede llegar a interrumpir las operaciones que se realicen en dicha organización. (Cruz & Rodríguez, D.D.V, 2010)

Hoy en día, la herramienta del internet representa una gran fuente de información por lo que es necesario la seguridad de la red que comprende el Hardware y Software de cada

dispositivo así como también la integridad y confidencialidad de los datos que circulan en ella. (Cruz & Rodríguez, D.D.V, 2010)

La falta de seguridad en las redes informáticas, es un problema que va en crecimiento. Cada vez el número de atacantes es mayor y se están organizando cada día y van adquiriendo muchas habilidades que les permiten obtener los objetivos que se proponen. Tampoco se debe de subestimar las fallas de seguridad que provienen dentro de dicha organización. (Cruz & Rodríguez, D.D.V, 2010)

La complejidad de una red dificulta la detección y corrección de muchos y variados problemas de seguridad que van surgiendo. Dentro de esta variedad, van aumentando acciones que irrespetan la privacidad y propiedad de los recursos y sistemas informáticos. Crackers, hackers, entre otros, están formando parte del vocabulario ordinario de usuarios y administradores de redes cada vez más. (Cruz & Rodríguez, D.D.V, 2010)

Aparte de métodos como la Criptografía, un punto importante que se debe de mencionar para la protección de los sistemas es la constante atención y vigilancia de los responsables de la red como es el administrador de la misma y que hoy por hoy no se preocupa demasiado de la seguridad de dicha red; todos las vulnerabilidades y riesgos que puedan existir en la misma y cuando llegan a tener problemas, el tiempo que pueda utilizar es mucho mayor que el que podría demorar si contara con un modelo, política o procedimiento para el uso correcto de los sistemas informáticos. (Cruz & Rodríguez, D.D.V, 2010)

Otro gran problema de los administradores de la red, es el implementar parches con esto se hace referencia al instalar programas que disminuyen el rendimiento de los equipos de cómputo en vez de atacar el problema que origina debilidad en la red. (Cruz & Rodríguez, D.D.V, 2010)

Es responsabilidad del administrador de la red estar en la búsqueda constante de riesgos y vulnerabilidades que existan en la red de datos, y en la mayoría de casos ni siquiera sabe cómo empezar, que preguntar o que investigar. (Cruz & Rodríguez, D.D.V, 2010)

Sin la búsqueda de riesgos y vulnerabilidades, las empresas crean una idea errónea de su seguridad, creen que la seguridad de su propia información es poco vulnerable, porque nunca se han visto afectados o puede ser que no sepan de eso. (Cruz & Rodríguez, D.D.V, 2010)

Es por ello, que es de mucha importancia abordar el tema de seguridad en las redes ya que un fallo en ellas puede resultar muy costoso en productividad, eficiencia, perdida de datos confidenciales e información valiosa y para proteger tal información de dichas organizaciones es recomendable el uso de dispositivos de Hardware o software que ayuden a detectar vulnerabilidades y riesgos que puedan surgir en dicha red y también de esta manera poder minimizar los mismos. (Cruz & Rodríguez, D.D.V, 2010)

La ubicación habitual de un firewall (geekland, 2016), es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protegen los sistemas internos de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los mismos.

1.3 Función de un firewall

Básicamente la función de un firewall es proteger los equipos individuales, servidores o equipos conectados en red contra accesos no deseados de intrusos que pueden robar datos confidenciales y hacer perder información valiosa.

Así por lo tanto queda claro que es altamente recomendable utilizar un firewall por los siguientes motivos:

1. Para preservar seguridad y privacidad.

2. Para proteger la red doméstica o empresarial.

3. Para tener a salvo la información almacenada en la red, servidores u ordenadores.

4. Para evitar intrusos no deseados en la red y ordenador. Los usuarios no deseados pueden ser hackers como usuarios pertenecientes a la misma red.

Por lo tanto un firewall debidamente configurado puede proteger, por ejemplo la red de virus cuando se navegue por internet.

Lo primero que se debe de saber es que para conocer el funcionamiento de un firewall es que la totalidad de información y tráfico que pasa por el router y que se transmite en la red es analizado por el firewall en la red.

Si el tráfico cumple con las reglas que se han configurado en el firewall el tráfico podrá entrar o salir de la red.

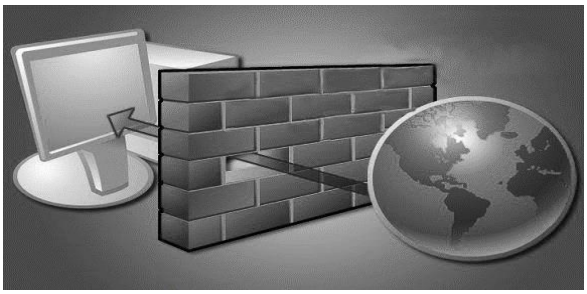


Figura N° 1, Entrada de la información a través de internet.

http://geekland.eu/que-es-y-para-que-sirve-un-firewall/

Si el tráfico no cumple con las reglas que se han configurado en los firewall entonces el tráfico se bloqueará no pudiendo llegar a su destino.

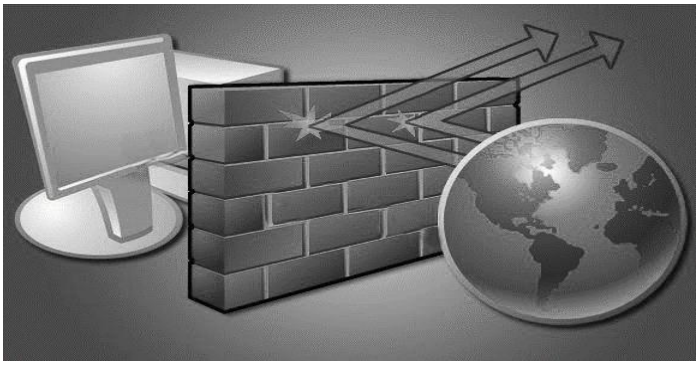


Figura N° 2, Bloqueo de la información hacia la red.
http://geekland.eu/que-es-y-para-que-sirve-un-firewall/

1.4 Tipos de reglas que se pueden implementar en un firewall

El tipo de reglas y funcionalidades que se pueden construir en un firewall son las siguientes:

1. Administrar los accesos de los usuarios a los servicios privados de la red como por ejemplo aplicaciones de un servidor.

2. Registrar todos los intentos de entrada y salida de una red.

3. Filtrar paquetes en función de su origen, destino, y número de puerto. Esto se conoce como filtro de direcciones. Así por lo tanto con el filtro de direcciones se puede bloquear o aceptar el acceso al equipo de la IP 192.168.1.125 a través del puerto específico.

4. Filtrar determinados tipos de tráfico en la red. Esto también se conoce como filtrado de protocolo. El filtro de protocolo permite aceptar o rechazar el tráfico en función del protocolo utilizado. Distintos tipos de protocolos que se pueden utilizar son http, https, TCP, UDP, SSH, FTP, etc.

5. Controlar el número de conexiones que se están produciendo desde un mismo punto y bloquearlas en el caso que superen un determinado límite.

6. Controlar las aplicaciones que pueden acceder a Internet. Así por lo tanto restringir el acceso a ciertas aplicaciones, como por ejemplo dropbox, a un determinado grupo de usuarios.

7. Detección de puertos que están en escucha y en principio no deberían estarlo. Así por lo tanto el firewall puede advertir que una aplicación quiere utilizar un puerto para esperar conexiones entrantes.

1.5 Limitaciones de los firewall

Un Servidor Firewall dispone de una serie de limitaciones. Las limitaciones principales de un firewall son las siguientes:

1. Un firewall en principio es probable que no pueda proteger la red contra ciertas vulnerabilidades internas. Por ejemplo cualquier usuario puede borrar el contenido de un ordenador sin que el firewall lo evite, introducir un USB en el ordenador y robar información, etcétera.

2. El firewall solo puede proteger la red frente a los ataques que atraviesan el firewall. Por lo tanto no puede repeler la totalidad de ataques que puede recibir la red o servidor.

1.6 Los firewall por hardware y software comercial

El firewall por software se instala directamente en los ordenadores o servidores que se van a proteger y solo protegen el ordenador o servidor en que se ha instalado.

Un firewall comercial funciona de la misma forma que uno gratuito (como el de Windows), pero normalmente incluye protecciones extra y mucho más control sobre su configuración y funcionamiento. (INFORMATICAHOY, 2016)

El firewall exclusivamente o como parte de un paquete de seguridad que incluye otros productos que complementan esta protección, como es el caso de los antivirus.

Un firewall por hardware se configura generalmente mediante una interfaz web, utilizando el mismo navegador que el usuario utiliza para conectarse a Internet. Este tipo de sistema ya viene instalado en los routers de acceso a Internet, con lo cual las máquinas que lo utilicen estarán protegidas. (Guías Prácticas.COM, 2016)

En cualquier caso, es poco probable que un firewall pueda identificar a un programa malicioso, virus o gusano, ya que no está diseñado para esa función, por lo que debe trabajar conjuntamente con un antivirus y antispyware.

1.7 Tipos de manuales

Los Manuales: Son textos utilizados como medio para coordinar, registrar datos e información en forma sistémica y organizada. También es el conjunto de orientaciones o instrucciones con el fin de guiar o mejorar la eficacidad de las tareas a realizar. (TiposDe.Org , 2016)

Manual Múltiple: estos manuales están diseñados para exponer distintas cuestiones, como por ejemplo normas de la empresa, más bien generales o explicar la organización de la empresa, siempre expresándose en forma clara. (TiposDe.Org , 2016)

Manual del Sistema: debe ser producido en el momento que se va desarrollando el sistema. Está conformado por otro grupo de manuales. (TiposDe.Org , 2016)

Manual de Finanzas: tiene como finalidad verificar la administración de todos los bienes que pertenecen a la empresa. Esta responsabilidad está a cargo del tesorero y el controlador. (TiposDe.Org , 2016)

Manual de Organización: es un documento normativo que permite conocer la estructura orgánica de la Dependencia o Entidad en su conjunto o parte de ella. Además define concretamente las funciones encomendadas a cada una de las áreas que integran la institución. Así, como también; describe funciones y departamentos de una organización, implementa las tareas específicas y la autoridad asignadas a miembro del

organismo. Un manual de organización especifica de forma más detallada la información que presenta y diseña el organigrama. (Slide Share.net, 2013)

Manual Departamental: este tipo de manual contiene las informaciones de cómo es legislada una empresa y de cómo se deben de realizar las funciones de cada área. (MasTiposde.com, 2016)

Manual de Política: en una empresa, este tipo de manuales detalla la forma en que esta está dirigida. (MasTiposde.com, 2016)

Manuales de Procedimientos: contiene información de la continuidad cronológica y secuencial de operaciones entrelazadas entre sí. Esto ayuda a la realización de cada función, tarea y actividad específicamente de la empresa. Se conocen también como Manuales de Normas y detalla las asignaciones de rutina por medio a los procedimientos en este indicado, siguiendo una secuencia lógica y organizadamente compuesto. Tiene como objetivo final controlar y unificar cada rutina diaria en las labores y así evitar al máximo cualquier tipo de alteraciones arbitrarias. (MasTiposde.com, 2016)

Manual de Técnicas: este tipo de manual detalla cómo deben ser realizadas las tareas particulares y trata acerca de las diferentes técnicas, tal como refiere su nombre. (MasTiposde.com, 2016)

Manual de puestos: es un instrumento de la Administración de los Recursos Humanos, que indica las funciones y actividades a ser cumplidas por los miembros de la Institución y la forma en que las mismas deberán ser realizadas ya sea, conjunta o Individualmente. (MasTiposde.com, 2016)

Manual de calidad: es un documento público que las empresas ponen a disposición de clientes, usuarios, proveedores e instituciones para que conozcan, se ajusten y supervisen respectivamente los estándares de calidad con los que la compañía se ha comprometido. (Retos en Supply Chain , 2014)

Ventajas de los manuales:

- Permiten al usuario tener una guía o tutorial.
- Facilitan el uso y aprendizaje.
- Son herramientas sin costo.
- Permite tener una información secuencial.
- Facilitan mucho una tarea
- Permite dar a conocer diferentes programas. (Google Sites, 2011)

1.8 Manual de usuario

El manual de usuario es un documento técnico de un determinado sistema que intenta dar asistencia a sus usuarios. Los manuales de usuario generalmente son incluidos a dispositivos hardware de computadora y aplicaciones. El manual de usuario puede venir tanto en forma de libro como en forma de documento digital, e incluso poder ser consultado por internet.

En general, un manual de usuario debería poder ser entendido por cualquier usuario principiante, como así también serle útil a usuarios avanzados. (Alegsa, 2010)

Un manual de usuario suele tener:

* Un prefacio, con información sobre cómo usar el propio manual.

* Un índice.

* Una guía rápida sobre cómo usar las funciones principales del sistema.

* Una sección para la resolución de problemas.

* Información de contacto.

* Una FAQ (Preguntas Frecuentes)

* Un glosario. (Alegsa, 2010)

2. Marco Teórico de la Solución

2.1 Unidad del sistema

La calidad de los dispositivos internos de un ordenador ha venido evolucionado de gran manera, al punto que se puede instalar sistemas operativos con grandes avances tecnológicos y ejecutar muchas tareas a la vez. Una unidad del sistema (CPU) con 12GB de memoria RAM, disco duro de 500GB, dos tarjetas de Red alámbricas Nexxt Siruis 1000 con una velocidad de 150 mb/s, con procesador Dual Core 3.2GHZ, case genérico, de aluminio y cuenta con una fuente de 550W, teclado, mouse, y bocinas; son requisitos del sistema para la instalación del Servidor Firewall.

2.2 Sistema operativo Endian

Encontrar una forma de utilizar mejor todos los recursos antes mencionados, ha llevado a facilitar la manera de cómo implementar un servidor firewall basado en una distribución de Linux llamada Endian. Instalar y configurar un firewall da la oportunidad también de implementar otros servicios como: modo proxy, modo proxy transparente, vpn entre otros. Además se puede tener una estructura de red con DMZ (zona desmilitarizada); Zona Verde: representa la zona segura de internet; Zona Roja: representa la zona insegura de internet; servidor DHCP: servidor que recibe peticiones de clientes solicitando una configuración de red IP. Y cuenta también, con un Antivirus Web: que brinda seguridad sencilla y eficaz desde un navegador web y un Antispyware: tecnología de seguridad que ayuda a proteger a una red contra intrusos y otro software potencialmente no deseado, otorgando de esta manera la posibilidad de hacerlo más sencillo y seguro; además de poder administrarlo por vía Web dando más facilidad en el momento de implementar las reglas o políticas en el firewall. La mayoría de los administradores, están en constante movimiento, por lo general no están en contacto directo con la maquina a administrar, lo que requieren herramientas que le brinden la posibilidad de administración remota por vía Web. Endian cumple este requisito, permitiendo desde cualquier máquina de la red acceder remotamente vía Web y administrar el firewall, ahorrando que se desplace hacia la propia maquina física. La expectativa que se quiere lograr implementando este firewall es tener más conocimiento de herramientas Open Source, que no solo existe ip tables, sino que hay muchas

herramientas que pueden ser más sencillas de configurar y administrar por vía Web el sistema. (Pineda, 2009)

2.3 Manual del usuario para la instalación y configuración del firewall Endian

El presente manual está dirigido al administrador de la red del Colegio La Asunción de San Salvador, para hacerle más sencillo detectar los riesgos y vulnerabilidades en la red local y minimizar los mismos; y a su vez, pueda controlar todo el tráfico de los sitios web que se visiten por internet. Así mismo, va dirigido a cualquier persona que desee instalar y configurar el sistema operativo Endian, para la protección de la red o redes que tenga a su cargo. Y también puede implementarse en otros centros escolares o empresas con bajos recursos económicos.

Configuración de las funciones principales del Servidor Firewall Endian

-Para con figurar el servidor DHCP, se da clic en la pestaña servicios, luego clic DHCP server y en configuración, luego se pone el rango de dirección ip que tendrá disponibles el servidor DHPC para asignar ip automáticamente a las computadoras. Después guardar y aceptar.

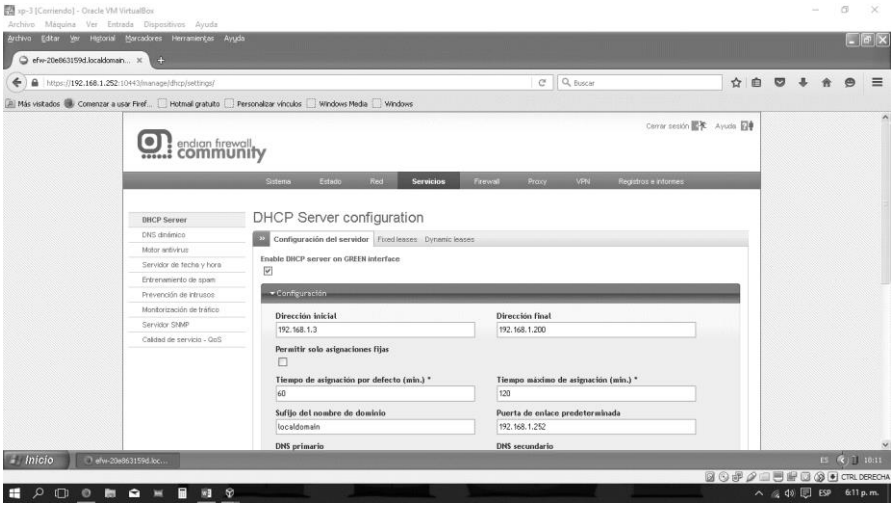


Figura N° 3 Rango de dirección ip disponibles para el servidor DHCP

-Configuración del proxy, en la pestaña proxy, opción http se activa "habilitar proxy http de modo trasparente, esto para que automáticamente las computadoras del Colegio La Asunción se conecten a internet, sin necesidad de configurar cada una de las computadoras.

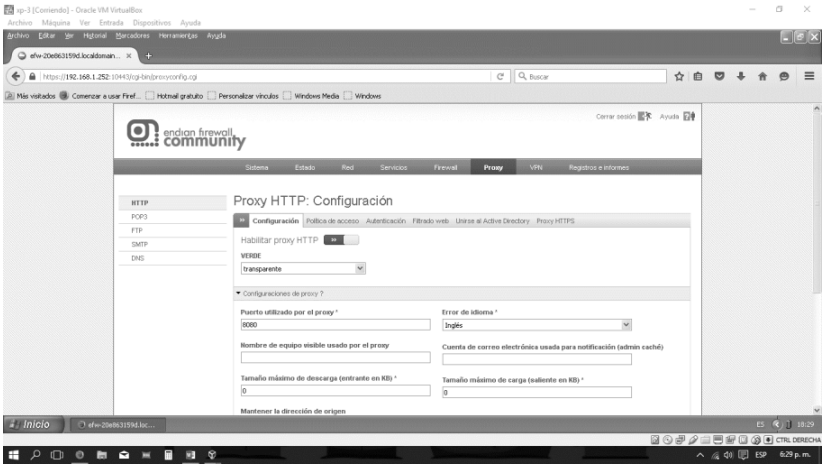


Figura N° 4 Activación del http proxy en modo transparente

-En filtrado web, siempre en pestaña proxy opción http, se tiene que seleccionar rutina de actualizaciones diariamente, luego se añade un nuevo perfil en donde se configuran las categorías de las páginas web que se permitirán y las que se bloquearán.

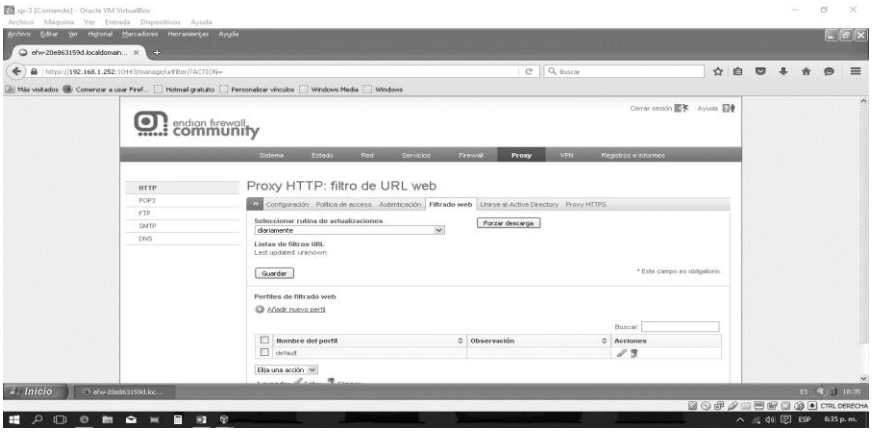


Figura N° 5 Configuración de rutinas de actualizaciones

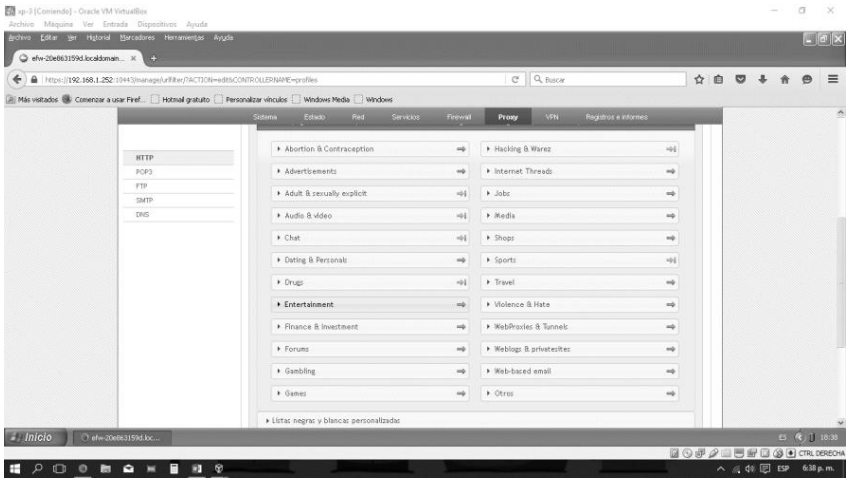


Figura N° 6 Agregar un nuevo perfil de filtrado web

- Para que el perfil de políticas de acceso quede aplicado en toda la red, en la pestaña de política de acceso, se da clic en crear política de acceso.

Tipo de fuente zona verde y a destino cualquiera, y permitir la política de acceso.

Después se selecciona el filtro de perfil que se ha creado, se coloca en primera posición.

Luego clic en guardar y aceptar.

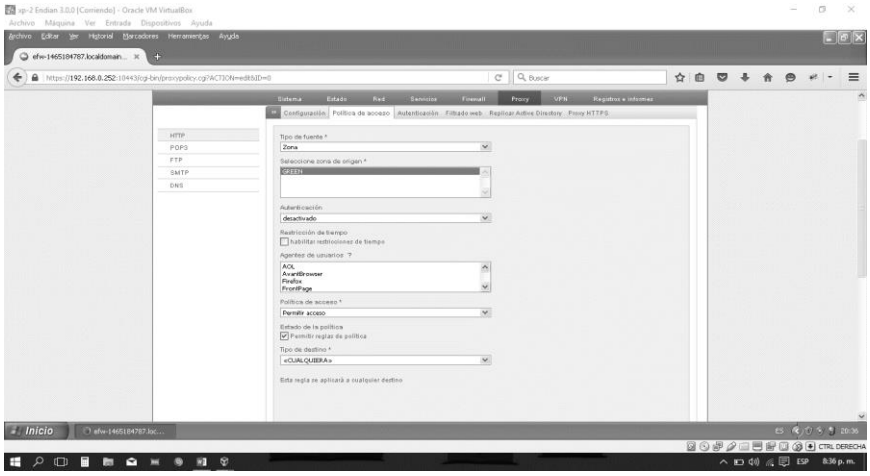


Figura N° 7 Habilitación de la zona verde del registro del Firewall con conexiones salientes

A continuación se detalla paso a paso, la instalación y configuración del sistema operativo Endian:

1) Seleccionar el idioma más conveniente.

Figura N° 8 Selección del Idioma

2) Luego seleccionar OK, para realizar la nueva instalación.

Figura N° 9 Realizar nueva instalación

3) Después aparecerá un mensaje, el cual indica que todo el contenido en el disco se perderá para la instalación de Endian, se selecciona YES.

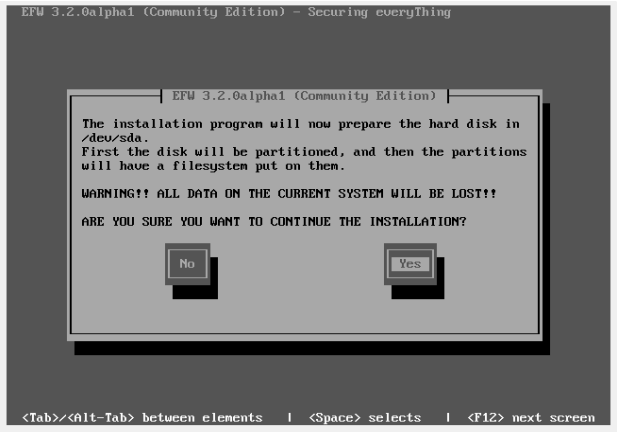


Figura N°10 Perdida del contenido para instalar Endian

4) En caso de que sea un disco duro de poca capacidad saldrá el siguiente mensaje, pero se puede realizar la instalación.

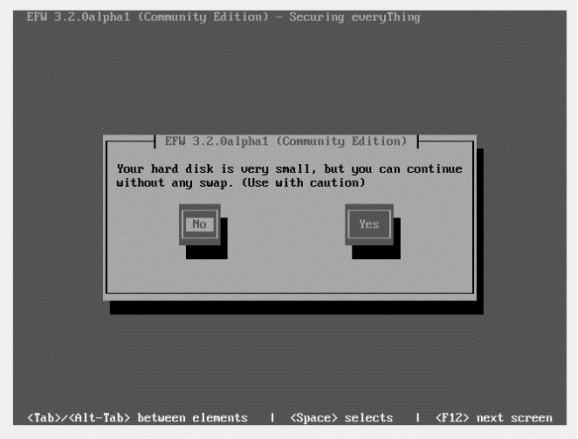


Figura N° 11 Disco duro de poca capacidad para instalar Endian

5) A continuación se formateará el disco para la instalación.

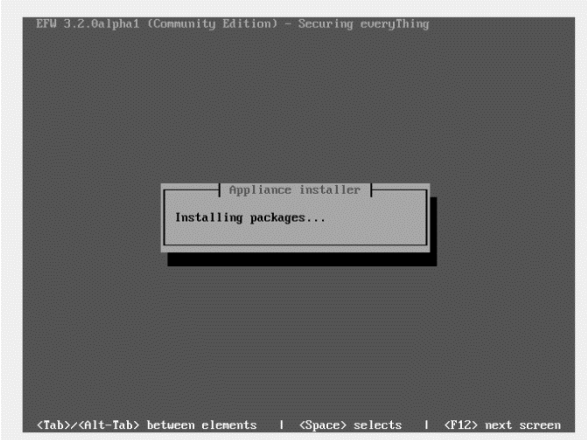


Figura N° 12 Formateo del disco duro

6) Luego aparece el siguiente mensaje, el cuál pregunta si se quiere configurar automáticamente el puerto serial, que el servidor Firewall desea administrar, se le dará clic en No.

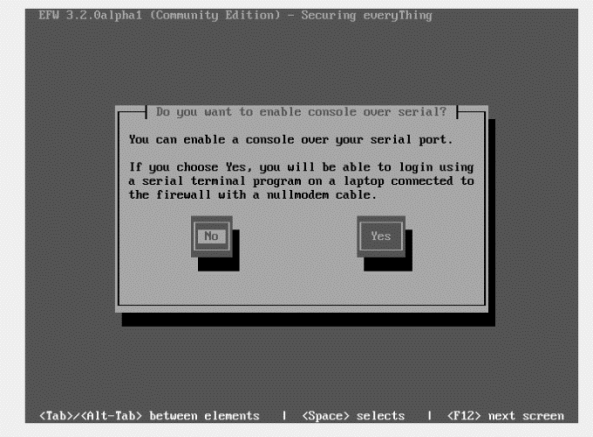


Figura N° 13 Configuración automática del puerto serial

7) Posteriormente se procede a configurar las zonas, se comienza con la zona verde, es donde estarán las computadoras clientes que tendrán el acceso a internet mediante el servidor Firewall.

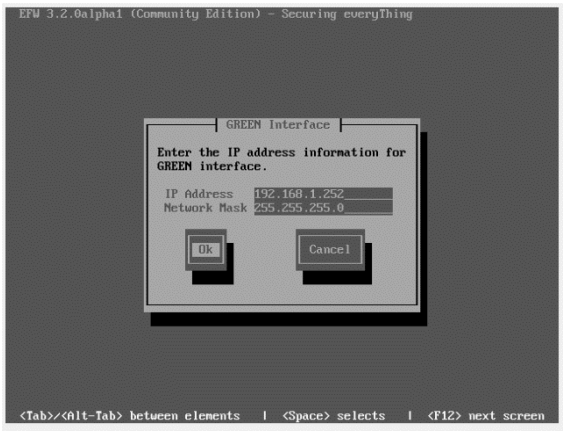


Figura N° 14 Configuración de las zonas

8) Emergerá un mensaje, comunicando que la instalación se ha realizado correctamente, para realizar las configuraciones de parámetros se debe de acceder a través de un navegador web a la dirección y puerto indicado.

Nota: la computadora que se utilizará para la configuración debe de estar en el mismo rango de ip que se asigna en la zona verde.

Figura N° 15 Configuración de parámetros

9) Una vez finalizada la instalación, se reiniciará el servidor Firewall y se podrá realizar las configuraciones.

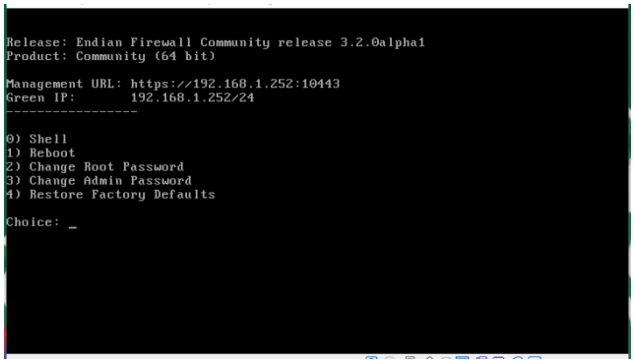


Figura N° 16 Reinicio del Servidor Firewall

10) Luego a través de otra computadora se configura la conexión de área local, se le coloca una ip fija dentro del rango de la zona verde y como puerta predeterminada la ip del firewall, esto se hará para poder acceder a la interfaz web del servidor firewall.

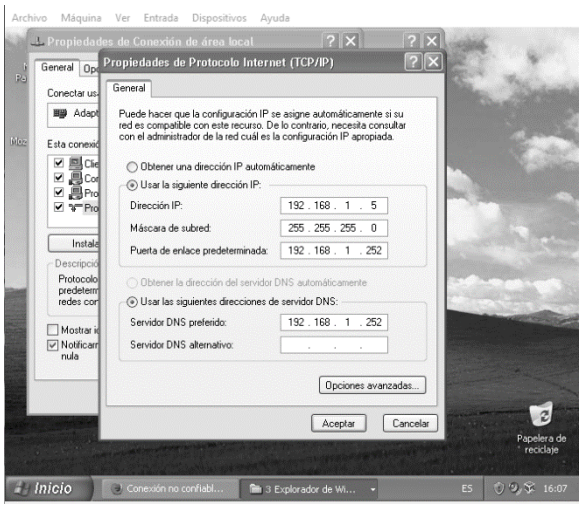


Figura N° 17 Configuración de la conexión de área local

11) Enseguida, en el navegador web se digita la dirección ip y puerto del servidor Firewall en este caso sería https://192.168.1.252:10443, saldrá una advertencia, que la web no está verificada, que es un certificado que automáticamente se crear para poder acceder a la interfaz, se da clic en opciones avanzadas y en añadir excepción.

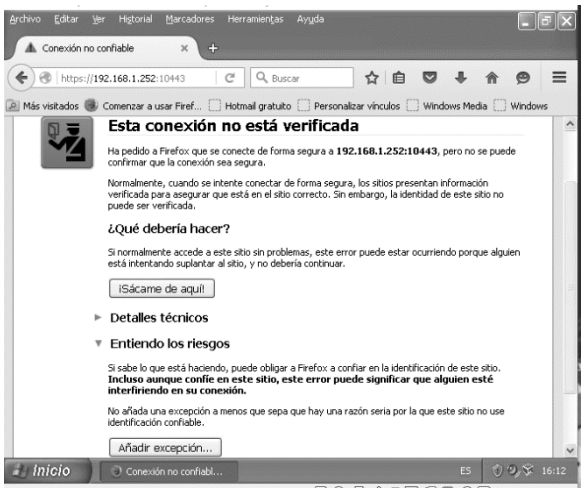


Figura N° 18 Se escribe la dirección ip y puerto del servidor Firewall

12) Después se debe de dar clic, en confirmar excepción de seguridad.

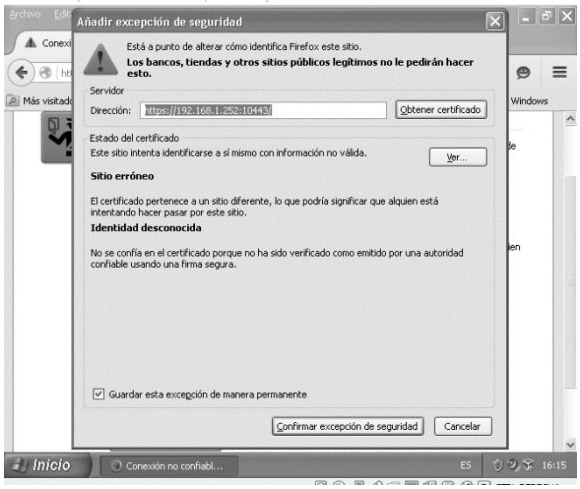


Figura N° 19 Excepción de la seguridad

13) Surgirá la página inicial para la configuración de Endian, se va a siguiente.

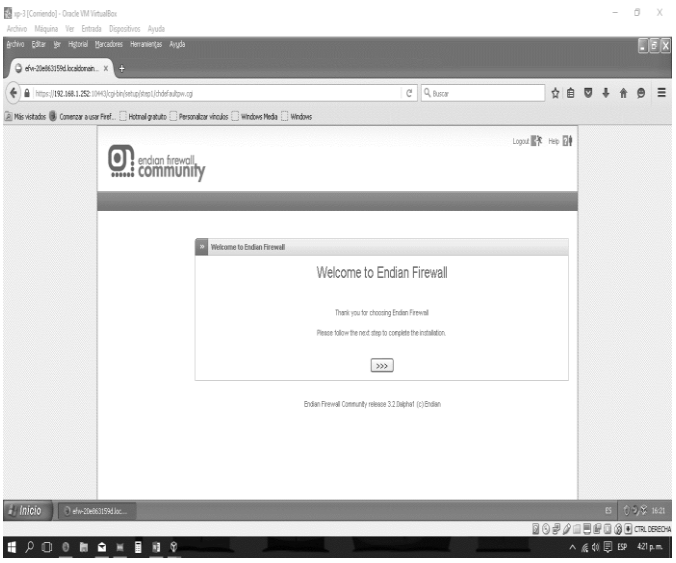


Figura N° 20 Página inicial de la configuración de Endian

14) Se selecciona el idioma y región de preferencia.

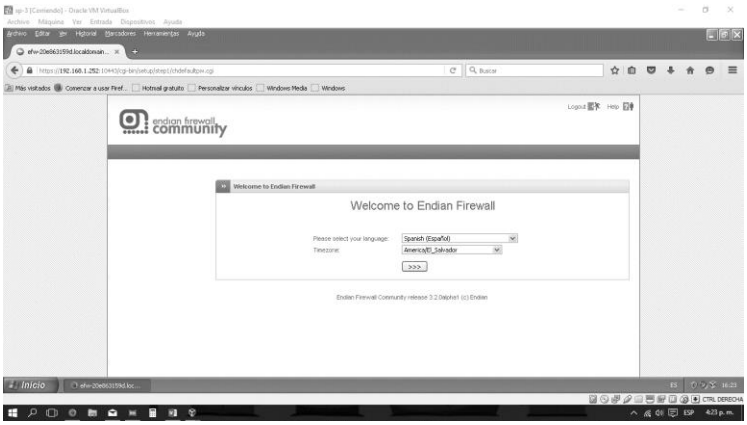


Figura N° 21 Selección del idioma y región

15) Se aceptan los términos de licenciamientos del software Endian.

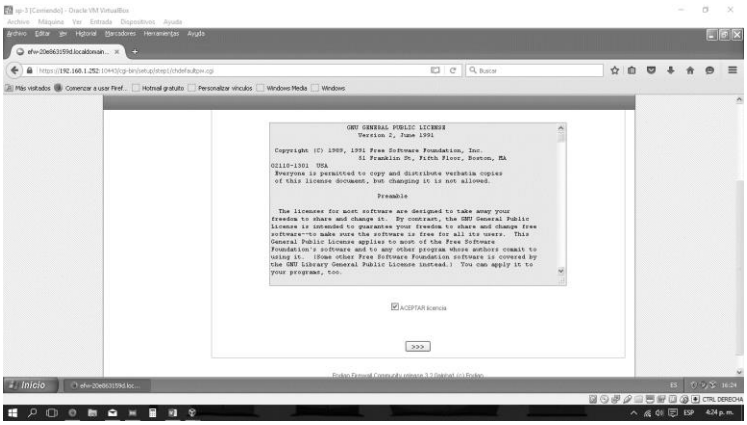


Figura N° 22 Términos de licencia de Endian

16) Si se cuenta con un backup de la configuración de Endian anterior, se puede subir esa configuración, de lo contrario clic en la opción no y continuar.

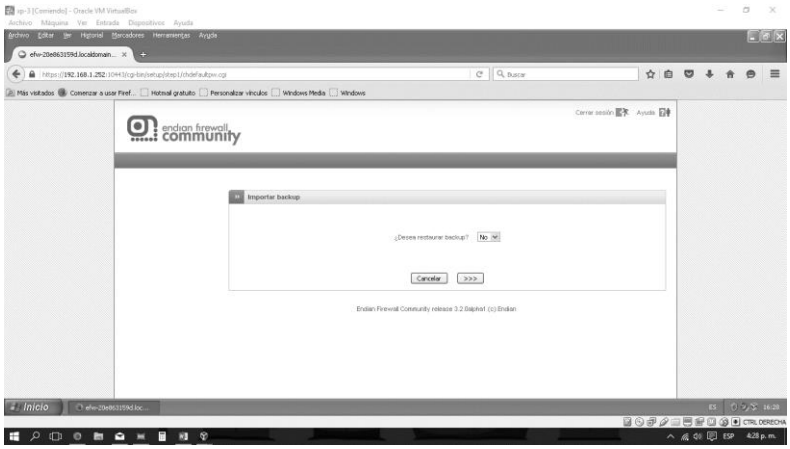


Figura N° 23 Backup de la configuración de Endian

17) Después se establecen las contraseñas de administrador y usuario root.

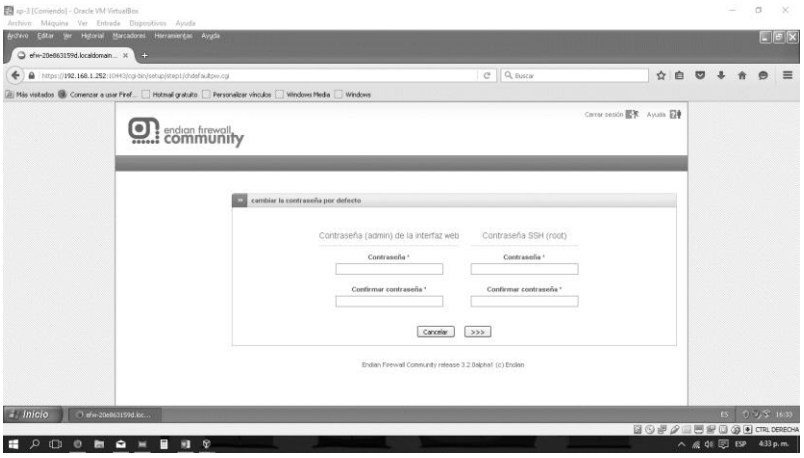


Figura N° 24 Contraseñas de administrador y usuario

18) Luego se selecciona el tipo de red de enrutamiento, y en tipo de enrutamiento en la zona roja, se coloca Ethernet por DHCP.

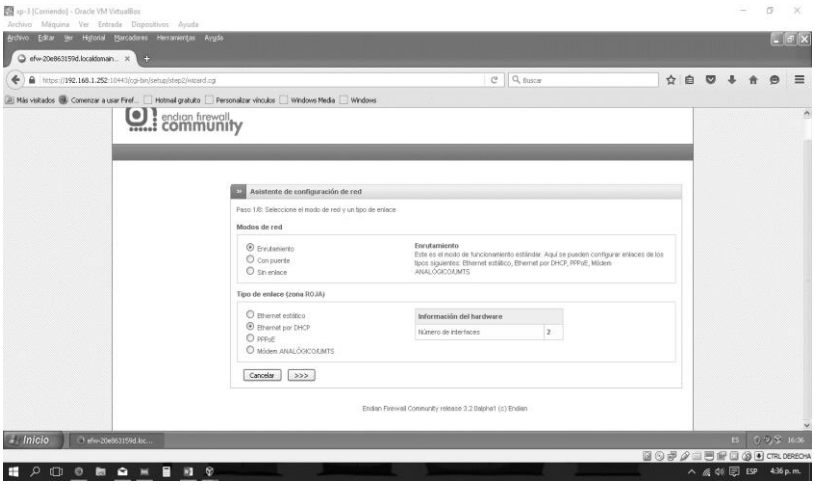


Figura N° 25 Selección del tipo de red de enrutamiento

19) En esta parte se puede configurar la zona azul que es el wifi, y la zona naranja que es la zona DMZ (zona desmilitarizada), donde se encuentran los servidores; en el caso que hubieran aquí, es donde se configuran esas zonas, de lo contrario clic en la opción ninguno.

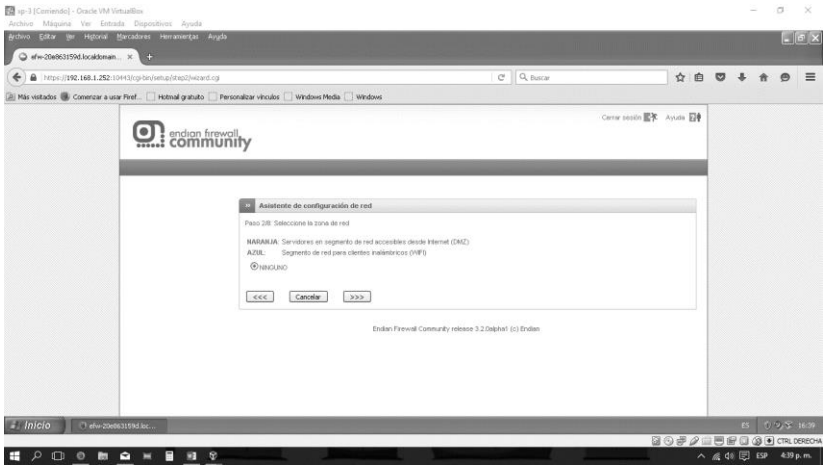


Figura N° 26 Configuración de la zona azul y naranja

20) Posteriormente aparece la zona verde y la ip que se configuró cuando se instaló Endian, al igual, cuál será la tarjeta de red que está conectada a esta zona, aquí se puede cambiar si es necesario la ip que muestra, es la puerta predeterminada donde saldrán las peticiones a internet de las computadoras clientes.

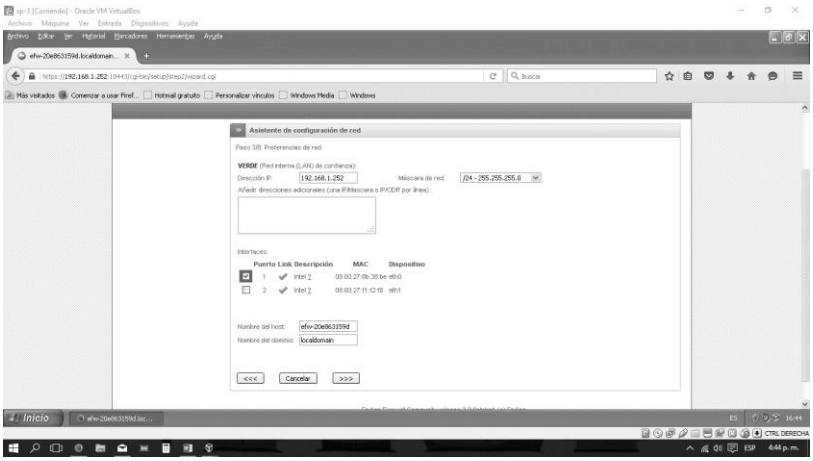


Figura N° 27 Cambio de la ip de ser necesario

21) De igual manera en la zona roja, solo que en este caso será en automático, si se quiere tener una ip fija en la zona roja, previamente debe de configurarse el router que brinda el servicio de internet, de lo contrario solo se deja en automático.

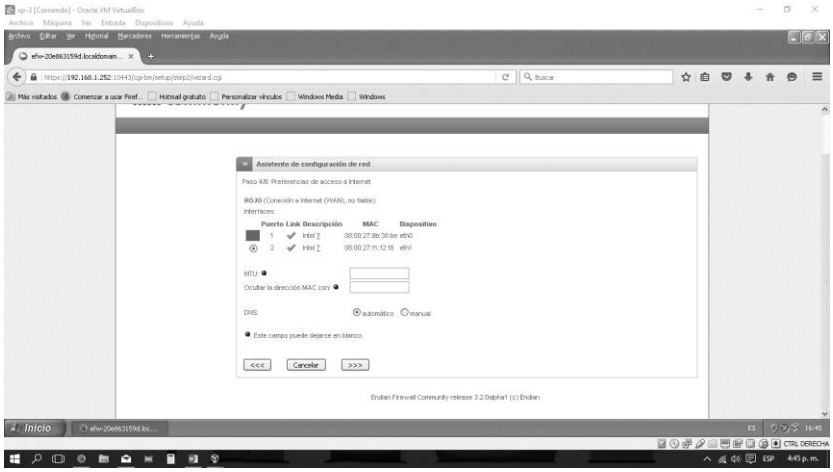


Figura N° 28 ip automática de la zona roja

22) Posteriormente, se coloca el correo de administrador, que puede ser de cualquier dominio como Gmail, Hotmail, etc., esto no es indispensable pero se puede configurar si se desea.

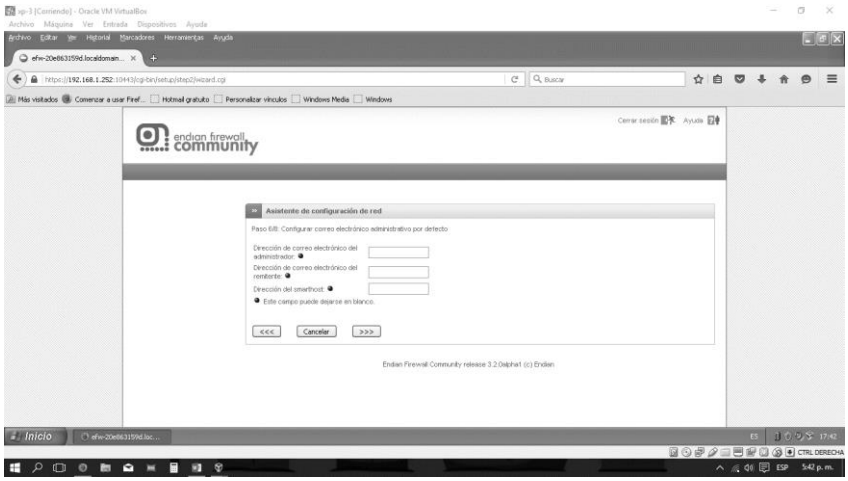


Figura N° 29 Configurar el correo del administrador

23) Luego saldrá un mensaje, comunicando que se ha configurado exitosamente el servidor Firewall Endian, después de esto se reiniciará y quedarán los parámetros que se le configuraron.

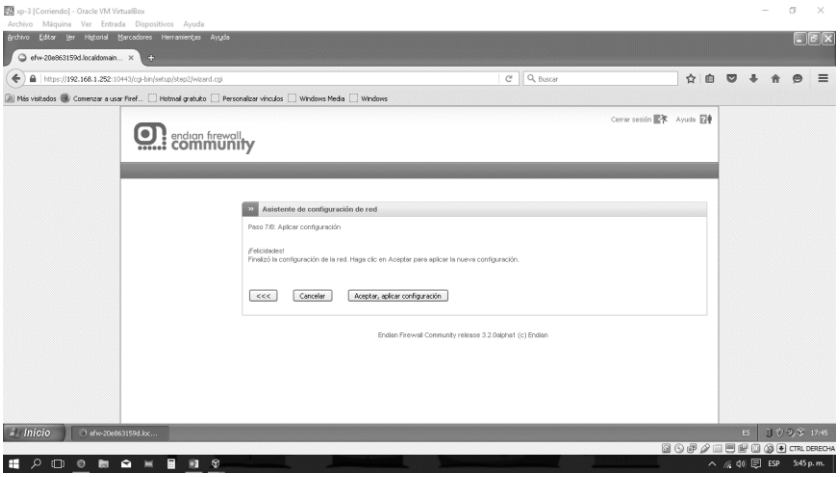


Figura N° 30 Configuración exitosa del Servidor Firewall

24) Enseguida solicitará el usuario y contraseña del administrador para ingresar.

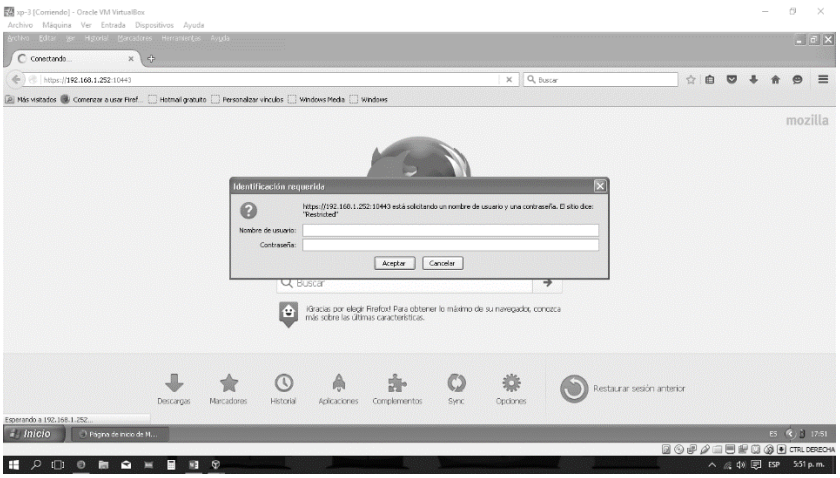


Figura N°31 Introducir usuario y contraseña para ingresar al Servidor Firewall

25) Y surgirá la página principal de Endian, en donde muestra el estado del servidor Firewall, con los gráficos de demanda de internet de los clientes en tiempo real.

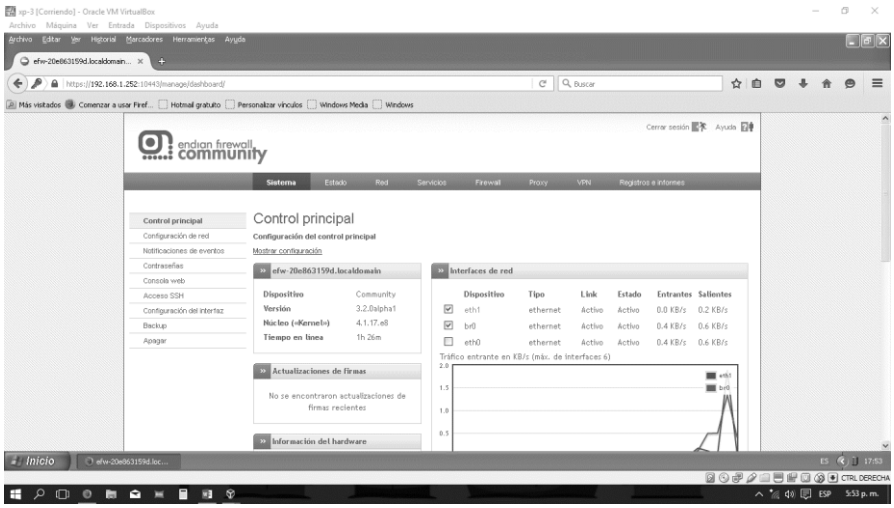


Figura N° 32 Página principal de Endian, mostrando el estado del Servidor Firewall

26) Ahora se debe de configurar el servidor DHCP dentro de la zona verde, para que Endian le coloque una ip automática a las computadoras clientes.

Se va a la opción servicios dentro de la consola de Endian, luego clic en la opción "DHCP server", después clic en la casilla "enable DHCP server on Green interface".

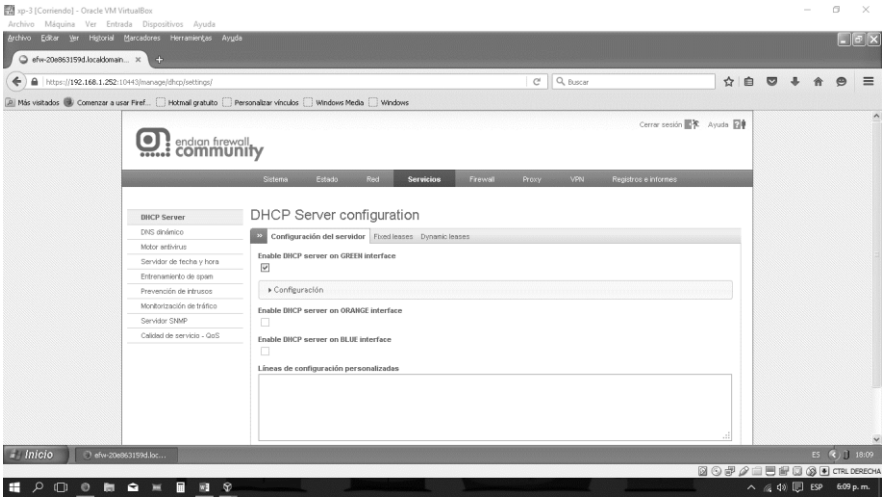


Figura N°33 Configuración del Servidor DHCP en zona verde

27) Posteriormente clic en configuración y se pone el rango de dirección ip que tendrá disponibles el servidor DHPC para asignar a las computadoras. Después clic en guardar y aceptar.

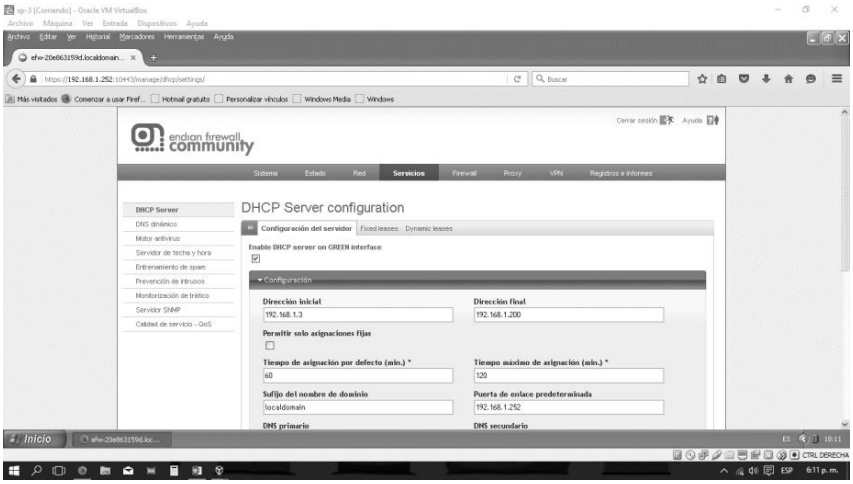


Figura N° 34 Rango de dirección ip disponibles para el servidor DHCP

28) La opción de “prevención de intrusos” debe de estar activada, de esta manera se sabe si hay alguien que este husmeando en la red.

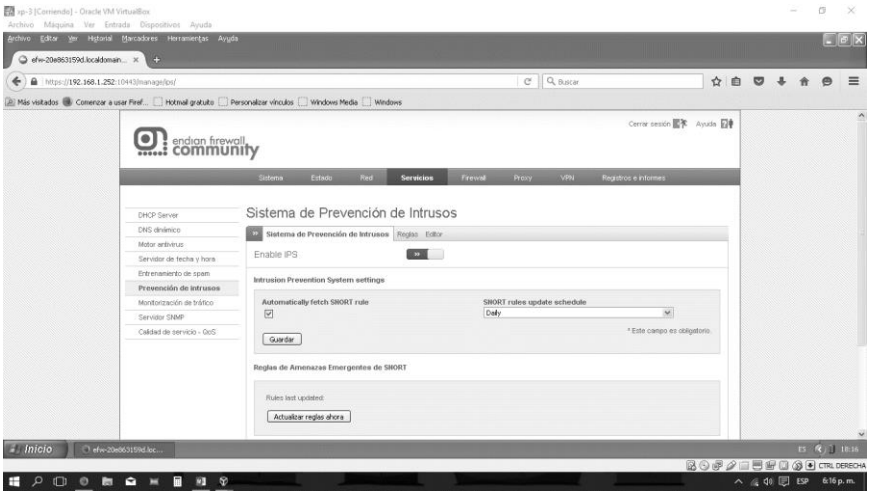


Figura N° 35 Activación de la opción prevención de intrusos

29) También debe de estar activo el “analizador de tráfico en la red”.

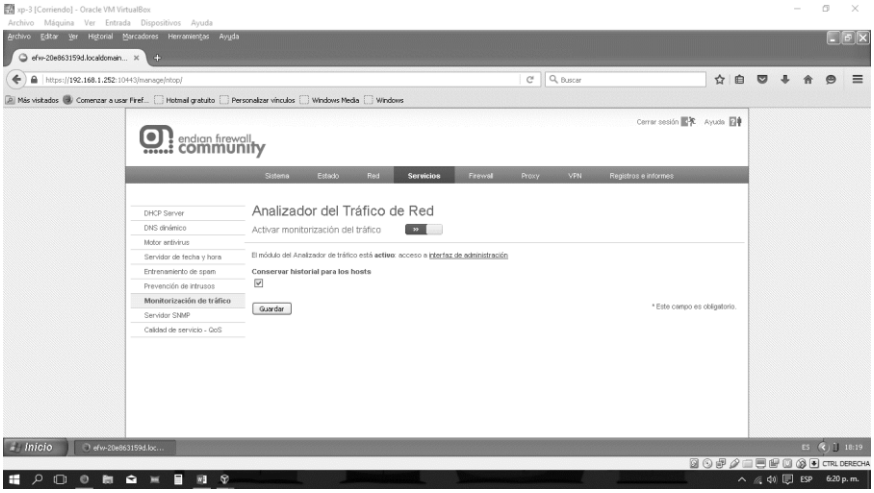


Figura N° 36 Activar el analizador de tráfico en la red

30) Luego en la pestaña “proxy”, opción HTTP, se debe de activar el http proxy de modo trasparente.

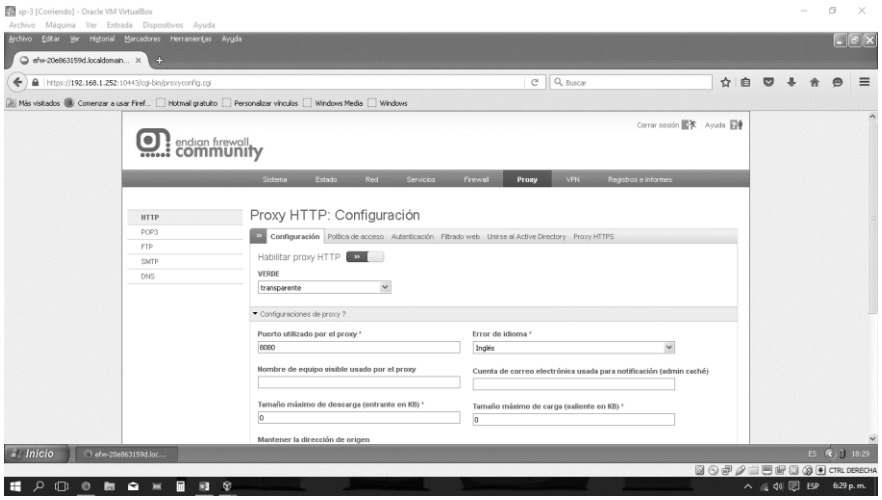


Figura N° 37 Activación del http proxy en modo transparente

31) A continuación en la opción “filtrado web”, se coloca la configuración de rutinas de actualizaciones a diario.

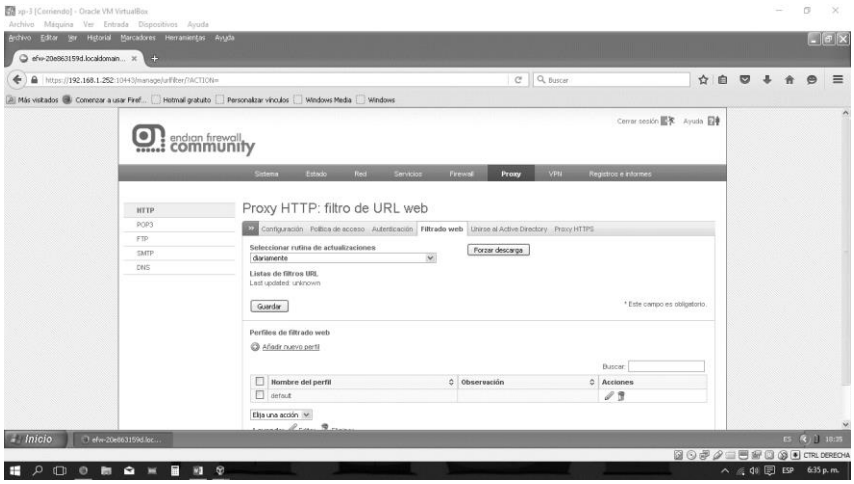


Figura N° 38 Configuración de rutinas de actualizaciones

32) Así mismo se agrega un nuevo perfil de filtrado web, en donde se restringirá el acceso a ciertas páginas por su categoría, se coloca el nombre del perfil.

Clic en nuevo perfil e inmediatamente clic en filtro de páginas conocidas por su categoría.

En seguida, clic sobre la flecha verde para negar el acceso a esa categoría.

Por último, aceptar y guardar los cambios.

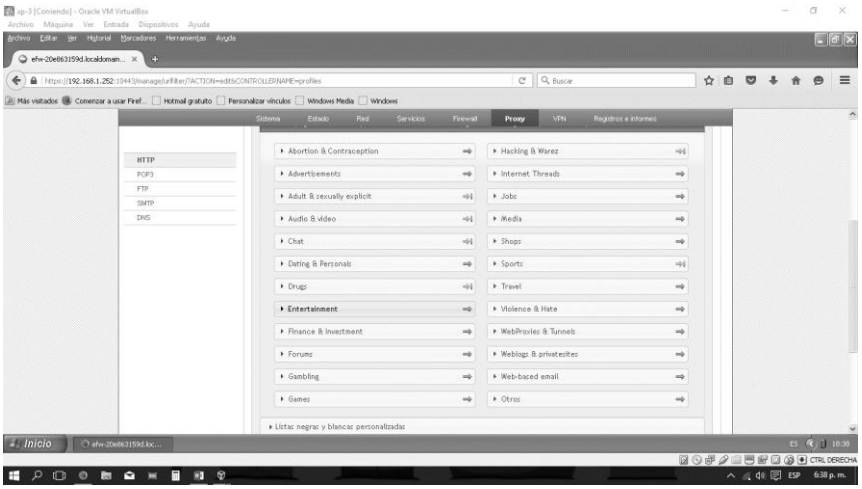


Figura N° 39 Agregar un nuevo perfil de filtrado web

33) Si lo que se quiere es bloquear o dar acceso a una página en específico pero que sea de protocolo http, se hacen en las listas negras y blancas personalizadas donde se pone la URL de la página que se quiera dar acceso o bloquear.

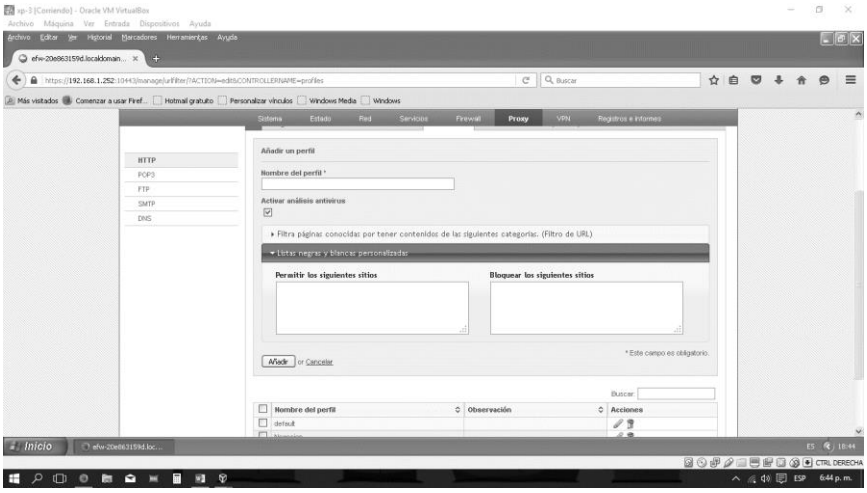


Figura N° 40 Realización de listas negras y blancas personalizadas

34) Para que el perfil de políticas de acceso quede aplicado en toda la red, en la pestaña de política de acceso, clic en crear política de acceso.

Tipo de fuente zona verde y a destino cualquiera, y permitir la política de acceso.

Selecciona el filtro de perfil que se ha creado, se coloca en primera posición.

Luego clic en guardar y aceptar.

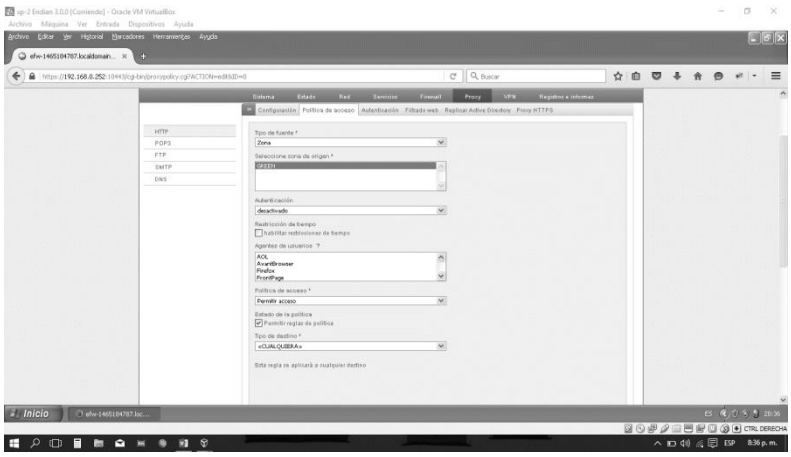


Figura N° 41 Habilitación de la zona verde del registro del Firewall con conexiones salientes

35) Siempre en la pestaña proxy en la opción “FTP”, se habilita la zona verde, y se habilita el registro de Firewall con conexiones salientes. Luego clic en aceptar y guardar.

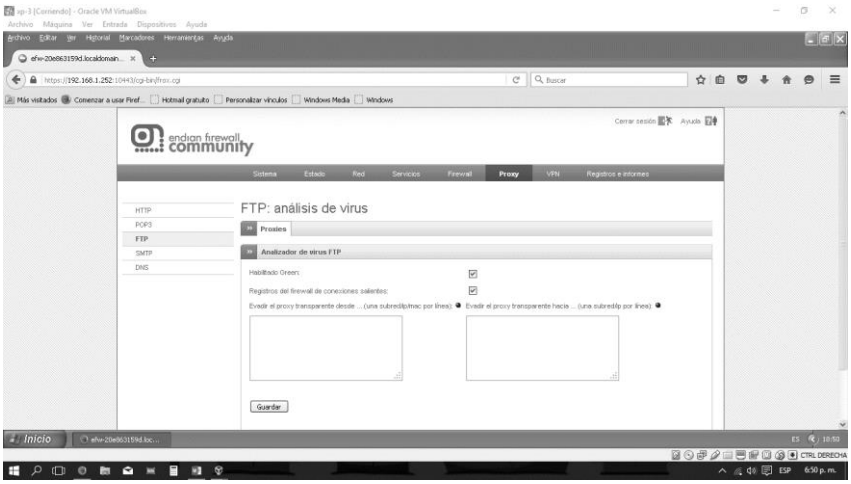


Figura N° 42 Habilitación de la zona verde del registro del Firewall con conexiones salientes

36) En seguida, en la opción SMTP, se activa el proxy SMTP, para la zona verde. Después se guarda y se aceptan los cambios.

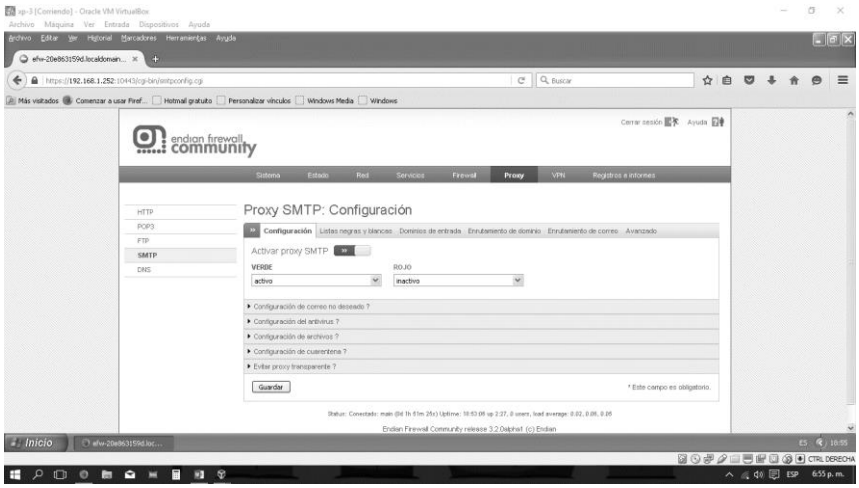


Figura N° 43 Activación del proxy SMTP para la zona verde

37) Posteriormente, en la pestaña “servicios” en opción estado del sistema, se puede ver todos los servicios que se han activado como los que están detenidos. Y así, saber si está completamente configurado el servidor Firewall.

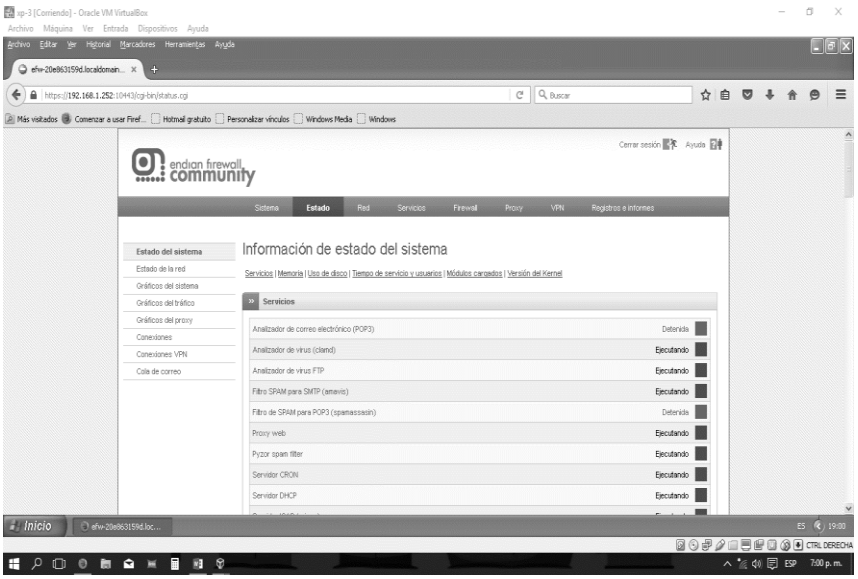


Figura N° 44 vista de servicios que sean activados en la pestaña de servicios

38) En la pestaña de Firewall, en la opción tráfico de salida, se permite el acceso o denegar ciertas paginas como por ejemplo “Facebook”, se coloca el origen zona Green, a destino las ip de Facebook y la acción denegar o permitir el acceso según sea el caso, luego clic en aplicar los cambio y guardar.

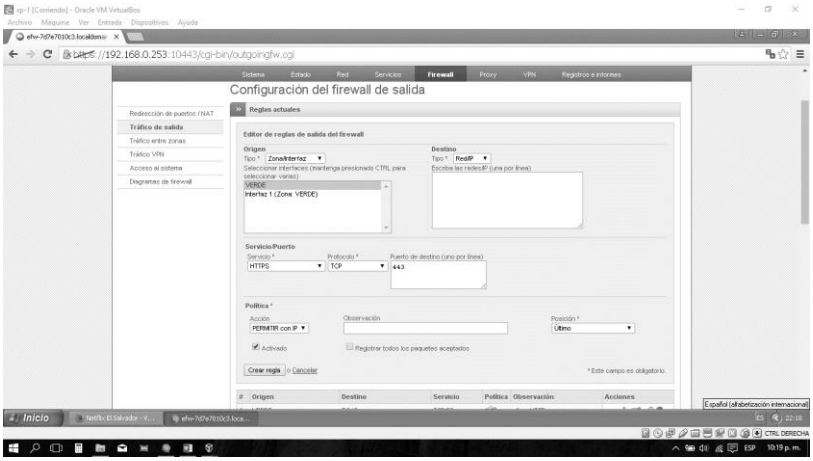


Figura N° 45 Firewall de tráfico de salida, en la pestaña Firewall

39) En la pestaña del proxy, opción DNS en Antispyware, se puede colocar los nombres de los dominios que se deseen bloquear, con esto, no se podrá acceder a esa página en toda la red, ni siquiera teniendo acceso como administrador, porque lo detectará como una página maliciosa.

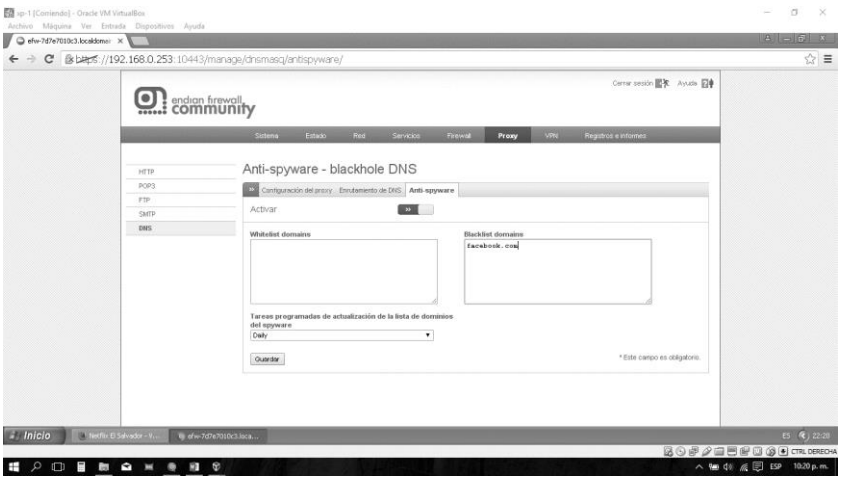


Figura N° 46 Bloqueo de dominio en la pestaña de proxy como antispyware

40) En la pestaña Registros e Informes, se puede visualizar los diferentes tipos de reportes como el estado del sistema, la detección de virus, el firewall, las páginas visitadas, etc.

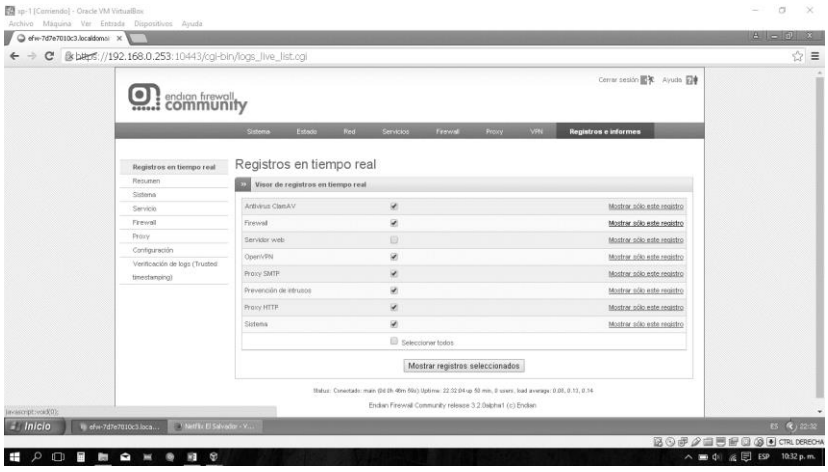


Figura N° 47 Pestaña de reportes e informes diagnósticos de los servicios de internet

41) Por último, en la siguiente imagen se poder visualizar los reportes del servidor Firewall, y muestra la información detallada, de acuerdo lo que se quiere ver.

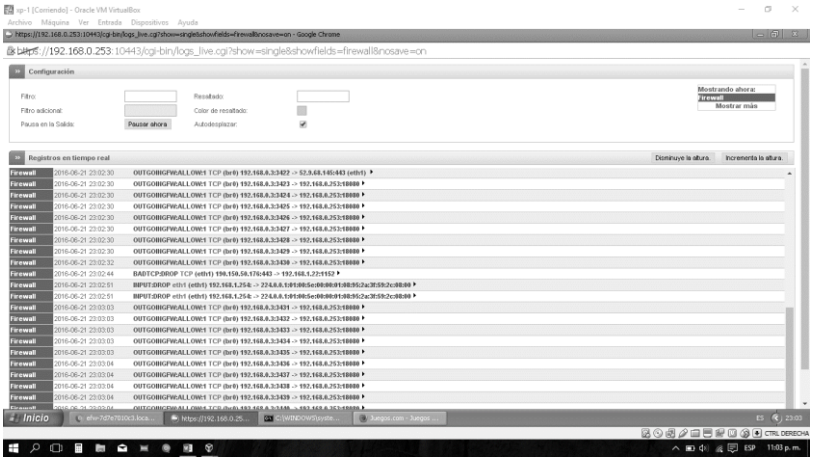


Figura N° 48 Visualización de informes de lo que ha pasado en el servidor Firewall

3. Marco Teórico Conceptual

-**Firewall:** Un firewall es software o hardware que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall. (Microsoft, 2016)

-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 que está accediendo. (Alvarez, 2016)

-Zona Verde: La zona verde es la zona segura de internet donde se encuentran las computadoras clientes, donde el firewall ya ha bloqueado todo tipo de restricción.

-Zona Roja: La zona roja es la zona insegura de internet, es donde de se encuentra el internet libre y donde está todo tipo de contenido, la zona roja es el rauter el servicio que brinda el proveedor de internet.

-**Zona DMZ:** La zona DMZ, es la zona desmilitarizada por sus siglas en inglés (demilitarized zone), es la zona donde se encuentran los servidores, son los que se aíslan de la zona verde y la zona roja, pero que si tienen comunicación entre las zonas, también es conocida como la zona naranja.

-Interface: Es la referencia a una conexión activa o inactiva, de las tarjetas de red. (Wikipedia.org, 2016)

-UTM: Por sus siglas en inglés (Unified Threat Management), gestión de unificada de amenazas, Se utiliza para describir los cortafuegos de red que engloban múltiples

funcionalidades en una misma máquina. Algunas de las funcionalidades que puede incluir son las siguientes: vpn, anti-spam, anti-spyware, filtro de contenido, antivirus.

-Dirección IP: es el número que identifica a cada dispositivo dentro de una red con protocolo IP.

-Http: (en español protocolo de transferencia de hipertexto) es el protocolo de comunicación que permite las transferencias de información en la World Wide Web.

-Https: (en español: Protocolo seguro de transferencia de hipertexto), más conocido por sus siglas HTTPS, es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP.

-TCP: Protocolo de Control de Transmisión, es uno de los protocolos fundamentales en Internet. Muchos programas dentro de una red de datos compuesta por redes de computadoras, pueden usar TCP para crear "conexiones" entre sí a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

-UDP: es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

-SSH: (Secure Shell, en español: intérprete de órdenes seguro) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

-FTP: (siglas en inglés de File Transfer Protocol, 'Protocolo de Transferencia de Archivos') en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

-Modo Proxy: Hacen uso de proxies para procesar y redirigir todo el tráfico interno.

-Modo Trasparente: No redirigen ningún paquete que pase por la línea, simplemente lo procesan y son capaces de analizar en tiempo real los paquetes.

-VPN: es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

-Criptografía: es el que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

-Servidor DHCP: es un servidor que usa protocolo de red 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 quedando 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. Así los clientes de una red IP pueden conseguir sus parámetros de configuración automáticamente.

-Dropbox: es un servicio de alojamiento de archivos multiplataforma en la nube, operado por la compañía Dropbox. El servicio permite a los usuarios almacenar y sincronizar archivos en línea y entre ordenadores y compartir archivos y carpetas con otros usuarios y con tabletas y móviles.

-**Antispyware:** programa espía es un malware que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador. El término spyware también se utiliza más ampliamente para referirse a otros productos que no son estrictamente spyware.

-Cracker: se utiliza para referirse a las personas que "rompen" algún sistema de seguridad. Los crackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta, o por el desafío.

-Hacker: es todo individuo que se dedica a programar de forma entusiasta, o sea un experto entusiasta de cualquier tipo, que considera que poner la información al alcance de todos constituye un extraordinario bien.

-**Antivirus Web:** Programa antivirus que, en lugar de estar instalado y ejecutándose de forma permanente en el sistema, funciona a través de un navegador web. Contrasta con los antivirus offline o antivirus tradicionales que se instalan. (Alegsa, 2010).

4. Documentación Técnica

Motherboard:

Para máquinas de escritorio, modelo H81MLV3 BIOSTAR, cuenta con las características técnicas necesarias, como son: un socket 1150, que soporta procesadores Pentium i3, i5 y i7, soporta 16GB de memoria RAM, lo suficiente para soportar el sistema operativo Firewall Endian.

Microprocesador:

Procesador Intel Dual Core 3.2GHZ cuenta con una velocidad de Reloj 3.2Ghz como mínimo, con socket 1150, y tiene 3MB de memoria cache.

Memoria RAM:

Memoria RAM DDR3, se ha optado por dos memorias RAM Kingston, la cual será una memoria RAM de 12GB, con un bus de datos de 1333MHZ, lo suficiente para tener en óptimo funcionamiento el servidor Firewall.

Disco duro:

Disco duro THOSIBA de 500GB, con una velocidad de 7200 rpm, con interfaz SATA; lo que hace más rápido la transferencia de datos.

Case:

Case Genérico, de aluminio polarizado y viene con una fuente de 550W, teclado, mouse, y bocinas; con puertos USB delanteros.

Tarjeta de Red Alambrica:

Nexxt Siruis 1000 con una velocidad de 150 mb/s, de acuerdo a las características técnicas es el mejor evaluado, incorpora un módulo de chips de avanzada tecnología para facilitar su instalación y garantizar la integración fluida de todos sus componentes. Con un extenso número de controladores, la tarjeta es capaz de funcionar con los sistemas operativos mayormente utilizados en la actualidad.

Sistema operativo:

Sistema operativo Firewall, se ha optado por el sistema operativo Endian, que es un sistema basado en Linux, en el cual se hacen las configuraciones, y se tiene el monitoreo a través de una interfaz web, Endian tiene el servicio de firewall, antivirus, anti-spyware, con usuario VPN, es la versión gratuita más completa.

Capítulo III Desarrollo de la Solución

1. Propuesta de la Solución

Imagen de la estructura de la red en El Colegio La Asunción

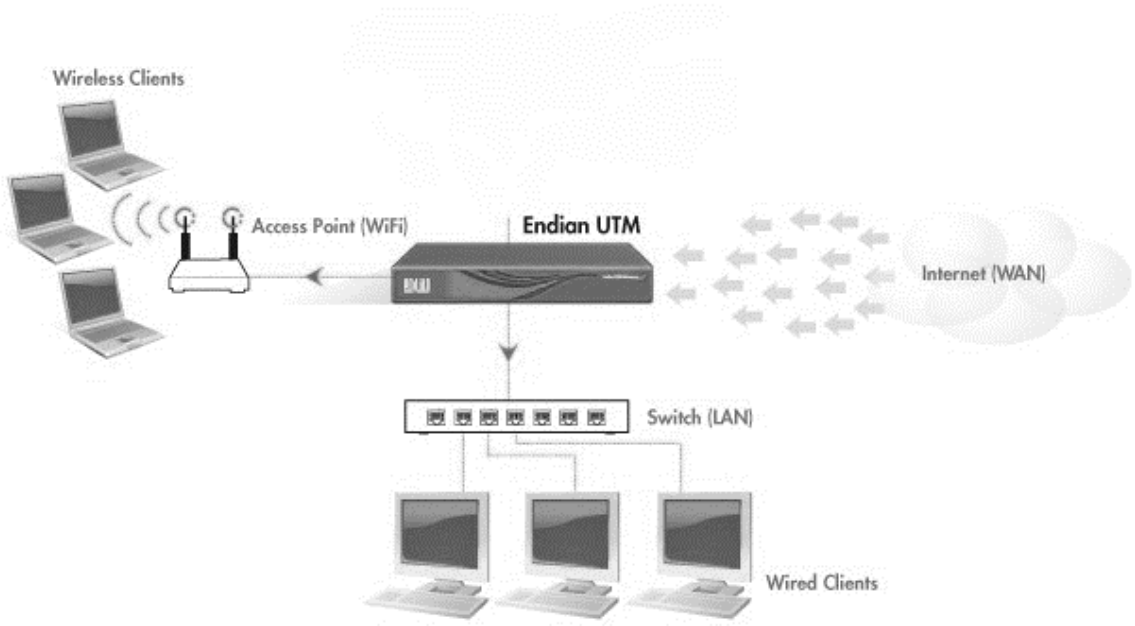


Figura N° 49, Topología de la red controlada por firewall Endian.
http://auditafirewall.blogspot.com/2013_11_01_archive.html

El colegio La Asunción de San Salvador, cuenta con dos laboratorios de informática sin acceso a internet libre, los alumnos y alumnas no pueden accesar a cualquier sitio por internet, es por ello, que no logran visitar páginas de ocio, de violencia explícita y sitios web con contenido sexual, entre otras. Por contar con servicio denominado Open DNS, pero el problema es que la dirección IP es asignada por DHCP por el proveedor de internet es decir que se modifica la IP en ocasiones y se pierden las configuraciones asignadas a la IP en el servicio Open DNS, En ese momento los estudiantes pueden

accesar a cualquier tipo de información. Hasta que se actualicen las configuraciones en la nueva IP asignada por el proveedor de Internet.

Otra situación que se debe tomar en cuenta que la red WIFI del Colegio La Asunción no puede ser controlada o no puede ser filtrado el contenido al cual pueden accesar.

Para la implementación del Servidor Firewall, y mantener en óptimas condiciones su funcionamiento, se han tomado en cuenta lo siguiente:

Se propone como servidor Firewall, una PC con características óptimas que cuente con una Motherboard BIOSTAR H81ML1150, un procesador Intel dual Core LGA 1150 de 3.2 GHz, dos memorias RAM Kingston una de 8GB y otra de 4GB con un bus de 1333 MHZ para hacer un total de 12GB de RAM, un Disco duro Toshiba de 500GB a 7200 Rpm, tarjeta de red alámbrica Nexxt Siruis 1000 de 150 Mbps y un case genérico con una fuente de 550 Watts.

Un sistema operativo basado en Linux, llamado Endian, posee características de un UTM, que lo hace funcionar como servidor Firewall, este sistema operativo cuenta con reglas de tráfico de internet, un antivirus web, antispyware, servidor DHCP, prevención de intrusos, proxy, conexiones VPN, seguridad SSH, bloqueo de categorías web y web específicas; además posee una estructura de red con DMZ (zona desmilitarizada) que ofrece la posibilidad de hacerlo más sencillo, y poder administrarlo por vía Web, brindando más facilidad en el momento de implementar las reglas o políticas del firewall, entre otras.

Además se brinda un manual al encargado de la red local de dicho colegio, con las instrucciones necesarias para el mantenimiento o cambio de configuraciones del servidor Firewall, de cómo ingresar a la consola a través de una página web, como bloquear categorías o páginas web específicas y como visualizar los informes de las páginas web que se visitan en la red local.

En el manual se utiliza un vocabulario técnico básico, por lo que esto no representa un problema alguno para la comprensión y seguimiento de dicho manual.

Con esto se pretende que los laboratorios de informática del Colegio la Asunción, cuenten con un servidor Firewall con las características óptimas, para ofrecer un servicio de seguridad web de buena calidad y así proteger la red local de virus e intrusos y a la vez hacer que las horas clase en los laboratorios del mencionado colegio, sean mejor aprovechadas y más eficientes; para mejorar el rendimiento académico de los alumnos y alumnas.

El proyecto consiste principalmente en brindar una PC, con características óptimas y la instalación y configuración de un servidor Firewall con el sistema operativo Endian, en los laboratorios del Colegio la Asunción, con el fin proteger la red de virus e intrusos y limitar el acceso a cualquier página web.

Lo primero que se hace para implementar el proyecto, es adquirir los componentes de hardware para montar la PC, luego se realiza la instalación del sistema operativo Endian, posteriormente se revisa la topología de la red de los laboratorios del Colegio la Asunción, para interceptar el cable que provee el servicio de internet, este se conecta a

una de las tarjetas de red del servidor Firewall y por la otra tarjeta de red alámbrica conectada al servidor surge el cable que proporciona el acceso a internet ya filtrado; después se configuran los parámetros que se crean convenientes en la dirección IP de la red del mencionado colegio, y el contenido web se bloquea o la página web en específico. El manual de usuario tiene como principal objetivo, mostrar los pasos de instalación y configuración del sistema operativo Endian.

Luego se hace la instalación y configuración de un servidor Firewall, el cuál protege y limita el acceso a páginas web en los laboratorios del Colegio la Asunción de San Salvador.

Un servidor Firewall, se compone con un sistema operativo basado en Linux llamado Endian, con el cuál se hace la configuración de las políticas de acceso; una unidad del sistema (CPU) con Motherboard BIOSTAR H81ML1150, un procesador Intel dual Core LGA 1150 de 3.2 GHz, dos memorias RAM Kingston una de 8GB y otra de 4GB con un bus de 1333MHZ para hacer un total de 12GB de RAM, un Disco duro Toshiba de 500GB a 7200 Rpm, tarjeta de red alámbrica Nexxt Siruis 1000 de 150 Mbps y un case genérico con una fuente de 550 Watts.

Básicamente su funcionamiento, es analizar todas las peticiones de internet que hagan los usuarios de los laboratorios del Colegio la Asunción, en detalle cuando un usuario de los laboratorios del mencionado colegio haga una búsqueda por internet, esta petición primero pasará por el servidor Firewall y hace la conexión a la página web solicitada y luego la analiza, para ver si dentro de sus configuraciones esta página está

permitida o no, dependiendo de este proceso se muestra al usuario. También el servidor Firewall analizará la web en busca de virus e intrusos.

El presente proyecto está dirigido, a los laboratorios de informática del Colegio la Asunción de San Salvador, pero puede implementarse en otros centros escolares y empresas con bajos recursos que quieran obtener estos servicios, por ser más económicos.

El diseño del servidor Firewall es sencillo, sólo cuenta con una PC con óptimas condiciones, la instalación de un sistema operativo Endian una distribución Linux libre, especializada en cortafuegos, con el cuál se hace las respectivas configuraciones para su uso.

Por último, lo que se debe de tomar en cuenta, es la cantidad de computadoras que se desea controlar con el servidor Firewall, ya que de eso depende el recurso de hardware que se necesita, el sistema operativo Endian es sencillo pero su funcionalidad correcta y óptima servirá para bloquear páginas web en tiempo real; por los dispositivos de hardware que lo componen es como se nota la factibilidad económica. Es por ello, que se ofrece la opción más económica, pero a la vez debe de cumplir con la factibilidad técnica indispensable para su buen funcionamiento. También el manual impreso del usuario, es una solución fácil, donde se siguen los para instalar y configurar el sistema operativo Endian.

Producto 1: Unidad de Sistema (CPU)

Los laboratorios del colegio la Asunción, no cuenta con una unidad de sistema (CPU) con características optimas que funcione como un servidor firewall, ya que por el momento sólo cuentan con el servicio Open DNS y con él limitan el acceso a internet, la dirección IP asignada por DHCP por el proveedor de internet se modifica en ocasiones y se pierden las configuraciones asignadas a la IP en el servicio Open DNS, en ese momento los estudiantes pueden accesar a cualquier tipo de información; por este problema, todas las computadoras de los laboratorios de informática del mencionado colegio pueden infectarse de virus, spam y hasta de extensiones maliciosas de motores de búsqueda de páginas de internet.

Por todo ello, se brinda una unidad de sistema (CPU) que sea lo suficientemente capaz, para que funcione como servidor Firewall en los laboratorios de informática del Colegio La Asunción.

Su diseño consiste en que la unidad de sistema (CPU) sirva como filtro, y se pretende que la conexión a internet de los laboratorios del Colegio La Asunción pase primero por el servidor Firewall y que por el mismo salga otra conexión a internet más segura.

Para el desarrollo de la unidad del sistema, y que este funcione como servidor Firewall en los laboratorios de Informática del mencionado colegio, se necesitan los siguientes componentes de hardware: una Motherboard BIOSTAR con socket de 1150LGA, procesador Dual Core de 3.2GHz, memoria RAM de 12GB, dos tarjetas de red

alámbrica, un disco duro de 500GB, un case con una fuente de poder de 550Watts y un sistema operativo en base Linux que es el Software del Firewall.

Su implementación se requiere de los componentes mencionados anteriormente ya analizados y cotizados; los componentes se deben ensamblar para crear la unidad del sistema (CPU) que sirve como servidor Firewall, y se ubica en un lugar seguro y adecuado dentro de los laboratorios del colegio la Asunción. También se debe de hacer la instalación del sistema operativo base Linux y la configuración para que este quede funcionando correctamente.

Producto 2: Sistema Operativo Endian

Los laboratorios de informática del colegio La Asunción solamente cuentan con un software llamado Open DNS con el cuál se hace el boqueo de páginas web, pero no es un programa muy fiable para un laboratorio de informática ya que es muy limitado en cuanto a funciones, y si falla se corre el riesgo de que las políticas de restricción no funcionen correctamente, dejando libre acceso a internet a las computadoras de dicho colegio.

Es por ello, que se ofrece el Sistema Operativo basado en Linux Endian configurado previamente, de acuerdo a las políticas del Colegio La Asunción, para que de esta manera se configuren categorías de sitios web o páginas web específicas, permitiendo su acceso o negándolo. También cuenta con productos como antispyware, antispam y antivirus que analiza el tráfico de las páginas web que se visiten por internet.

Su diseño se hace de acuerdo a las políticas de seguridad del Colegio La Asunción, de esta manera el sistema operativo Endian se configura para que cuando una computadora de los laboratorios de informática del mencionado colegio haga la búsqueda de una página web por internet la analice y de acuerdo a los parámetros establecidos permita o no el acceso a ella.

Para el desarrollo de bloqueo de páginas web, se necesita que en la unidad de sistema (CPU) tenga instalado el sistema operativo base Linux Endian, para hacer las configuraciones de bloqueo de categorías de páginas web con contenido sexual, de deporte, hacking, violencia, etc. de igual manera se puede bloquear una página web específica sin afectar a toda una categoría.

Para instalar y configurar Endian, en primer lugar, se debe de conocer las políticas de seguridad que el Colegio La Asunción establezca, es decir, a que páginas se permite el acceso y que páginas se pretende omitir. Además de esto se necesita que la unidad de sistema (CPU), tenga instalado el sistema operativo base Linux Endian, con el cuál se debe de acceder al servidor Firewall desde un navegador web con otra máquina que esté conectada en la misma red, para realizar las configuraciones de las políticas de acceso.

Producto 3: Manual del Usuario Para la Instalación del Firewall Endian

El administrador de la red informática del Colegio La Asunción no cuenta con los conocimientos necesarios del sistema operativo Endian para la administración y mantenimiento del mismo, es por esto que se le entrega un manual instructivo para que

le sirva como guía y hacer el mantenimiento y cambios en el futuro del servidor Firewall.

El diseño es un manual tipo libro, que posee la información de cómo accesar al Firewall desde un navegador web en la red local del colegio; como modificar las categorías de los perfiles de filtrado web para permitir o negar el acceso a páginas web y como crear nuevos perfiles de filtrados web, además de como analizar el estado del Firewall.

Para el desarrollo del manual instructivo se hace a través de capturas de pantalla y una breve descripción de lo que se está haciendo, para que se tenga la idea de forma visual las configuraciones y opciones que tiene el Firewall, y de esta manera el administrador de la red del colegio La Asunción va a poder realizar el mantenimiento y configuraciones futuras.

Para la implementación del manual instructivo, se va a entregar una copia impresa y una digital al administrador de red y a la vez se le proporciona una breve capacitación presencial en la cual se le irá guiando con el contenido del manual de las opciones que tiene el Firewall, de manera que se vaya familiarizando con el sistema operativo Endian.

2. Conclusiones

Se ha llegado a la conclusión, que es de suma importancia llevar a cabo innovaciones y aprovechar los recursos a nivel de software y hardware; una computadora con características óptimas es indispensable para implementar un servidor Firewall, ya que este garantiza la protección de los sitios web que se visiten por internet. Además de evitar que las computadoras se infecten de virus que provienen de internet o de otra red y previene efectos causados por espías incluyendo el lento funcionamiento de los equipos de cómputo, ventanas con mensajes emergentes, cambios no deseados en las configuraciones de Internet y uso no autorizado de la información privada.

En el caso de los laboratorios de centros educativos o empresas, el firewall es necesario para evitar que los usuarios pierdan el tiempo visitando páginas por internet que causan distracción, y a la vez ayuda a aprovechar el tiempo en hora clase y hacer un buen desempeño en el lugar de trabajo.

Con el sistema del servidor Firewall, en este caso el sistema operativo basado en Linux, Endian, el beneficio que aporta, es que es gratuito pero no por ser gratis se limita, y lo mejor es que no requiere de un hardware potente, esto hace de que el firewall Endian sea la mejor opción en cuanto al costo, aparte de los beneficio que aporta al Colegio La Asunción de San Salvador.

Es un sistema operativo fácil de configurar e instalar, guiándose por las instrucciones del manual de usuario, ya que en este se detalla paso a paso el procedimiento a seguir.

3. Recomendaciones

Se recomienda al Colegio La Asunción de San Salvador, implementar un servidor firewall con sistema operativo en base Linux Endian con licencia libre especializada en cortafuegos. A pesar que es gratuito, es la solución para proteger la red de amenazas externas, ofreciendo todos los servicios que brinda un UTM (Gestión Unificada de Amenazas) ya que es fácil de usar e instalar.

Se recomienda al administrador de la red del colegio la Asunción, seguir las instrucciones del manual de usuario, ya que en este se detalla paso a paso el procedimiento a seguir para la instalación y configuración del sistema operativo Endian.

Antes de comenzar la instalación se debe hacer un breve análisis de donde se hará la instalación del servidor Firewall, que cuente con toma polarizado, a una temperatura adecuada y en una zona que no corra riesgos dentro de los laboratorios de informática del Colegio la Asunción.

Es necesario que el encargado de la red del mencionado colegio, deba dar mantenimiento preventivo, es decir, hacer una limpieza interna y externa de la pc que tenga instalado el Sistema operativo Endian y en caso extraordinario lo mejor sería el cambio de un componente interno de la pc, previamente se haya diagnosticado cual ha

sido el error, esto con el fin de mantener funcionando correctamente el servidor Firewall, dentro del colegio la Asunción.

Si el Colegio La Asunción posteriormente cuenta con mayor demanda, y se ve en la necesidad de adquirir uno o varios laboratorios de informática, se le recomienda optar por un servidor firewall con mejores características óptimas de hardware para que funcione satisfactoriamente y de esta manera prevenir fallos.

Otra recomendación, es que se adquiera un software firewall de paga ya que beneficia con más funciones que la versión gratuita y ofrece la asistencia de soporte técnico, de esta manera, se tiene más opciones y beneficios en el control de la red del Colegio La Asunción.

También es recomendable que la unidad del sistema (CPU) que es el servidor firewall quede como protección principal de la red local y como segunda opción el software open DNS, para tener un respaldo de seguridad en la red local del mencionado colegio u omitir el servicio.

4. *Referencias*

Alegsa, L. (2010). *Definición de Manual de usuario*. Recuperado de http://www.alegsa.com.ar/Dic/manual%20de%20usuario.php.

Alvarez, M. A. (2016). *Qué es un proxy*. Recuperado de http://www.desarrolloweb.com/actualidad/.

Cruz, M. & Rodríguez, D.D.V. (2010). *Modelo de Seguridad para la Medición de Vulnerabilidades y Reducción de Riesgos en Redes de Datos.* Recuperado de http://itzamna.bnct.ipn.mx/dspace/bitstream/123456789/8428/1/IF2.52.pdf.

Edward. (2012). *Historia del Firewall*. Recuperado de http://walle.blogspot.com/2012/10/historia-del-firewall.html.

geekland. (2016). *Qué es y para que sirve un firewall*. Recuperado de http://geekland.eu/que-es-y-para-que-sirve-un-firewall/.

Google Sites. (2011). *Ventajas y desventajas del manual de usuario*. Recuperado de https://sites.google.com/site/manualdeusuario2011/ventajas-y-desventajas-del-manual-de-usuario.

Guías Prácticas.com. (2016). *Seguridad en el ordenador firewall por Hardware*. Recuperado de http://www.guiaspracticas.com/seguridad-en-el-ordenador/firewall-por-hardware.

InformaticaHoy. (2016). *Seguridad Informática Tipos de Firewall*. Recuperado de http://www.informatica-hoy.com.ar/seguridad-informatica/Tipos-de-firewall.php.

MasTiposde.com. (2016). *Tipos de Manuales*. Recuperado de http://www.mastiposde.com/manuales.html.

Microsoft. (2016). *¿Qué es un firewall?*.Recuperado de http://windows.microsoft.com/es-419/windows/what-is-firewall#1TC=windows-7.

Pineda, C. (2009). *Manual Endian*. Recuperado de http://es.slideshare.net/ces1227/manual-endian.

Retos en Supply Chain. (2014). *Definición, especificaciones y estructura de un manual de calidad*. Recuperado de http://retos-operaciones-logistica.eae.es/2014/11/definicion-especificaciones-y-estructura-de-un-manual-de-calidad.htm.

Slide Share.net. (2013). *Manual de organizacion*. Recuperado de http://es.slideshare.net/kuphy/manual-de-organizacion-17240645.

Tiposde.Org. (2016). *Tipos de manuales*. Recuperado de http://www.tiposde.org/cotidianos/568-tipos-de-manuales/.

Wikipedia la Enciclopedia Libre.(2016). *Tarjeta de red*. Recuperado de https://es.wikipedia.org/wiki/Tarjeta_de_red.

Anexos

Matriz de Congruencia		
Tema: Instalación y configuración de un sistema operativo que funcione como firewall para protección de la red en el Colegio La Asunción de San Salvador.		
Enunciado del Problema: ¿Será necesario instalar y configurar un Firewall para evitar riesgos y vulnerabilidades en la red del Colegio La Asunción?		
Objetivo General: Identificar e instalar un sistema operativo que funcione como firewall, para la protección de la red del Colegio La Asunción de San Salvador.		
Objetivo Específico 1: Seleccionar una unidad del sistema (CPU) con las características óptimas que funcionará como servidor firewall.	**Objetivo Específico 2:** Utilizar y configurar un sistema operativo basado en Linux, para controlar el tráfico de los sitios que se visiten por internet, y que cuente con antivirus y anti-spyware.	**Objetivo Específico 3:** Crear un instrumento al administrador de la red del Colegio La Asunción para la administración de funciones básicas del servidor firewall.
Alcance 1: Una pc de características óptimas, que funcionará como servidor firewall.	**Alcance 2:** Utilizar y configurar un sistema operativo como firewall basado en Linux, que controle el tráfico de los sitios que se visiten por internet, y que cuente con antivirus y anti-spyware.	**Alcance 3:** Crear un instrumento al usuario para la administración de funciones básicas del servidor firewall.

Producto 1: Una unidad del sistema (CPU) con 12GB de memoria RAM, disco duro de 500GB, 2 tarjetas de Red alámbricas, procesador Dual Core 3.2GHZ, teclado y mouse. De acuerdo al análisis técnico y económico.	**Producto 2:** Sistema operativo Endian.	**Producto 3:** Un manual impreso de la configuración básica del sistema operativo Endian.
Motherboard Biostar	Para máquinas de escritorio, modelo H81MLV3 BIOSTAR, cuenta con las características técnicas necesarias, como son: un socket 1150, que soporta procesadores Pentium i3, i5 y i7, soporta 16GB de memoria RAM, lo suficiente para soportar el sistema operativo Firewall Endian.	
Procesador Intel Dual Core	Procesador Intel Dual Core 3.2GHZ cuenta con una velocidad de Reloj 3.2Ghz como mínimo, con socket 1150, y tiene 3MB de memoria cache.	
Memoria RAM Kingston	Memoria RAM DDR3, se ha optado por dos memorias RAM, la cual será una memoria RAM de 12GB, con un bus de datos de 1333MHZ, lo suficiente para tener en óptimo funcionamiento el servidor Firewall.	
Disco Duro Toshiba	De 500GB, con una velocidad de 7200 rpm, con interfaz SATA; lo que hace más rápido la transferencia de datos.	

Case	Case Genérico, de aluminio polarizado y viene con una fuente de 500W, teclado, mouse, y bocinas; con puertos USB delanteros.
Tarjeta de Red Alambrica:	Sirius Nexxt 1000, con una velocidad de 150 mb/s, incorpora un módulo de chips de avanzada tecnología para facilitar su instalación y garantizar la integración fluida de todos sus componentes. Con un extenso número de controladores.
Software Endian basado en Linux	Es un sistema basado en Linux, en el cual se hacen las configuraciones, y se tiene el monitoreo a través de una interfaz web, Endian tiene el servicio de firewall, antivirus, anti-spyware, con usuario VPN, es la versión gratuita más completa.

Detalle del Presupuesto Proyectado:

Unidad	**Concepto**	**Precio**
1	Motherboard Biostar	$ 54.00
2	Tarjetas de Red alambrica	$ 10.50
1	Procesador Intel Dual Core	$ 73.50
1	Memoria RAM Kingston	$ 87.00
1	Disco Duro Toshiba	$ 54.00
1	Case	$ 32.50
1	Software Endian basado en Linux	$ 00.0
	Total Presupuesto	$ 311.50

Oferta Económica

Se propone la siguiente oferta económica:
Precios obtenidos de la empresa Tecnoservice y R. G NIETO, ya que cumplen con los requisitos indispensables para la realización del proyecto, de acuerdo al cuadro de evaluación económica.

Unidad	Concepto	Precio
1	Motherboard Biostar	$ 54.00
2	Tarjetas de Red alambrica	$ 10.50
1	Procesador Intel Dual Core	$ 73.50
1	Memoria RAM Kingston	$ 87.00
1	Disco Duro Toshiba	$ 54.00
1	Case	$ 32.50
1	Software Endian basado en Linux	$ 00.0
	Total	$ 311.50

San Salvador, 1 de Julio de 2016

Directora General del Colegio La Asunción de San Salvador
Madre Ethel María Saavedra Montoya

Estimada Señora Directora:

Por la presente, estamos expresándole nuestro agradecimiento, por habernos dado la oportunidad de instalar en ese prestigiado centro educativo el servidor Firewall con el sistema operativo basado en Linux Endian (Herramienta de protección y control de internet).

Para que ese proyecto se hiciese realidad, gustosamente aportamos nuestro trabajo, esfuerzo y conocimiento; también aportamos el 50% en efectivo para la compra de: una Motherboard, Tarjetas de Red Alámbrica Sirius Nexxt 1000, Procesador Intel Dual Core de 3.2GHZ, Memoria RAM Kingston de 12GB, Disco Duro Toshiba de 500GB y Case Genérico, de aluminio polarizado que viene con una fuente de 550W, teclado, mouse, y bocinas, con puertos USB delanteros; componentes todos para implementar dicho servidor; todo lo cual, queda como nuestra donación para ese colegio, como una muestra más de agradecimiento.

Sin otro particular, nos despedimos de usted, muy atentamente:

F _____
Jorge Alberto Henríquez Campos
Carnet: 28-3347-2011

F _____
Samuel Eduardo García García
Carnet: 28-6299-2012

Recibido
06/07/16

CORPORACIÓN LA ASUNCIÓN

Portada del Manual

MANUAL INSTRUCTIVO DE INSTALACION Y CONFIGURACION DEL SERVIDOR FIREWALL ENDIAN

REALIZADO POR:

Jorge Alberto Henríquez

Samuel Eduardo García

Para obtener más información de cómo utilizar el Firewall Endian, vaya a www.endian.com. Además, en la página web también puede consultar la sección de soporte técnico, nuevos productos y preguntas frecuentes (FAQ), y realizar la actualización del software, etc.

Introducción

El presente manual está dirigido al administrador de la red del Colegio La Asunción de San Salvador, para hacerle más sencillo detectar los riesgos y vulnerabilidades en la red local y minimizar los mismos; y a su vez, pueda controlar todo el tráfico de los sitios web que se visiten por internet. Así mismo, va dirigido a cualquier persona que desee instalar y configurar el sistema operativo Endian, para la protección de la red o redes que tenga a su cargo.

Desde activar el servidor DHCP, crear perfiles de filtrado web, aplicar las políticas de acceso, además de la configuración de tráfico de salida y bloqueo de dominios, así como también como visualizar los diferentes reportes de las páginas web que se visitan por internet.

Configuración de las funciones principales del Servidor Firewall Endian

-Para con figurar el servidor DHCP, se le da clic en la pestaña servicios, luego clic DHCP server y en configuración, luego se pone el rango de dirección ip que tendrá disponibles el servidor DHPC para asignar ip automáticamente a las computadoras. Después guardar y aceptar.

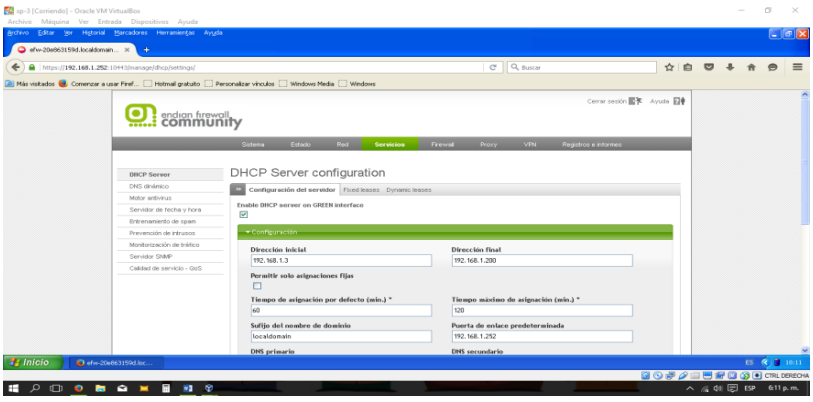


Figura N° 1 Rango de dirección ip disponibles para el servidor DHCP

-Configuración del proxy, en la pestaña proxy, opción http se activa “habilitar proxy http de modo trasparente, esto para que automáticamente las computadoras del Colegio La Asunción se conecten a internet, sin necesidad de configurar cada una de las computadoras.

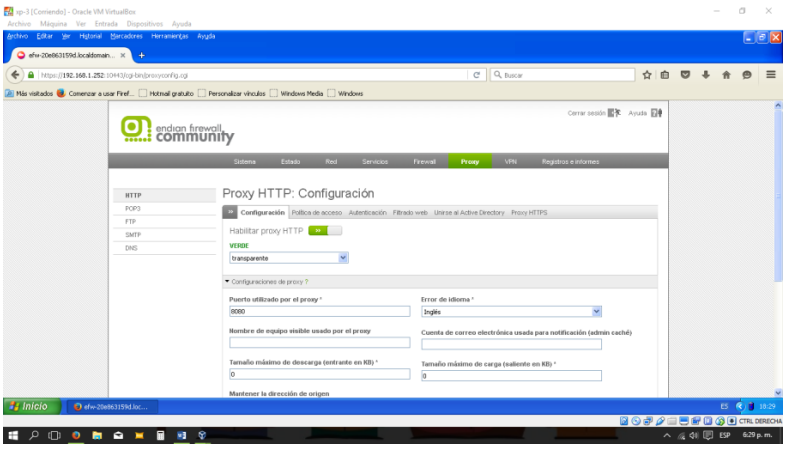


Figura N° 2 Activación del http proxy en modo transparente

-En filtrado web, siempre en pestaña proxy opción http, se tiene que seleccionar rutina de actualizaciones diariamente, luego se añade un nuevo perfil en donde se configuran las categorías de las páginas web que se permitirán y las que se bloquearán.

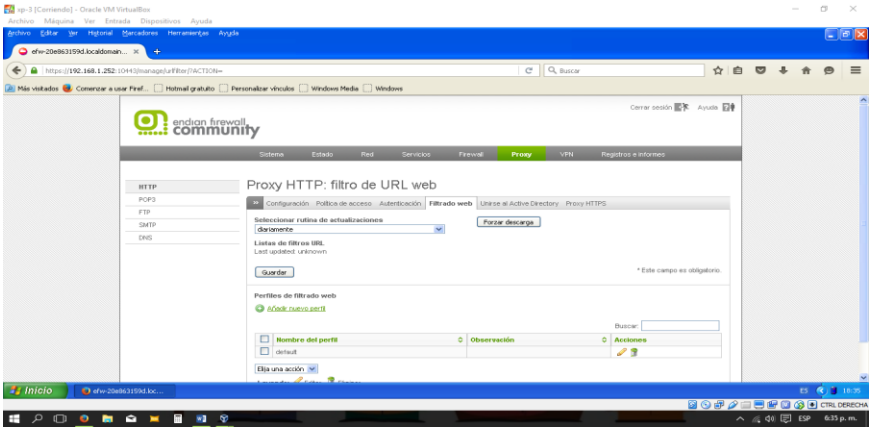


Figura N° 3 Configuración de rutinas de actualizaciones

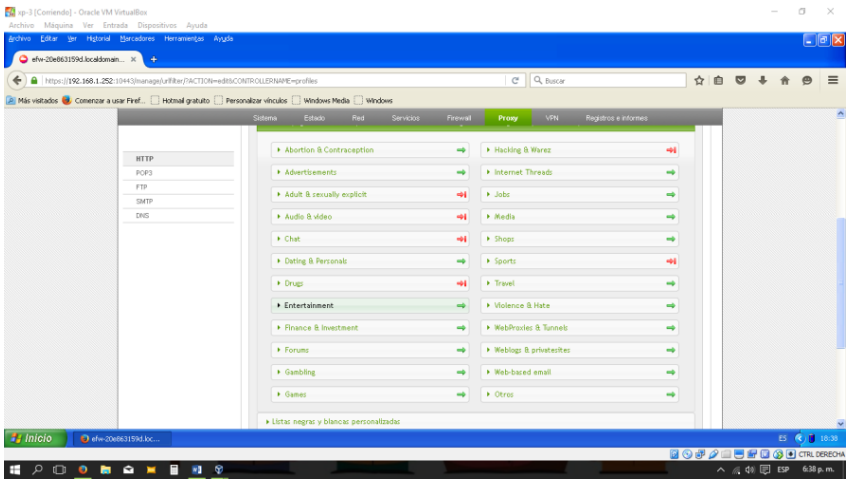


Figura N° 4 Agregar un nuevo perfil de filtrado web

- Para que el perfil de políticas de acceso quede aplicado en toda la red, en la pestaña de política de acceso, se da clic en crear política de acceso.

Tipo de fuente zona verde y a destino cualquiera, y permitir la política de acceso.

Después se selecciona el filtro de perfil que se ha creado, se coloca en primera posición.

Luego clic en guardar y aceptar.

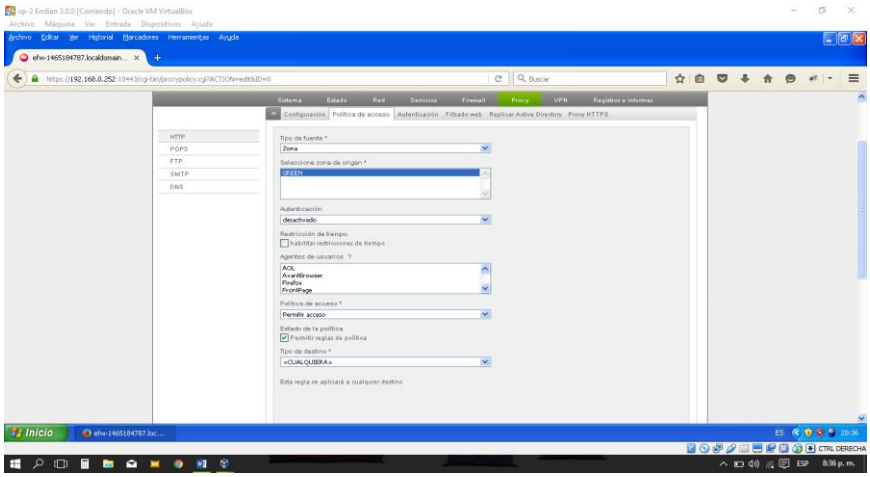


Figura N° 5 Habilitación de la zona verde del registro del Firewall con conexiones salientes

A continuación se detalla paso a paso, la instalación y configuración del sistema operativo Endian:

1) Seleccionar el idioma más conveniente.

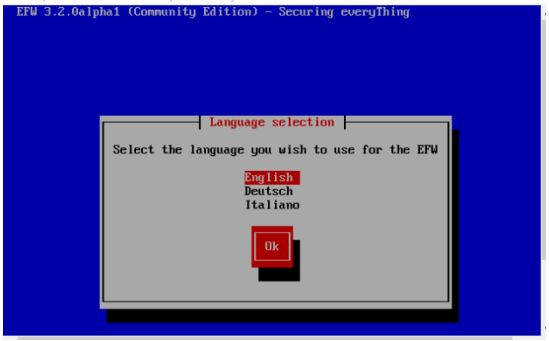


Figura N° 6 Selección del Idioma

2) Luego seleccionar OK, para realizar la nueva instalación.

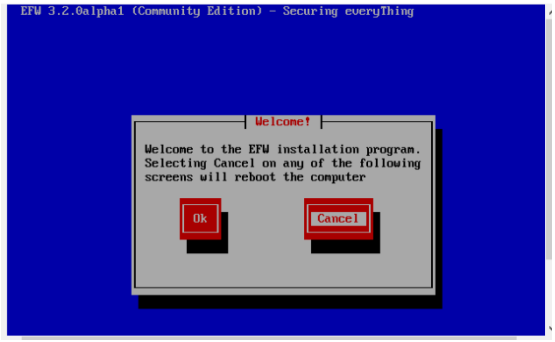


Figura N° 7 Realizar nueva instalación

3) Después aparecerá un mensaje, el cual indica que todo el contenido en el disco se perderá para la instalación de Endian, se selecciona YES.

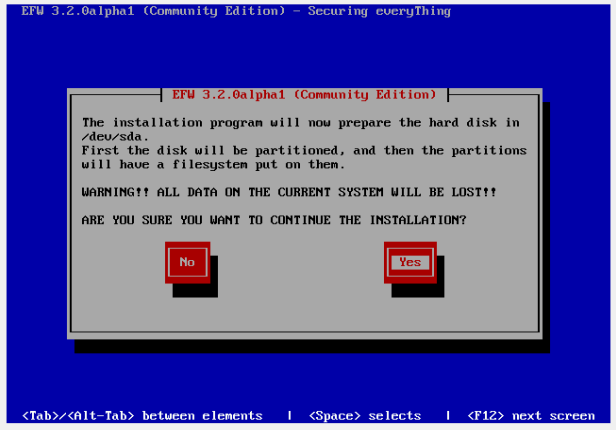


Figura N°8 Perdida del contenido para instalar Endian

4) En caso de que sea un disco duro de poca capacidad saldrá el siguiente mensaje, pero se puede realizar la instalación.

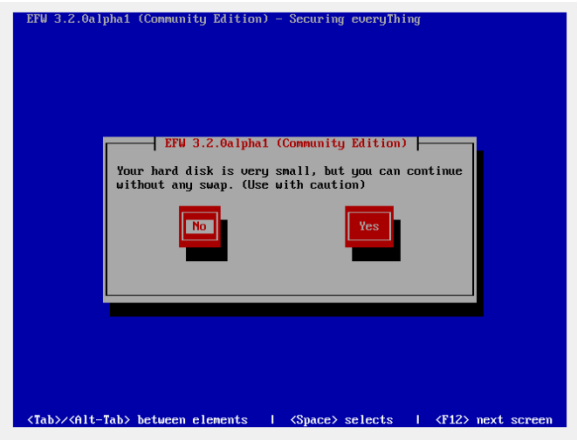


Figura N° 9 Disco duro de poca capacidad para instalar Endian

5) A continuación se formateará el disco para la instalación.

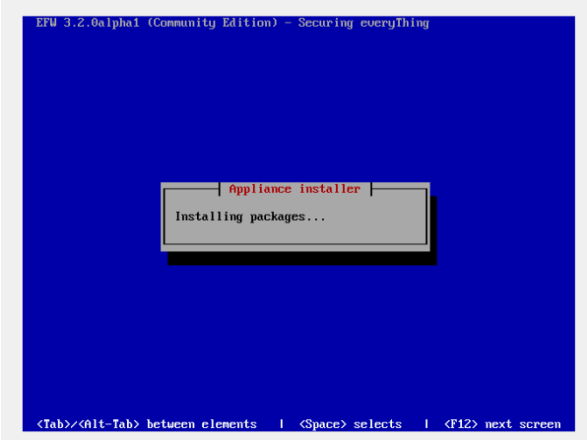


Figura N° 10 Formateo del disco duro

6) Luego aparece el siguiente mensaje, el cuál pregunta si se quiere configurar automáticamente el puerto serial, que el servidor Firewall desea administrar, se le dará clic en No.

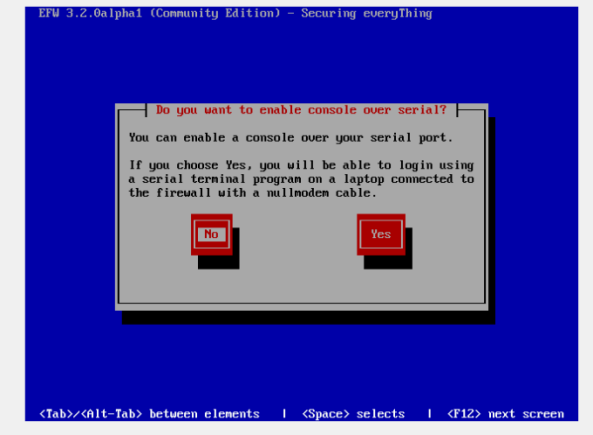


Figura N° 11 Configuración automática del puerto serial

7) Posteriormente se procede a configurar las zonas, se comienza con la zona verde, es donde estarán las computadoras clientes que tendrán el acceso a internet mediante el servidor Firewall.

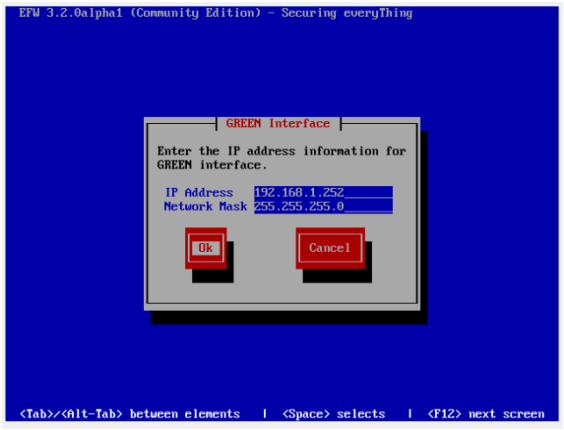


Figura N° 12 Configuración de las zonas

8) Emergerá un mensaje, comunicando que la instalación se ha realizado correctamente, para realizar las configuraciones de parámetros se debe de acceder a través de un navegador web a la dirección y puerto indicado.

Nota: la computadora que se utilizará para la configuración debe de estar en el mismo rango de ip que se asigna en la zona verde.

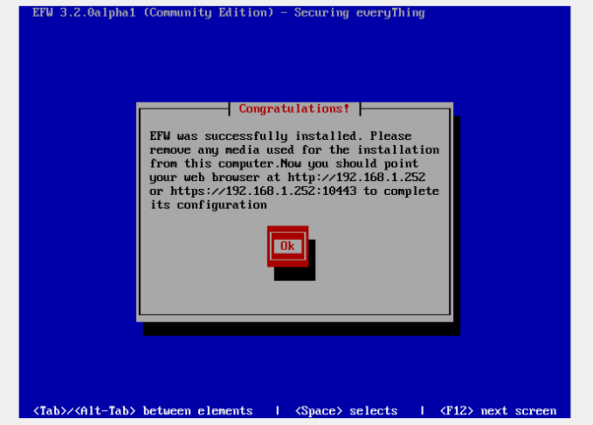


Figura N° 13 Configuración de parámetros

9) Una vez finalizada la instalación, se reiniciará el servidor Firewall y se podrá realizar las configuraciones.

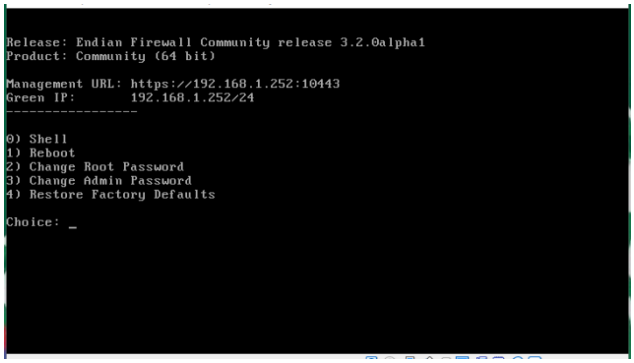


Figura N° 14 Reinicio del Servidor Firewall

10) Luego a través de otra computadora se configura la conexión de área local, se le coloca una ip fija dentro del rango de la zona verde y como puerta predeterminada la ip del firewall, esto se hará para poder acceder a la interfaz web del servidor firewall.

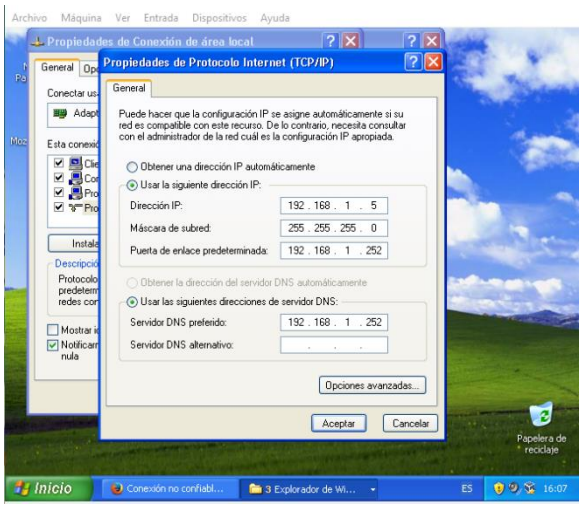


Figura N° 15 Configuración de la conexión de área local

11) Enseguida, en el navegador web se digita la dirección ip y puerto del servidor Firewall en este caso sería https://192.168.1.252:10443, saldrá una advertencia, que la web no está verificada, que es un certificado que automáticamente se crear para poder acceder a la interfaz, se da clic en opciones avanzadas y en añadir excepción.

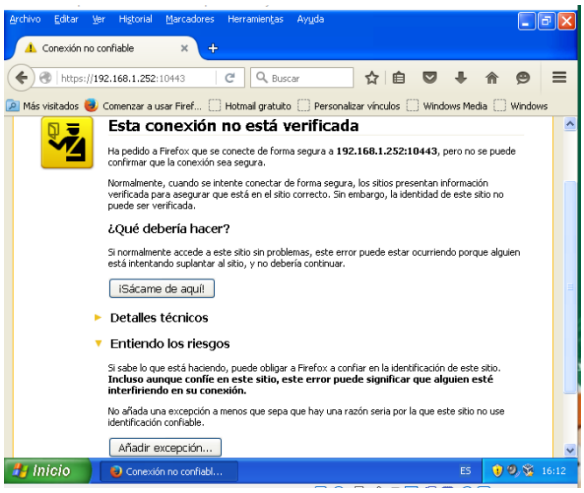


Figura N° 16 Se escribe la dirección ip y puerto del servidor Firewall

12) Después se debe de dar clic, en confirmar excepción de seguridad.

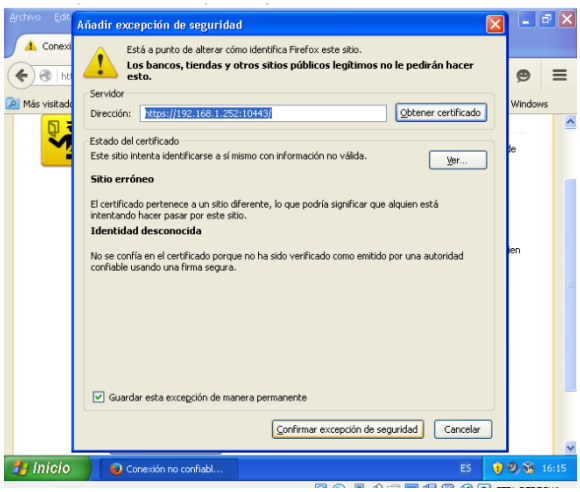


Figura N° 17 Excepción de la seguridad

13) Surgirá la página inicial para la configuración de Endian, se va a siguiente.

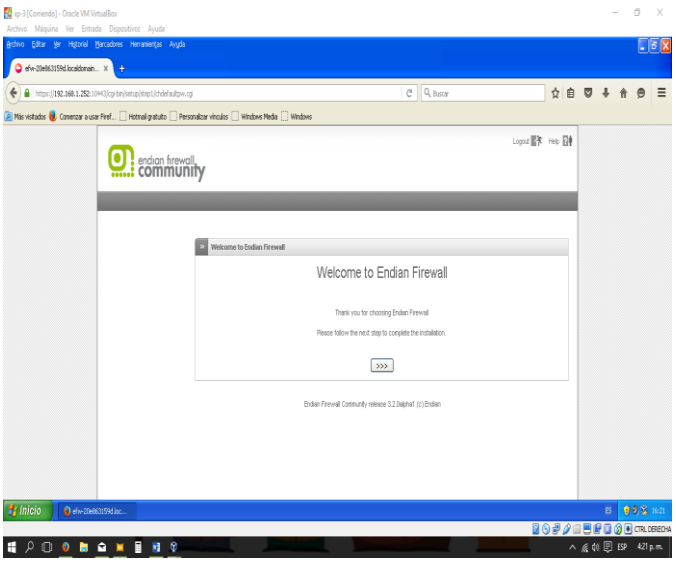


Figura N° 18 Página inicial de la configuración de Endian

14) Se selecciona el idioma y región de preferencia.

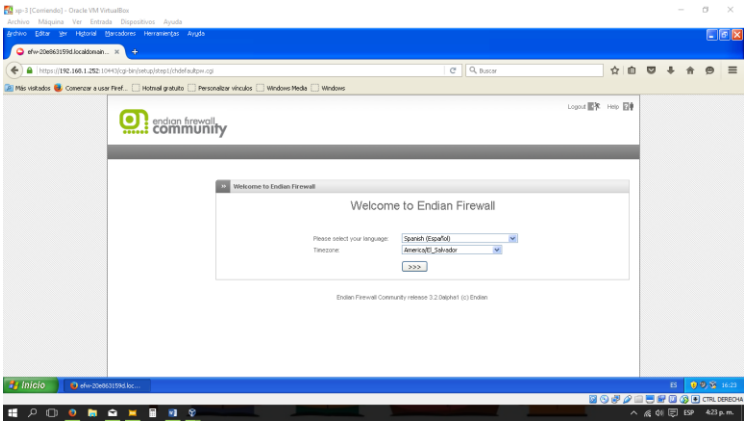


Figura N° 19 Selección del idioma y región

15) Se aceptan los términos de licenciamientos del software Endian.

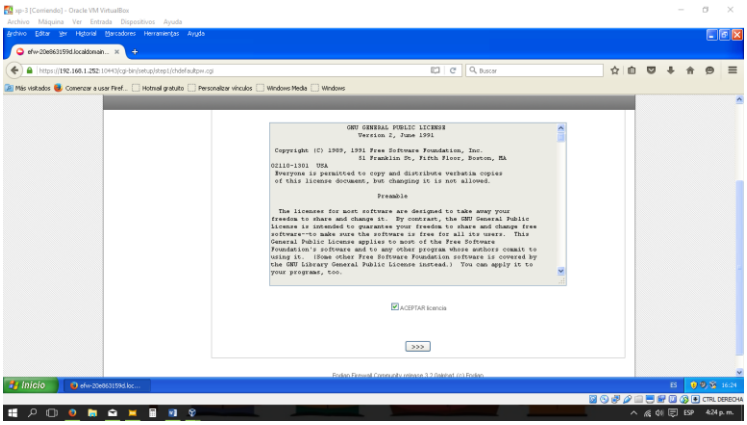


Figura N° 20 Términos de licencia de Endian

16) Si se cuenta con un backup de la configuración de Endian anterior, se puede subir esa configuración, de lo contrario clic en la opción no y continuar.

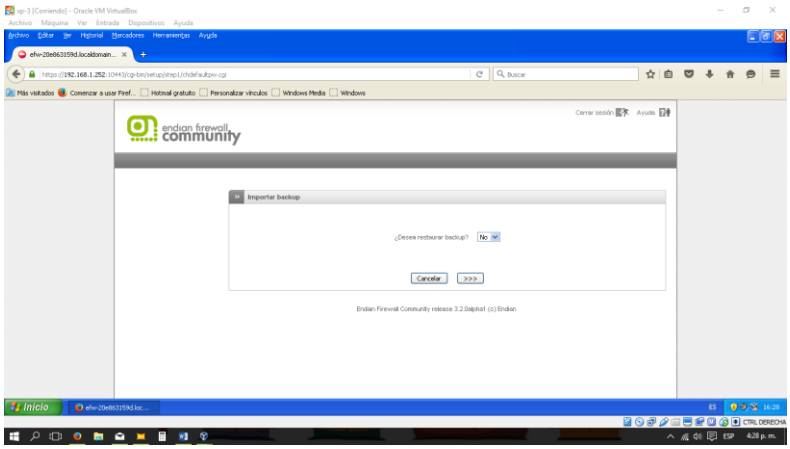


Figura N° 21 Backup de la configuración de Endian

17) Después se establecen las contraseñas de administrador y usuario root.

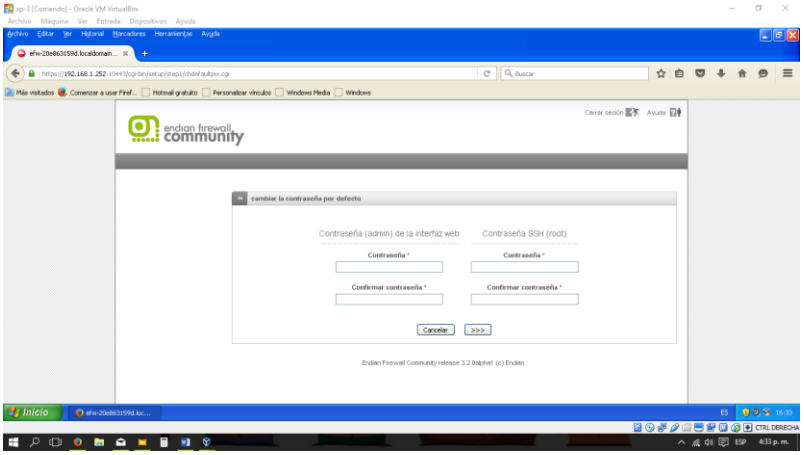


Figura N° 22 Contraseñas de administrador y usuario

18) Luego se selecciona el tipo de red de enrutamiento, y en tipo de enrutamiento en la zona roja, se coloca Ethernet por DHCP.

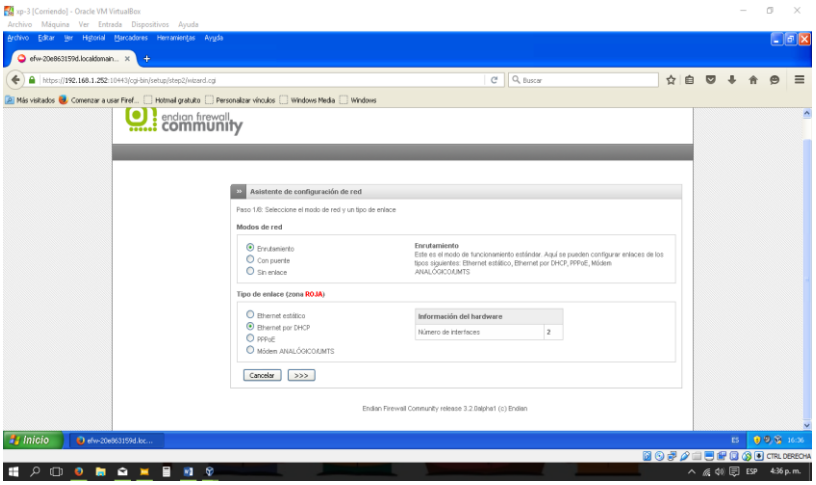


Figura N° 23 Selección del tipo de red de enrutamiento

19) En esta parte se puede configurar la zona azul que es el wifi, y la zona naranja que es la zona DMZ (zona desmilitarizada), donde se encuentran los servidores; en el caso que hubieran aquí, es donde se configuran esas zonas, de lo contrario clic en la opción ninguno.

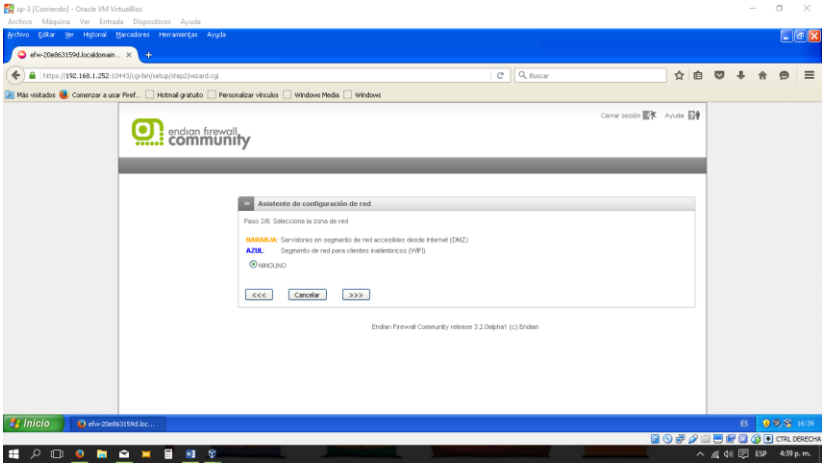


Figura N° 24 Configuración de la zona azul y naranja

20) Posteriormente aparece la zona verde y la ip que se configuró cuando se instaló Endian, al igual, cuál será la tarjeta de red que está conectada a esta zona, aquí se puede cambiar si es necesario la ip que muestra, es la puerta predeterminada donde saldrán las peticiones a internet de las computadoras clientes.

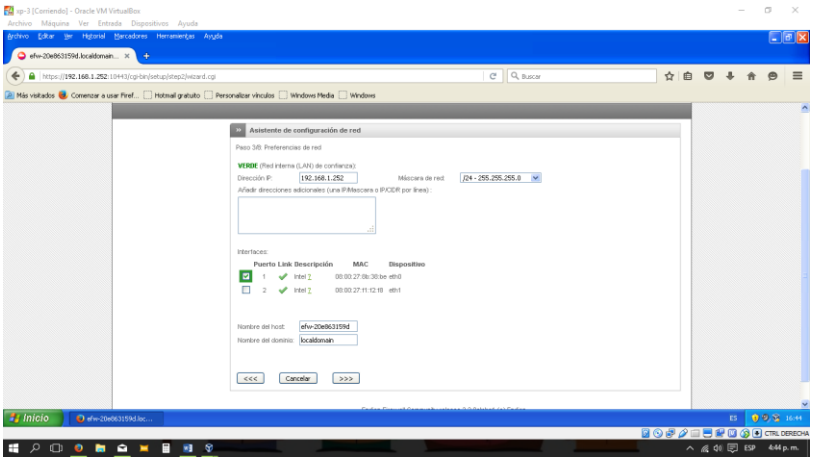


Figura N° 25 Cambio de la ip de ser necesario

21) De igual manera en la zona roja, solo que en este caso será en automático, si se quiere tener una ip fija en la zona roja, previamente debe de configurarse el router que brinda el servicio de internet, de lo contrario solo se deja en automático.

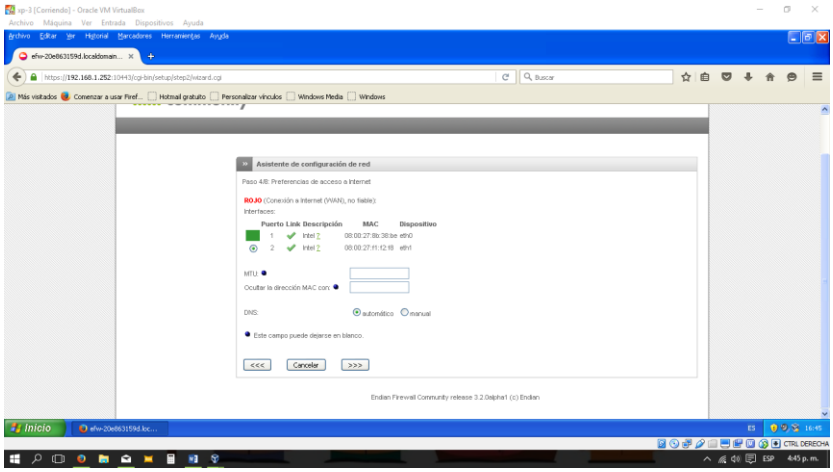


Figura N° 26 ip automática de la zona roja

22) Posteriormente, se coloca el correo de administrador, que puede ser de cualquier dominio como Gmail, Hotmail, etc., esto no es indispensable pero se puede configurar si se desea.

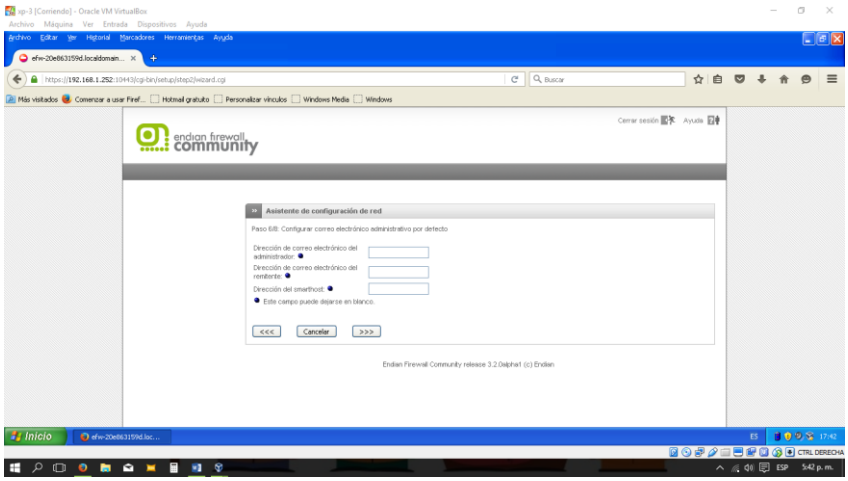


Figura N° 27 Configurar el correo del administrador

23) Luego saldrá un mensaje, comunicando que se ha configurado exitosamente el servidor Firewall Endian, después de esto se reiniciará y quedarán los parámetros que se le configuraron.

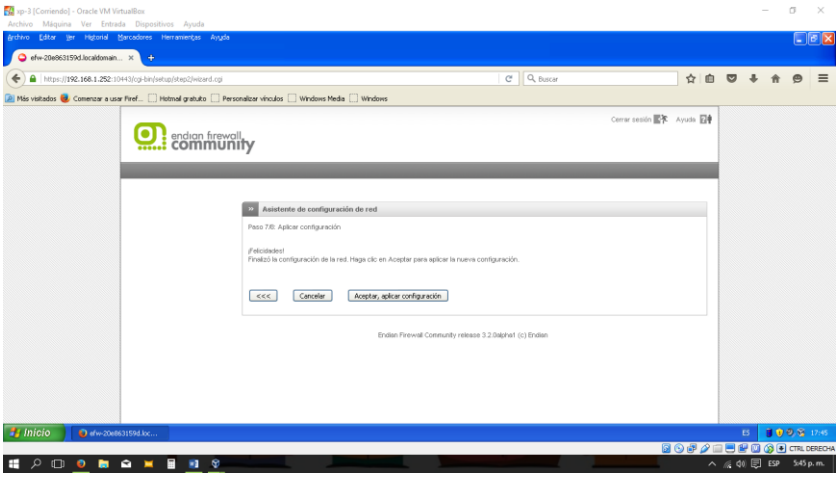


Figura N° 28 Configuración exitosa del Servidor Firewall

24) Enseguida solicitará el usuario y contraseña del administrador para ingresar.

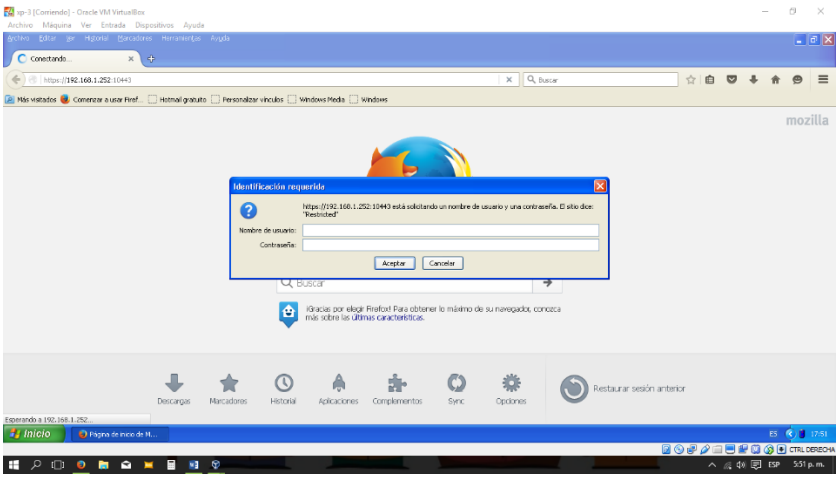


Figura N°29 Introducir usuario y contraseña para ingresar al Servidor Firewall

25) Y surgirá la página principal de Endian, en donde muestra el estado del servidor Firewall, con los gráficos de demanda de internet de los clientes en tiempo real.

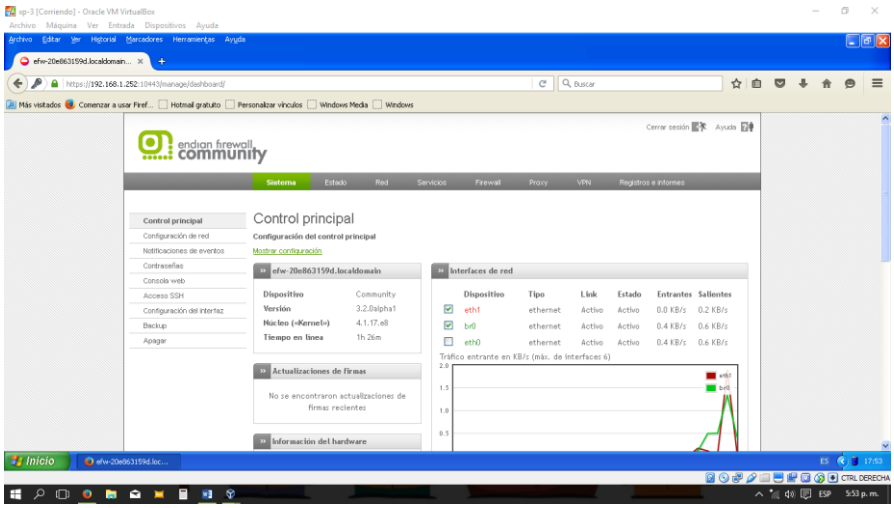


Figura N° 30 Página principal de Endian, mostrando el estado del Servidor Firewall

26) Ahora se debe de configurar el servidor DHCP dentro de la zona verde, para que Endian le coloque una ip automática a las computadoras clientes.

Se va a la opción servicios dentro de la consola de Endian, luego clic en la opción "DHCP server", después clic en la casilla "enable DHCP server on Green interface".

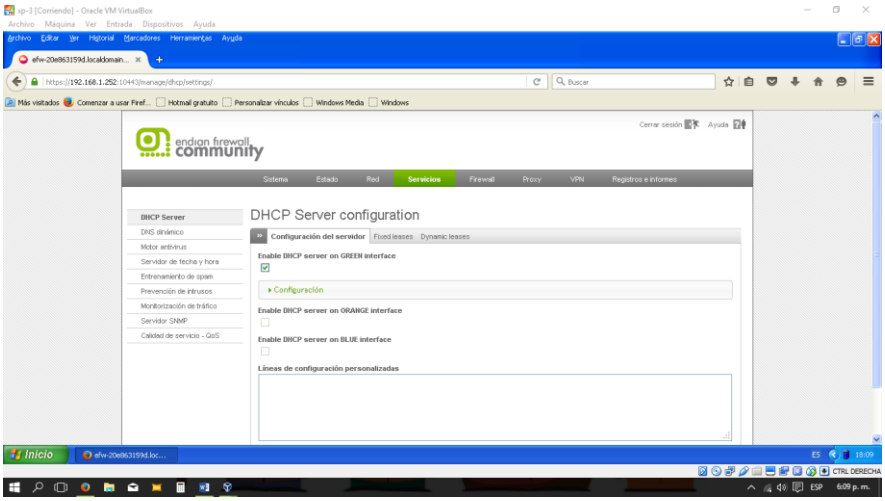


Figura N°31 Configuración del Servidor DHCP en zona verde

27) Posteriormente clic en configuración y se pone el rango de dirección ip que tendrá disponibles el servidor DHPC para asignar a las computadoras. Después clic en guardar y aceptar.

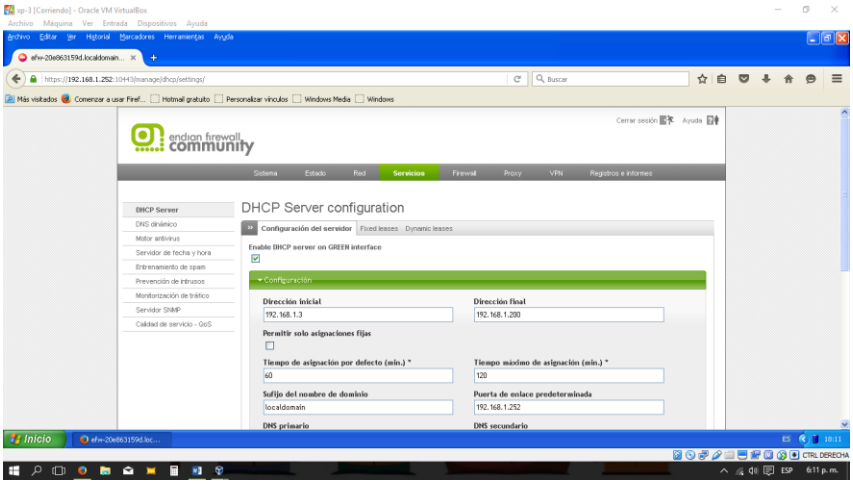


Figura N° 32 Rango de dirección ip disponibles para el servidor DHCP

28) La opción de “prevención de intrusos” debe de estar activada, de esta manera se sabe si hay alguien que este husmeando en la red.

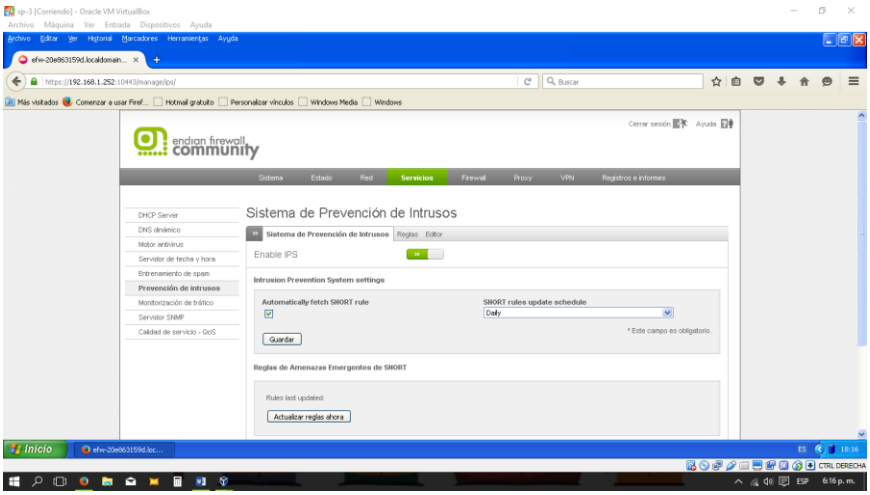


Figura N° 33 Activación de la opción prevención de intrusos

29) También debe de estar activo el “analizador de tráfico en la red”.

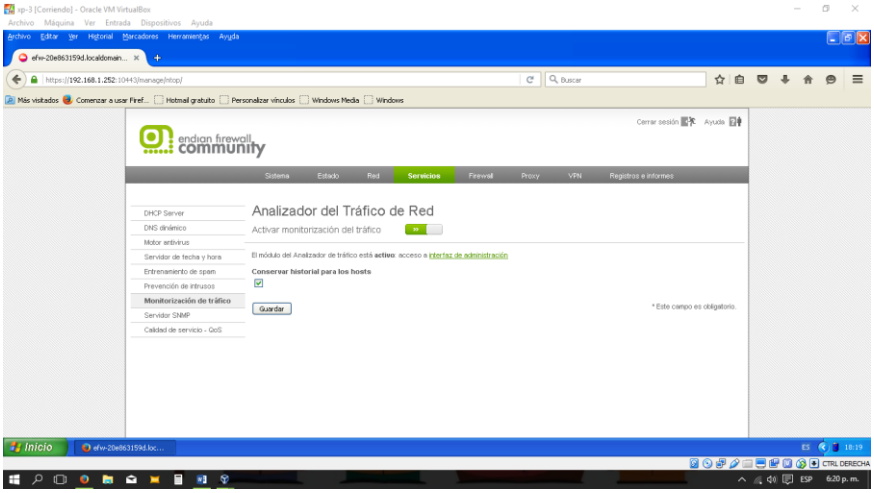


Figura N° 34 Activar el analizador de tráfico en la red

30) Luego en la pestaña “proxy”, opción HTTP, se debe de activar el http proxy de modo trasparente.

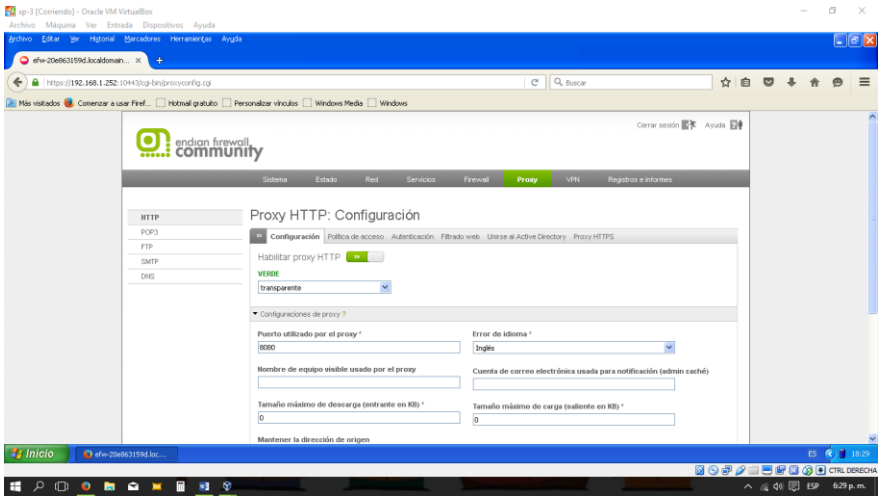


Figura N° 35 Activación del http proxy en modo transparente

31) A continuación en la opción “filtrado web”, se coloca la configuración de rutinas de actualizaciones a diario.

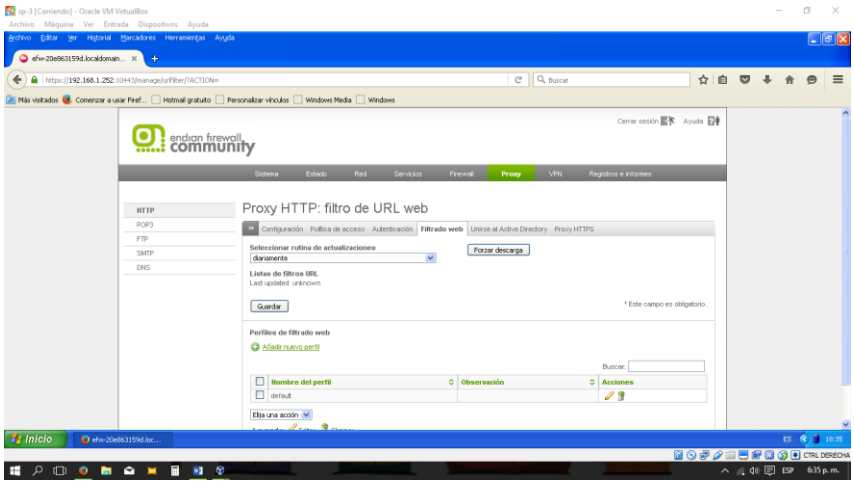


Figura N° 36 Configuración de rutinas de actualizaciones

32) Así mismo se agrega un nuevo perfil de filtrado web, en donde se restringirá el acceso a ciertas páginas por su categoría, se coloca el nombre del perfil.

Clic en nuevo perfil e inmediatamente clic en filtro de páginas conocidas por su categoría.

En seguida, clic sobre la flecha verde para negar el acceso a esa categoría.

Por último, aceptar y guardar los cambios.

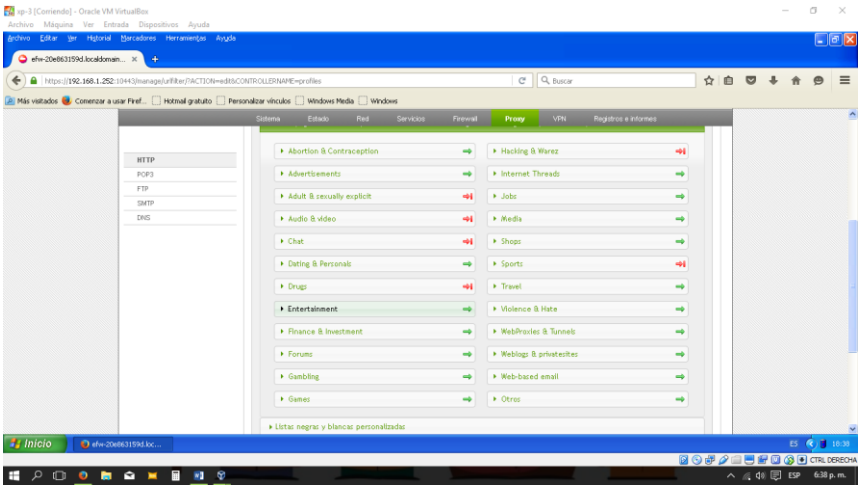


Figura N° 37 Agregar un nuevo perfil de filtrado web

33) Si lo que se quiere es bloquear o dar acceso a una página en específico pero que sea de protocolo http, se hacen en las listas negras y blancas personalizadas donde se pone la URL de la página que se quiera dar acceso o bloquear.

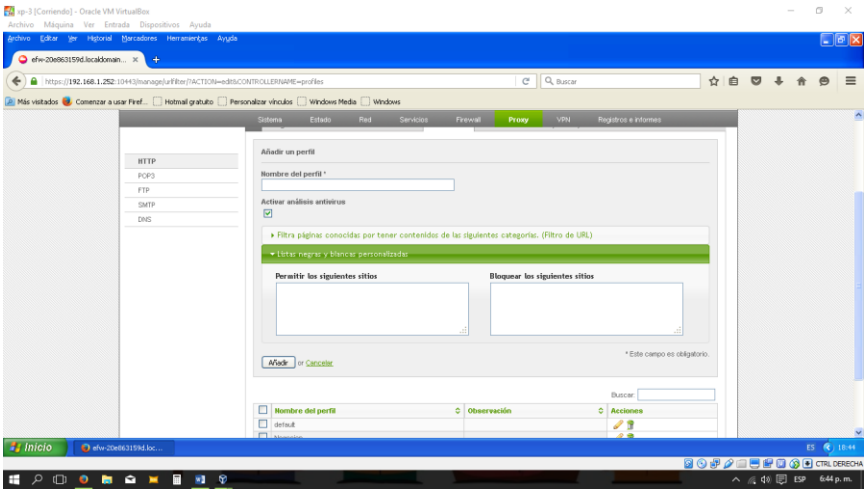


Figura N° 38 Realización de listas negras y blancas personalizadas

34) Para que el perfil de políticas de acceso quede aplicado en toda la red, en la pestaña de política de acceso, clic en crear política de acceso.

Tipo de fuente zona verde y a destino cualquiera, y permitir la política de acceso.

Selecciona el filtro de perfil que se ha creado, se coloca en primera posición.

Luego clic en guardar y aceptar.

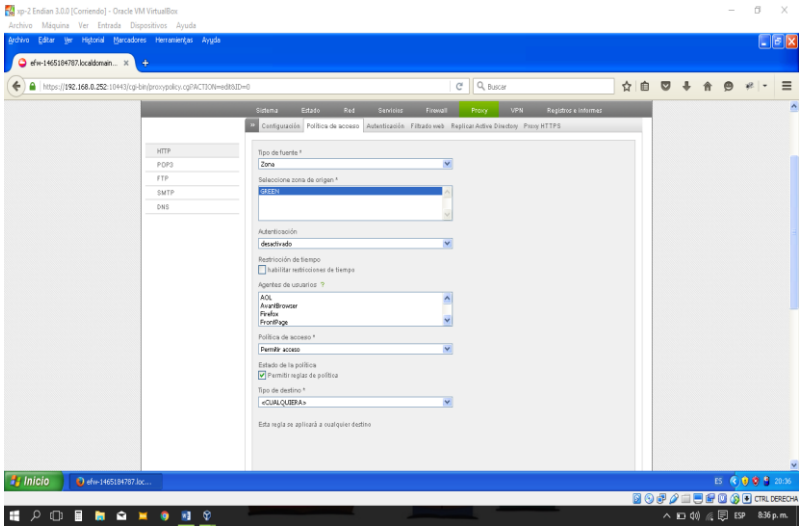


Figura N° 39 Habilitación de la zona verde del registro del Firewall con conexiones salientes

35) Siempre en la pestaña proxy en la opción “FTP”, se habilita la zona verde, y se habilita el registro de Firewall con conexiones salientes. Luego clic en aceptar y guardar.

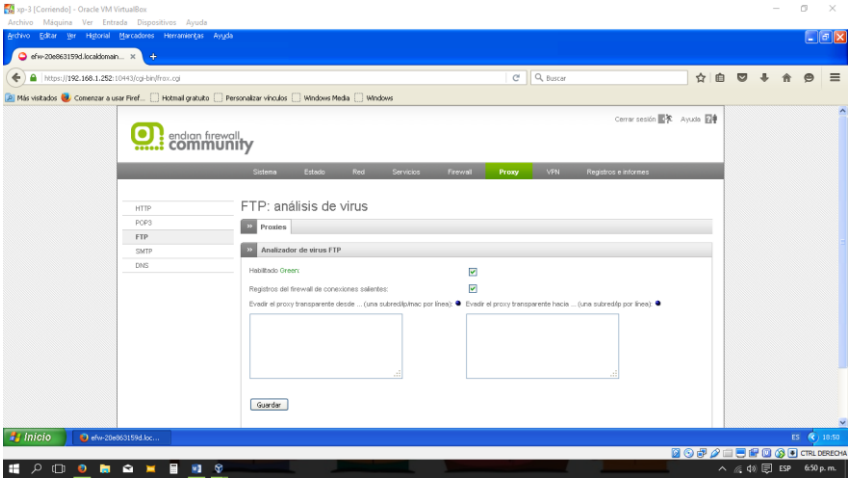


Figura N° 40 Habilitación de la zona verde del registro del Firewall con conexiones salientes

36) En seguida, en la opción SMTP, se activa el proxy SMTP, para la zona verde. Después se guarda y se aceptan los cambios.

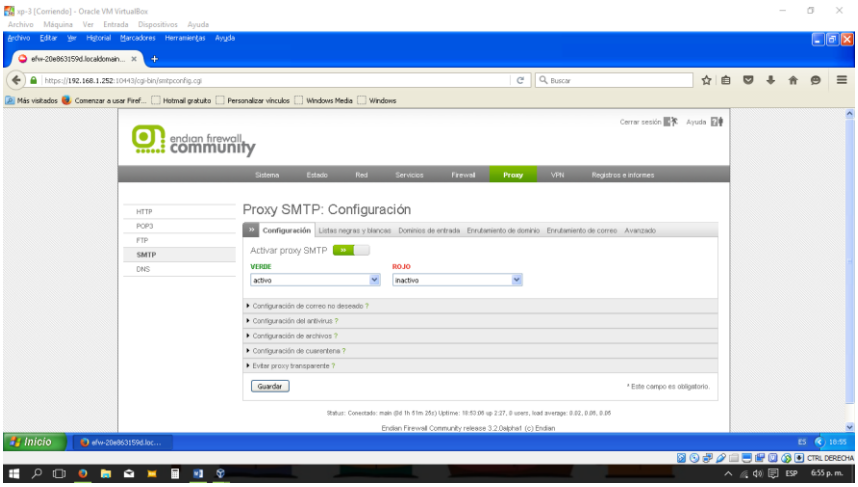


Figura N° 41 Activación del proxy SMTP para la zona verde

37) Posteriormente, en la pestaña “servicios” en opción estado del sistema, se puede ver todos los servicios que se han activado como los que están detenidos. Y así, saber si está completamente configurado el servidor Firewall.

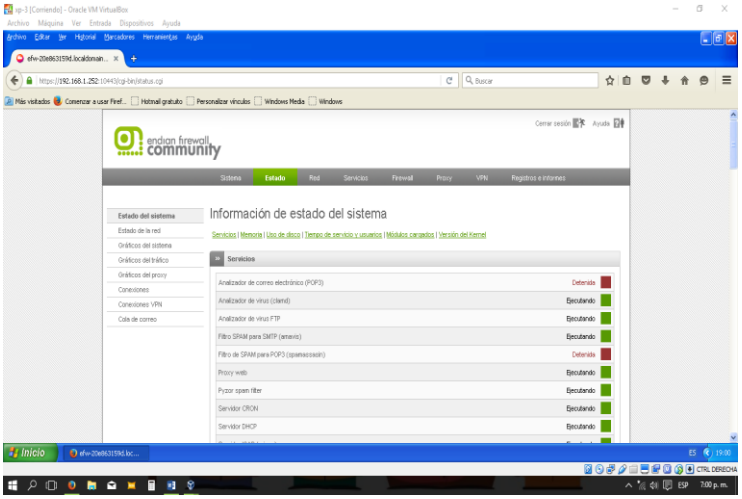


Figura N° 42 vista de servicios que sean activados en la pestaña de servicios

38) En la pestaña de Firewall, en la opción tráfico de salida, se permite el acceso o denegar ciertas paginas como por ejemplo “Facebook”, se coloca el origen zona Green, a destino las ip de Facebook y la acción denegar o permitir el acceso según sea el caso, luego clic en aplicar los cambio y guardar.

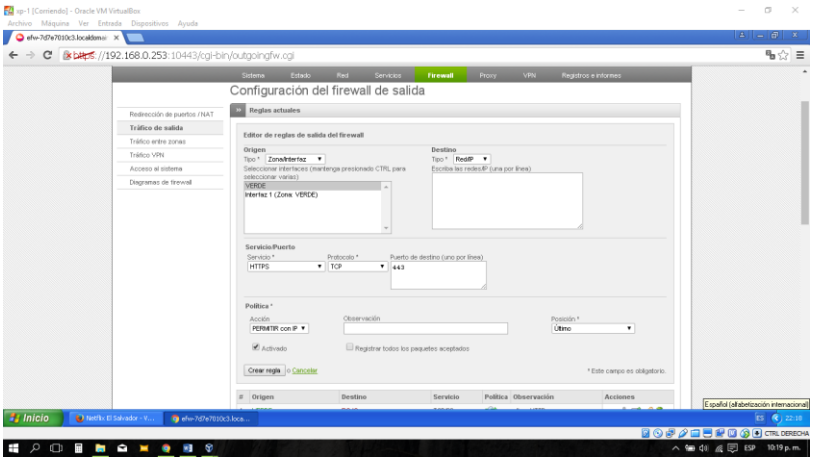


Figura N° 43 Firewall de tráfico de salida, en la pestaña Firewall

39) En la pestaña del proxy, opción DNS en Antispyware, se puede colocar los nombres de los dominios que se deseen bloquear, con esto, no se podrá acceder a esa página en toda la red, ni siquiera teniendo acceso como administrador, porque lo detectará como una página maliciosa.

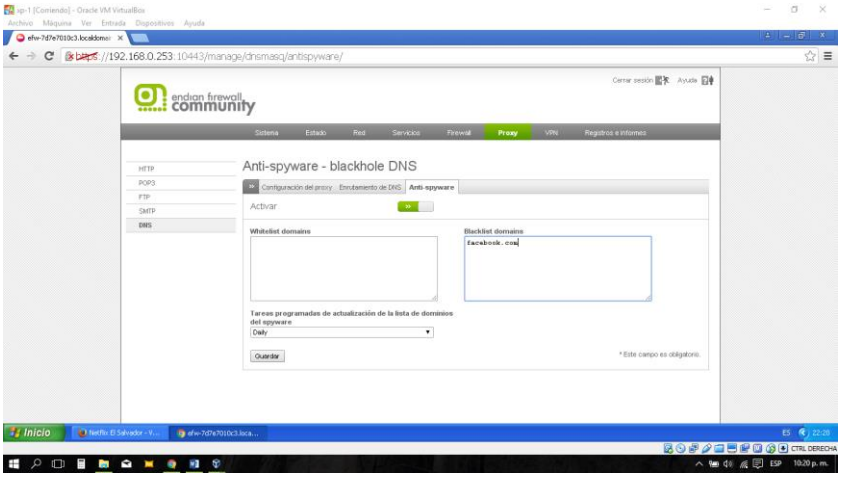


Figura N° 44 Bloqueo de dominio en la pestaña de proxy como antispyware

40) En la pestaña Registros e Informes, se puede visualizar los diferentes tipos de reportes como el estado del sistema, la detección de virus, el firewall, las páginas visitadas, etc.

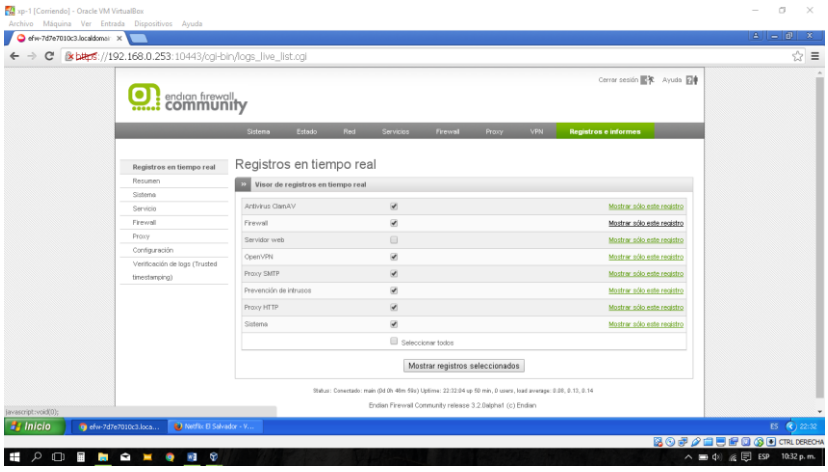


Figura N° 45 Pestaña de reportes e informes diagnósticos de los servicios de internet

41) Por último, en la siguiente imagen se poder visualizar los reportes del servidor Firewall, y muestra la información detallada, de acuerdo lo que se quiere ver.

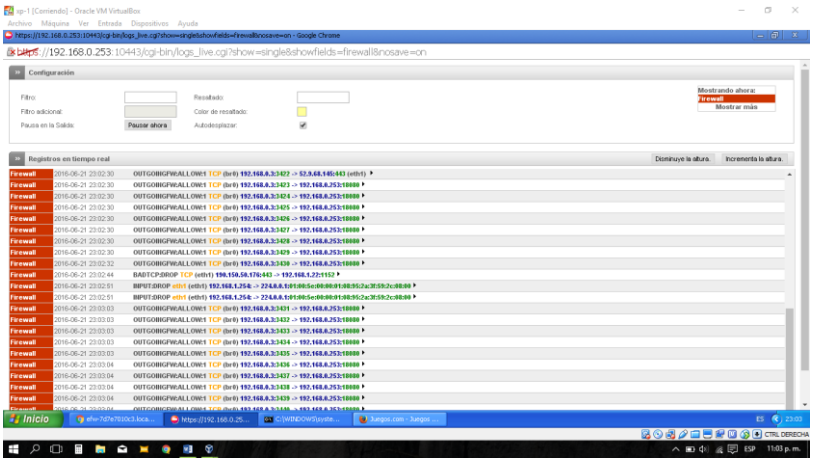


Figura N° 46 Visualización de informes de lo que ha pasado en el servidor Firewall

Glosario

-**Firewall:** Un firewall es software o hardware que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall.

-**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 que está accediendo.

-**Zona Verde:** La zona verde es la zona segura de internet donde se encuentran las computadoras clientes, donde el firewall ya ha bloqueado todo tipo de restricción.

-**Zona Roja:** La zona roja es la zona insegura de internet, es donde de se encuentra el internet libre y donde está todo tipo de contenido, la zona roja es el rauter el servicio que brinda el proveedor de internet.

-**Zona DMZ:** La zona DMZ, es la zona desmilitarizada por sus siglas en inglés (demilitarized zone), es la zona donde se encuentran los servidores, son los que se aíslan de la zona verde y la zona roja, pero que si tienen comunicación entre las zonas, también es conocida como la zona naranja.

-**Interface:** Es la referencia a una conexión activa o inactiva, de las tarjetas de red.

-**UTM:** Por sus siglas en inglés (Unified Threat Management), gestión de unificada de amenazas, Se utiliza para describir los cortafuegos de red que engloban múltiples funcionalidades en una misma máquina. Algunas de las funcionalidades que puede incluir son las siguientes: vpn, anti-spam, anti-spyware, filtro de contenido, antivirus.

-**Dirección IP**: es el número que identifica a cada dispositivo dentro de una red con protocolo IP.

-Http: (en español protocolo de transferencia de hipertexto) es el protocolo de comunicación que permite las transferencias de información en la World Wide Web.

-Https: (en español: Protocolo seguro de transferencia de hipertexto), más conocido por sus siglas HTTPS, es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP.

-TCP: Protocolo de Control de Transmisión, es uno de los protocolos fundamentales en Internet. Muchos programas dentro de una red de datos compuesta por redes de computadoras, pueden usar TCP para crear "conexiones" entre sí a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

-UDP: es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

-SSH: (Secure Shell, en español: intérprete de órdenes seguro) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

-FTP: (siglas en inglés de File Transfer Protocol, 'Protocolo de Transferencia de Archivos') en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

-Modo Proxy: Hacen uso de proxies para procesar y redirigir todo el tráfico interno.

-Modo Trasparente: No redirigen ningún paquete que pase por la línea, simplemente lo procesan y son capaces de analizar en tiempo real los paquetes.

-VPN: es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

-Servidor DHCP: es un servidor que usa protocolo de red 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 quedando 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. Así los clientes de una red IP pueden conseguir sus parámetros de configuración automáticamente.

-**Antispyware:** programa espía es un malware que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador. El término spyware también se utiliza más ampliamente para referirse a otros productos que no son estrictamente spyware.

-**Antivirus Web:** Programa antivirus que, en lugar de estar instalado y ejecutándose de forma permanente en el sistema, funciona a través de un navegador web. Contrasta con los antivirus offline o antivirus tradicionales que se instalan.