SISTEMA DE SEGURIDAD INFORMATICO PARA EL COLEGIO COOPERATIVO ESPIRITU SANTO DE GIRARDOT

EDGAR ANDRES BERMUDEZ SANMIGUEL

DIEGO ALEJANDRO TAFUR TORRES

CORPORACION UNIVERSITARIA MINUTO DE DIOS

FACULTAD DE INGENIERIA DE SISTEMAS

TECNOLOGIA EN REDES DE COMPUTADORES Y SEGURIDAD INFORMATICA

GIRARDOT

2011

SISTEMA DE SEGURIDAD INFORMATICO PARA EL COLEGIO COOPERATIVO ESPIRITU SANTO DE GIRARDOT

EDGAR ANDRES BERMUDEZ SANMIGUEL

DIEGO ALEJANDRO TAFUR TORRES

TRABAJO DE GRADO REALIZADO PARA OPTAR AL TÍTULO DE TECNÓLOGO EN REDES DE COMPUTADORES Y SEGURIDAD INFORMATICA

Presentado a:

FERNANDA ISMELDA MOSQUERA MOTTA

INGENIERA SISTEMAS

CORPORACION UNIVERSITARIA MINUTO DE DIOS

FACULTAD DE INGENIERIA DE SISTEMAS

TECNOLOGIA EN REDES DE COMPUTADORES Y SEGURIDAD INFORMATICA

GIRARDOT

201

Nota de aceptación

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

_____

Jurado

Girardot, 27 de mayo de 2011

Edgar Andrés Bermúdez Sanmiguel

Para mis padres que me apoyaron desde el inicio de mi carrera, mis hermanos, y a todos los docentes de la Universidad Minuto de Dios que me dejaron muchas enseñanzas para el resto de la vida.

Diego Alejandro Tafur Torres

Para mi mama y mi tía quienes han hecho posible que estudie y culmine mi carrera y mi formación como persona, a mis profesores de la Universidad Minuto de Dios quienes me han llenado de sabiduría.

AGRADECIMIENTOS

Queremos agradecerle a la Corporación Universitaria Minuto de Dios la cual nos abrió las puertas del aprendizaje, a los docentes que día a día se esforzaban por llenarnos de sabiduría, que con su esfuerzo y dedicación hoy hacen de nosotros unas mejores personas como también unos excelentes profesionales.

Gracias también al Colegio Cooperativo Espíritu Santo el cual nos abrió las puertas para la realización de nuestro proyecto.

CONTENIDO

INTRODUCCION Pág.

1. PROBLEMA 11

1.1 Formulación

1.2 Descripción

2. JUSTIFICACION 12

3. OBJETIVOS 13

3.1 Objetivo General

3.2 Objetivos Específicos

4. MARCOS DE REFERENCIA 14

4.1 Marco legal

4.2 Marco conceptual

4.3 Marco teórico

5. METODOLOGIA DE DESARROLLO DEL PROYECTO 18

5.1 Participantes

5.2 Materiales

5.3 Procedimientos

5.3.1 Planeación

5.3.2 Análisis

5.3.3 Diseño

5.3.4 Desarrollo

5.3.5 Pruebas

5.3.6 Documentación

6. ANALISIS DE LA SITUACION ACTUAL 22

6.1 Descripción situación actual

6.2 Descripción solución propuesta

BIBLIOGRAFIA

ANEXOS

LISTA DE TABLAS

	Pág.
Tabla 1. Materiales.	18
Tabla 2. Características computadores.	23
Tabla 3. Elementos sala de sistemas.	29

LISTA DE DIAGRAMAS

Pág.

Diagrama uno 1. Diseño de red. 30

LISTA DE ANEXOS

	Pág.
Anexo A. Carta Colegio Cooperativo Espiritu Santo	36
Anexo B. Cotización Ciber-Recarga	37
Anexo C. Cotización Sun Computer	38

INTRODUCCION

La seguridad ha sido el principal tema a tratar cuando una organización desea conectar su red privada al Internet. Sin tomar en cuenta el tipo de negocios, se ha incrementado el número de usuarios de redes privadas por la demanda del acceso a los servicios de Internet tal es el caso del World Wide Web (WWW), Internet Mail (e-mail), Telnet, y File Transfer Protocol (FTP). Adicionalmente los corporativos buscan las ventajas que ofrecen las paginas en el WWW y los servidores FTP de acceso público en el Internet.

Los administradores de red tienen que incrementar todo lo concerniente a la seguridad de sus sistemas, debido a que se expone la organización privada de sus datos así como la infraestructura de su red a los expertos de Internet (Internet Crackers). Para superar estos temores y proveer el nivel de protección requerida, la organización necesita seguir una política de seguridad para prevenir el acceso no-autorizado de usuarios a los recursos propios de la red privada, y protegerse contra la exportación privada de información. Todavía, aun si una organización no está conectada al Internet, esta debería establecer una política de seguridad interna para administrar el acceso de usuarios a porciones de red y proteger sensitivamente la información secreta.

Con este tipo de seguridad lo que buscamos es proporcionarle a la sala de sistemas del Colegio Cooperativo Espíritu Santo una mayor concentración por parte de los alumnos a la hora de la utilización del internet, ya que no tendrán acceso a páginas distractoras, con esto se buscara que el alumno pueda tener un mejor desempeño en la clase. Para que nuestro firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece en torno a este.

En este firewall nosotros no podemos garantizar al Colegio un mejor rendimiento del estudiante lo que si les podemos garantizar es que no van a tener paginas distractoras a la hora de trabajar en internet.

1. PROBLEMA

1.1 FORMULACION

¿Cuál es la mejor manera para realizar un control efectivo a los contenidos o páginas visitadas por los usuarios de internet de las instituciones educativas de Girardot?

1.2 DESCRIPCION

Los docentes del Colegio Cooperativo Espíritu Santo están alarmados por que cuando sus alumnos ingresan a la sala de sistemas no hacen otra cosa que estar en páginas como Facebook, YouTube, Messenger online, ares y descargando software ilegal entonces ellos quieren implementar una medida qué erradique este problema ya que esto está provocando una baja considerable en la falta de atención a lo explicado en clases y no solo eso sino el daño en el sistema operativo por la descarga indiscriminada de virus a este sistema como tal. Como desaparecer esta problemática de raíz pues fácil con la implementación de un firewallque será instalado en un equipo servidor en la sala de sistemas denegando no en lo absoluto el ingreso a internet si no todas las páginas y servicios que afecten con la atención del estudiante frente a la clase y con esto también se proveerá de seguridad toda la red del plantel educativo y los equipos estarán en muy buen estado por mucho tiempo.

2. JUSTIFICACION

Estas son unas de las razones más relevantes por las cuales se establecerá la implementación de un firewall en la red del plantel educativo.

Ahorro de Tráfico: las peticiones de páginas Web se hacen al servidor y no a Internet directamente. Por lo tanto, aligera el tráfico en la red y descarga los servidores destino, a los que llegan menos peticiones.

Velocidad en Tiempo de respuesta: el firewall crea un caché que evita transferencias idénticas de la información entre servidores durante un tiempo (configurado por el administrador) así que el usuario recibe una respuesta más rápida.

Demanda a Usuarios: puede cubrir a un gran número de usuarios, para solicitar, a través de él, los contenidos Web.

Filtrado de contenidos: el servidor puede hacer un filtrado de páginas o contenidos basándose en criterios de restricción establecidos por el administrador dependiendo valores y características de lo que no se permite, creando una restricción cuando sea necesario.

Modificación de contenidos: basándose en la misma función del filtrado, tiene el objetivo de proteger la privacidad en Internet, puede ser configurado para bloquear direcciones y Cookies por expresiones regulares y modifica en la petición el contenido.

Con este proyecto se pretende concientizar a los estudiantes del Colegio Cooperativo Espíritu Santosobre su baja concentración en las clases de sistemas y lo que les afecta el estar interactuando mucho tiempo con este tipo de páginas en la web.

Este proyecto nos sirve de mucha referencia para nuestro emprendimiento como tecnólogos de redes ya que se pretende conseguir plasmar todos nuestros conocimientos e ideas que se han aprendido a lo largo de la carrera universitaria y plasmarlos en ayuda a la sociedad como se intenta en este proyecto beneficiar al Colegio.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Implementar un Firewall que permite el control y la seguridad de la red del Colegio Cooperativo Espíritu Santo utilizando las distintas políticas de seguridad donde se establezca que contenido web puede ser mostrado a los estudiantes.

3.2 OBJETIVOS ESPECÍFICOS

- Analizar las necesidades del por qué instalar un firewall

- Implementación del firewall en la sala de sistemas del Colegio.

- Desarrollar la gran aplicabilidad que tiene un firewall en una red

- Probar todas las características proporcionadas por el firewall para que ayude a la denegación de páginas que afecten el rendimiento académico.

4. MARCOS DE REFERENCIA

4.1 MARCO LEGAL

GNU: La Licencia Pública General de GNU o más conocida por su nombre en inglés GNU General PublicLicense o simplemente sus siglas del inglés GNU GPL, es una licenciacreada por la Free Software Foundation en 1989 (la primera versión), y está orientada principalmente a proteger la libre distribución, modificación y uso de software. Su propósito es declarar que el software cubierto por esta licencia es software libre y protegerlo de intentos de apropiación que restrinjan esas libertades a los usuarios.

Existen varias licencias "hermanas" de la GPL, como la licencia de documentación libre de GNU (GFDL), la Open Audio License, para trabajos musicales, etcétera, y otras menos restrictivas, como la MGPL, o la LGPL (Lesser General PublicalLicense, antes Library General PublicalLicense), que permiten el enlace dinámico de aplicaciones libres a aplicaciones no libres.

El proxy a montar cumple con los requisitos de la GNU ya que este se basa de programas libres, los cuales se dejaran descargar, configurar y modificar al gusto del cliente, al ser un software libre permite que este sea trabajado sin licencia lo cual no representa ningún gasto de dinero.

4.2 MARCO CONCEPTUAL

FIREWALL: se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del firewall, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

DNS: Es una base de datos distribuida, con información que se usa para traducir los nombres de dominio, fáciles de recordar y usar por las personas, en números de protocolo de Internet (IP) que es la forma en la que las máquinas pueden encontrarse en Internet. El DomainNameSystem (DNS), o Sistema de Nombres de Dominio, comprende personas, instituciones reguladoras, archivos, máquinas y software trabajando conjuntamente.

FRECUENCIA: Frecuencia es una medida que se utiliza generalmente para indicar el número de repeticiones de cualquier fenómeno o suceso periódico en la unidad de tiempo.

Ejemplos de ondas de distintas frecuencias; se observa la relación inversa con la longitud de onda.

Para calcular la frecuencia de un suceso, se contabilizan un número de ocurrencias de este teniendo en cuenta un intervalo temporal, luego estas repeticiones se dividen por el tiempo transcurrido.

GATEWAY: gateway (puerta de enlace) es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

El gateway o «puerta de enlace» es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP (NAT: Network AddressTranslation). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada IP Masquerading (enmascaramiento de IP), usada muy a menudo para dar acceso a Internet a los equipos de una red de área local compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa.

INTERFACE: Interfaz es la conexión entre dos ordenadores o máquinas de cualquier tipo dando una comunicación entre ambas.

ISP: proveedor de servicios de Internet (o ISP, por la sigla en inglés de Internet ServiceProvider) es una empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a internet a través de diferentes tecnologías como DSL, Cable, módem, GSM, Dial-up, Wifi, entre otros. Muchos ISP también ofrecen servicios relacionados con Internet, como el correo electrónico, alojamiento web, registro de dominios, etc.

SWITCHES: Un conmutador o switch es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs (Local Area Network- Red de Área Local).

POLITICAS DE SEGURIDAD RED:Los objetivos de la política de seguridad de red son establecer políticas proteger las redes y sistemas de ordenador del uso inadecuado. Los mecanismos de Políticas de Seguridad de Red ayudarán en la identificación y la prevención del abuso de sistemas de ordenador y redes. Las Políticas de Seguridad de Red proporcionan un mecanismo para responder a

quejas y preguntas sobre verdaderas redes y sistemas de ordenador. Las Políticas de Seguridad de Red establecen mecanismos que protegerán y satisfarán responsabilidades legales a sus redes y conectividad de sistemas de ordenador al Internet mundial. Los mecanismos de Políticas de Seguridad de Red apoyarán los objetivos de existir políticas. La responsabilidad de la seguridad de los recursos de calcular descansa con los administradores de sistema que manejan aquellos recursos.

CACHE´: En informática, una cache es un conjunto de datos duplicados de otros originales, con la propiedad de que los datos originales son costosos de acceder, normalmente en tiempo, respecto a la copia en la caché. Cuando se accede por primera vez a un dato, se hace una copia en el caché; los accesos siguientes se realizan a dicha copia, haciendo que el tiempo de acceso medio al dato sea menor.

LISTAS BLANCAS: Listas en donde los emisores de emails poseen buena reputación. Ayudan a resolver el problema de la reputación. Estas listas son creadas y mantenidas por los ISP. Contienen direcciones de IP y dominios que han ganado una buena reputación.

LISTAS NEGRAS: Es una lista de direcciones IP (Protocolo de Internet) o dominios que son percibidos como fuentes emisoras de Spam (correo no solicitado).

SPAM: Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La palabra ¨Spam¨ proviene de la segunda guerra mundial, cuando los familiares de los soldados en guerra les enviaban comida enlatada. Entre estas comidas enlatadas estaba ¨Spam¨ una carne enlatada, que en los Estados Unidos era y es muy común.

VPN: Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

4.3 MARCO TEORICO

Algunos pueden llegar a creer que tanta seguridad en nuestro entorno informático termina por convertirse en algo molesto, pero lo cierto es que nunca viene mal tener una forma extra de protección. La red de redes está repleta de bichos que buscan constantemente puertos abiertos en nuestros cortafuegos para hacer de las suyas, al punto de volverse muy sofisticados en sus métodos, y de paso causar una buena dosis de paranoia. Además, un firewall adicional es una buena forma de reutilizar ese ordenador que tienes depositado en un rincón desde que actualizaste tu sistema. IPCop es una excelente opción, pero no podemos negar que Endian Firewall también lo es.

Su instalación es cuestión de un par de minutos, siempre y cuando tengamos a la mano los datos necesarios para proceder con la configuración. Si hemos lidiado con números IP anteriormente, la instalación de Endian no causará mayores problemas. En el primer paso configuramos la dirección IP de la tarjeta de red denominada *"verde"*, que es la que se encuentra del lado seguro del firewall. El resto de la configuración se realiza a través de la ventana del navegador, accediendo a la página HTTPS.

La primera vez que ingresamos a la página privada, Endian nos recibe con un asistente que configurará el resto de los parámetros. El más importante es sin lugar a dudas el que involucra a la interfaz *"roja"*, la que está del lado inseguro del firewall, expuesta a la red. Lo más lógico es que se trate de una tarjeta de red adicional, pero hay opciones para configurar un módem telefónico en caso de ser necesario. Después del asistente, realizaremos las modificaciones necesarias para adaptar el firewall a su entorno de red. Aquellos puertos que deban ser abiertos pueden especificarse en la sección *"Port Forwarding"*, mientras que también pueden aplicarse reglas especiales para limitar o restringir la transmisión de datos.

Otra opción importante es la del web proxy, que irá descargando información de la red para presentarla al usuario de forma más rápida (las redes locales internas son más veloces que las conexiones promedio de banda ancha), y el sistema de detección de intrusos basado en *Snort*. A pesar de haber usado IPCop durante un buen tiempo, debo reconocer que la forma de manejar las actualizaciones de Snort que posee Endian es sencillamente *fabulosa*. Podemos actualizar la lista de patrones automáticamente, o en caso de ser necesario, podemos descargar el archivo y actualizarlo manualmente. Como adición, Endian Firewall cuenta con soporte para antivirus y un sistema de detección de spam (que según Endian debe ser entrenado a través de un servidor IMAP).

Los únicos puntos flojos que hemos notado en Endian son la traducción incompleta al español (con instancias que comienzan en inglés y terminan en nuestro idioma, y viceversa), y la aparente falta de un sistema de actualización dinámico. IPCop cuenta con un sistema de esas características, lo que permite a los usuarios aplicar actualizaciones sin tener que reinstalar el firewall.

5. METODOLOGIA DE DESARROLLO DEL PROYECTO

5.1 PARTICIPANTES

- Edgar AndrésBermúdez Sanmiguel y Diego Alejandro Tafur Torres, estudiantes encargados de llevar a cabo el proyecto
- Luis Barreto, docente de la universidad cooperativa de Colombia en el espinal y a la vez docente de la corporación universitaria minuto de Dios, el ingeniero nos servirá de apoyo en caso de dudas.
- Mauricio Rodríguez, docente de la universidad de Ibagué y de la corporación universitaria minuto de Dios.
- Blanca Edith Araujo Torres, docente y administradora de la sala de sistemas del colegio cooperativo espíritu santo
- Carlos Julio Barragán, rectos colegio cooperativo espíritu santo.

5.2 MATERIALES

Nombre	Cantidad
equipo servidor	1
tarjeta de red	1
internet	15 horas
transporte	40 pasajes ida y vuelta
rj-45	10
ponchadora	1

Tabla 1.

5.3 PROCEDIMIENTO

5.3.1 PLANEACION

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

Lo primero es mirar la sala a trabajar, verificar las capacidades de cada equipo, las posibles páginas a las cuales se les prohibirá el acceso, una vez realizado esto se buscara que proxy sea el adecuado para prohibir el ingreso a sitios que no son necesarios para los estudiantes.

ACTIVIDADES

- Realizar la respectiva investigación del tema para la elaboración adecuada del proyecto.

- Lectura de manuales y tutoriales encontrados en internet.

- Verificar el estado de los computadores y de la red a nivel de hardware y software.

5.3.2 ANALISIS

Una vez identificados los problemas de los equipos en el ingreso a páginas prohibidas, se procede a buscar el proxy indicado para evitar problemas tanto de páginas como de descargas. Se filtrara la información de los equipos para tener una buena administración de nuestra red.

Se verificara que los equipos sean compatibles con el proxy a trabajar,

ACTIVIDADES

- Conseguir las partes necesarias para armar un buen servidor que permita que el proxy trabaje en óptimas condiciones.

- Buscar que problemas tiene la sala en acceso a páginas no educativas y relacionarlas.

- Investigar y descargar el proxy adecuado dependiendo las necesidades de la sala de internet a trabajar.

5.3.3 DISEÑO

Se ubicara un servidor el cual trabajara con el proxy, para crear este servidor necesitaremos un equipo con las características necesarias para garantizar un 100% de rendimiento, a este servidor solo podrá acceder el administrador de la sala para que nadie pueda des configurar el proxy.

ACTIVIDADES

- Ubicación del servidor para evitar que los alumnos accedan a él.

- Reunirnos con los altos mandos de la institución para llegar a un común acuerdo con las páginas que se les denegara el acceso.

- Proceder a realizar el ensamble del servidor que llevara el proxy a utilizar en el proyecto.

5.3.4 DESARROLLO

El desarrollo de ese proxy se realizara en una sala de la institución educativa donde se buscara bloquear páginas que no sean educativas como también darle una buena administración a la red, mejorar el rendimiento y la fiabilidad a los usuarios.

ACTIVIDADES

- Configuración del proxy como también de los equipos de la sala que navegaran a través de él.

- Realizar pruebas con los equipos de la sala para verificar que el proxy está denegando el acceso a las páginas acordadas.

- En caso de que el proxy presente alguna falla, se verificara una vez más su configuración y se le dará corrección a este problema.

5.3.5 PRUEBAS

Una vez configurado el servidor con el proxy y los equipos de la red se procede a hacer pruebas de descarga de archivos bloqueados, paginas inseguras, para verificar que el proxy está funcionando y está dando el rendimiento esperado.

En caso de que el proxy no del rendimiento esperado se buscara los errores y se aplicaran las correcciones necesarias para que este quede funcionando a placer.

ACTIVIDADES

- Ingresar a páginas ya bloqueadas para verificar el trabajo del proxy.

- Bloquear redes p2p.

- Autenticación de Mac.

5.3.6 DOCUMENTACION

Una vez terminada la parte de instalación, configuración, pruebas y correcciones se entregara al administrador de la sala un documento donde quedaran todos los cuidados que los equipos deben tener, las recomendaciones y los alcances del firewall.

Ubicación del servidor para evitar que los alumnos accedan a él.

Reunirnos con los altos mandos de la institución para llegar a un común acuerdo con las páginas que se les denegara el acceso.

Proceder a realizar el ensamble del servidor que llevara el proxy a utilizar en el proyecto.

ACTIVIDADES

- Se entregara facturas y cotización de los equipos.

- Se creara un documento donde se explicara cómo se ensamblo y configuro el servidor, anexando las investigaciones hechas.

- También se entregara al administrador de la sala un documento para que el pueda utilizar el servidor con el proxy sin ningún problema ni riesgo a des configurar.

6. ANALASIS DE LA SITUACION ACTUAL

Lo primero que se hizo fue una auditoria de la sala de informática del Colegio Cooperativo Espíritu Santo donde analizamos tanto en la parte física como en la lógica la red, lo primero que encontramos es que el rack lo tienen muy desordenado, algunos patch cord tienen botas y otros no, todo está con norma EIA/TIA 568 A, los cables están ubicados en sus canaletas, los equipos básicamente la mayoría están en buen estado; por los lados del sistema operativo todos manejan Windows xp professional, en cuanto a seguridad la sala no manejan nada lo único que utilizan para el bloqueo de páginas de internet es el filtro de seguridad que maneja el internet Explorer.

6.1. DESCRIPCION SITUACION ACTUAL

En estos momentos el cliente necesita que su red de un mejor funcionamiento para las actividades que ellos necesitan, también necesitan que se les dé seguridad en la red como restringir páginas que no son educativas y producen distracción en los alumnos a la hora de clase.

En estos momentos tenemos 2 opciones de firewall para ser instaladas por un lado tenemos el ClearOs que es una distribución Linux basada en CentOS y Red Hat Enterprise Linux, diseñado para su uso en pequeñas y medianas empresas como una puerta de enlace de red y servidor de red con una administración basada en interfaz web.

Otro que tenemos en mente por recomendación del ingeniero Mauricio Rodriguez es el IPCop que tiene como objetivos ser un cortafuegos sencillo, con pocos requerimientos hardware orientado a usuarios domésticos o a pequeñas empresas (SOHO), administrado a través de una interfaz web, con funcionalidades basicas y avanzadas, yendo (a manera de ejemplo) desde el simple filtrado de paquetes hasta la asignación de ancho de banda fijo a cada puesto de trabajo o la configuración de redes virtuales VPN. IPCop se actualiza desde la Interfaz Web de manera muy sencilla, incluyendo actualizaciones del Kernel.

La duda nos pasa es porque ambas herramientas son muy buenas pero el ClearOs ha sido puesto varias veces en práctica por nosotros mientras que el ipcop solo sabemos de el en teoría aún no hemos realizados prácticas y sería bastante arriesgados trabajar con este firewall.

A continuación se anexa inventario de la sala, tanto físico como lógico:

PC 0

MARCA	CARACTERISTICA	UNIDAD	OFFICE	ANTIVIRUS
Generico	WIN XP SP3 PRO	no tiene	2007	AVG
	RAM 512 MB			
	DISCO DURO 80GB			
Tabla 3	PENTIUM 4 "3.0" GHZ			

PC 1

MARCA	CARACTERISTICA	UNIDAD	OFFICE	ANTIVIRUS
hp compaq	WIN XP SP2 PRO	CD	2007	AVG
	RAM 1 GB			
	DISCO DURO 500GB			
	PENTIUM 4 "3.0" GHZ			

PC 2

MARCA	CARACTERISTICA	UNIDAD	OFFICE	ANTIVIRUS
Delux	WIN XP SP3 PRO	CD	2007	AVAST
	RAM 1 .512 MB	DVD		
	DISCO DURO 80GB			
	SEMPROM "1.84" GHZ			

PC 3

MARCA	CARACTERISTICA	UNIDAD	OFFICE	ANTIVIRUS
hp compaq	WIN XP S23 PRO	CD	2007	AVG
	RAM 2 GB			
	DISCO DURO 320GB			
	PENTIUM 4 "3.0" GHZ			

PC 4

MARCA	CARACTERISTICA	UNIDAD	OFFICE	ANTIVIRUS
hp compaq	WIN XP SP3 PRO	CD	2007	AVG
	RAM 2 GB			
	DISCO DURO 320GB			
	PENTIUM 4 "3.0" GHZ			

PC 5

MARCA	CARACTERISTICA	UNIDAD	OFFICE	ANTIVIRUS
Argom	WIN XP SP3 PRO	CD	2007	AVAST
	RAM 2 GB			
	DISCO DURO 500GB			
	PENTIUM 4 "3.0" GHZ			

PC6

MARCA	CARACTERISTICA	UNIDAD	OFFICE	ANTIVIRUS
hp compaq	WIN XP SP2 PRO	CD	2007	AVG
	RAM 2 GB			
	DISCO DURO 40GB			
	PENTIUM 4 "3.0" GHZ			

PC7

MARCA	CARACTERISTICA	UNIDAD	OFFICE	ANTIVIRUS
hp compaq	WIN XP SP3 PRO	CD	2007	AVG
	RAM 2 GB			

Este es el diseño actual de la sala de sistemas del Colegio Cooperativo Espíritu Santo.

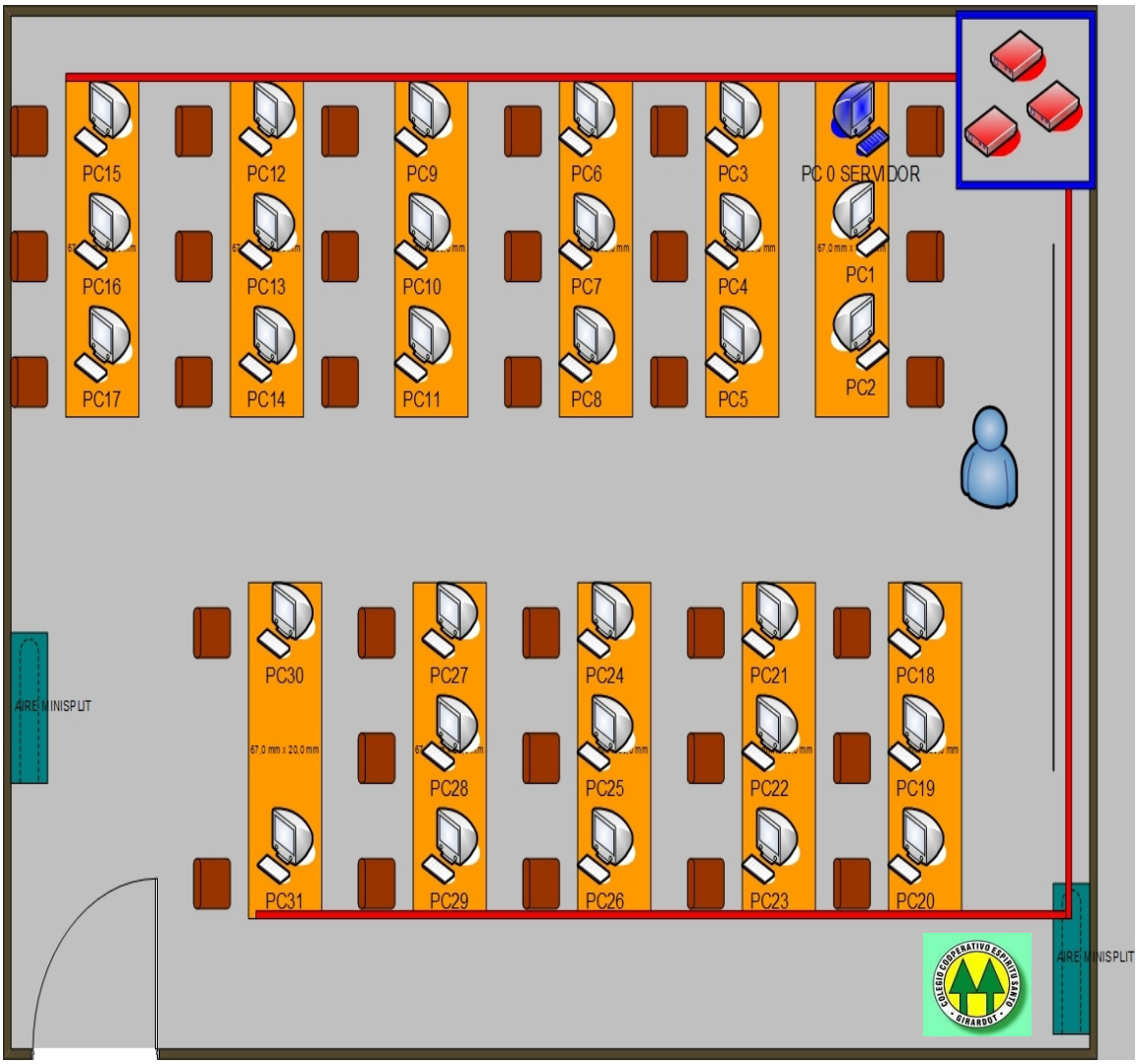

Diagrama 1.

Para el equipo servidor tenemos tres opciones:

La primera es un computador nuevo, para el cual se pasaron cotizaciones para que los encargados de la sala y los directivos tomen la decisión teniendo en cuenta del presupuesto que manejan

La segunda es utilizar un computador de la sala, el problema de esta opción es que la sala quedaría con un equipo menos para el trabajo de los alumnos.

La tercera y mas probable es la de utilizar partes de equipos que tienena defectuosos y con estas partes armar un equipo el cual nos quede como servidor.

Por otra parte hasta el miércoles 11 de mayo solucionar el problema del internet pero lastimosamente la profesora Blanca encargada de la sala de sistemas no se encuentra durante la semana del 9 al 13 de mayo no se encuentra en el colegio debido a unas prácticas que está realizando. El lunes 16 de mayo se realizara una reunión con la profesora Blanca, el rector y otro administrativo del colegio llamado renteria para determinar a que horas del dia 18 de mayo que es miércoles se empezara a realizar la implementación del proyecto.

También instalaremos el firewall que seleccionamos que es el Clearos, solo nos falta la configuración de las ip y las paginas a bloquear que los docentes nos entregaron (salas de chat, redes sociales, paginas xxx y juegos)

En estos momentos le solicitamos al rector nos colabore un inconveniente que se presentó con la ETG que es el ISP del colegio para continuar con el proceso de configuración del firewall.

6.2 DESCRIPCION SOLUCION PROPUESTA

Uno de los aspectos fundamentales para la seguridad de la red es la instalación de un firewall junto con un antivirus de calidad. Es importante instalar esta medida de protección cuando utilizamos los computadores para el acceso a internet.

El firewall crea una barrera entre los datos privados de la red y las amenazas externas que nos pueden atacar cuando estamos conectados.

Un firewall protege la red de varios tipos de ataques, incluyendo:

Gusanos, que se esparcen de computador en computador vía internet y después toman el control del computador.

Bloquea el tráfico de salida para no dejar que determinados protocolos sean utilizados para esparcir los virus que pueden llegar a tener la red.

Por si solo un firewall no impide todos los ataques, pro si no tenemos ninguno instalado basta con conectarse a internet para que la probabilidad de ser infectado en poco tiempo se agrande.

Para la implementación del firewall necesitamos un equipo servidor ya sea nuevo o de segunda, al colegio se le pasaron cotizaciones pero en el momento el presupuesto no les daba para comprar un computador, la salida que le buscamos a esto fue armar un equipo con partes de otro que ya tenían fuera de servicio.

Nos reunimos con los docentes encargados y con el rector para así definir el equipo servidor el cual lo armamos con equipos que se encuentran fuera de servicio en la institución.

Una vez armado nuestro equipo servidor el cual está conformado por una board Intel, con procesador Intel Pentium III de 1.6 GHz, memoria RAM ddr de 512 Mb y un disco duro de 40 Gb, procedimos a la instalación del Clearos que fue el firewall elegido para este proyecto.

Se configuro teniendo en cuenta las características de la red y las peticiones hechas por los encargados de la sala de sistemas del colegio.

Las políticas que se manejaron con este firewall fueron; el bloqueo de páginas no educativas o distractoras para los estudiantes, estas páginas son Facebook (principal puesto que todos los estudiantes los primero que hacen cuando llegan a la sala es abrirlo), paginas XXX y salas de chat. En cuanto a YouTube no fue del todo bloqueado ya que la docente encargada de la sala para algunas de sus clases lo necesita.

En la parte del cacheo dejamos 30 Gb del disco para esta utilidad, con 4 Mb como mínimo por archivo y con descarga ilimitada, el firewall estará en un periodo de prueba de un mes por parte del colegio, depende del señor rector y de los docentes encargados de la sala si el firewall se deja por tiempo indefinido.

Ahora se mostrara una breve descripción de las características generales del ClearOS por las cuales determinamos que era la mejor opción de Firewall.

ClearOS es una red de gran alcance y el servidor de puerta de enlace diseñado para organizaciones pequeñas y entornos distribuidos. Aunque ClearOS viene con una extensa lista de características y servicios integrados (véase el recuadro), la solución es fácil de configurar gracias a la intuitiva interfaz basada en web.

La revolución de código abierto en la industria del software ha hecho posible para proporcionar ClearOS sin costo alguno. Entre otras características, antivirus, antispam, VPN y filtrado de contenidos van incorporadas en el software - sin necesidad de costosas de terceros add-ons. Con ClearOS, puede

evitar costosos proveedor lock-in y formatos propietarios, sino que pueden adoptar los estándares y protocolos abiertos.

Sí. Todas las características básicas que usted ve allí figuran a la derecha son libres de usar e instalar. ClearOS se basa en software de código abierto, por lo que al instalar el motor antivirus - por ejemplo - también obtener las actualizaciones de código abierto que vienen con él! ClearCenter proporciona mejoras de estas características fundamentales de código abierto - por ejemplo, más actualizaciones de antivirus en profundidad la firma - pero no quita el software de código abierto subyacente.

Funciones y servicios generales como:

- Antimalware - antivirus, antiphishing, antispyware
- Antispam
- Gestión de ancho de banda
- Protección de intrusiones, prevención de intrusiones, detección de intrusiones
- Filtrado de protocolos como Peer-to-Peer Detection
- Filtro de contenido
- Web Proxy
- Control de Acceso
- De red de Windows con soporte PDC
- Servicios de archivo e impresión
- Flexshares
- Trabajo en grupo con Outlook Connector
- Servidor de correo - POP, IMAP, SMTP, Webmail, Recuperación
- Filtrado de correo - Antispam, Antimalware, lista gris, Cuarentena
- Archivo de Correo
- Base de Datos con MySQL
- Servidor web con PHP Apoyo

En estos momentos el firewall ya se encuentra funcionando en la sala del colegio cooperativo espíritu santo, la docente de la sala de sistemas Blanca Araujo a la cual se le dio una breve inducción (mientras le entregamos el manual de usuario) para que sea la administradora del firewall y pueda hacer los ajustes que ella encuentre convenientes para así darle una mejor utilización al firewall y sacarle el máximo provecho a esta herramienta.

BIBLIOGRAFIA

ACEITUNO CANAL, Vicente.Seguridad de la información: expectativas, riesgos y técnicas de protección. 2004, 176 p.

CARBALLAR, José Antonio. WI-FI instalación, seguridad y aplicaciones. 2007, 319 p.

DHANJANI, Nitesh.La Nueva Generación Hacker. 2010, 320 p.

FOROUZAN, Behrouz.Transmisión De Datos Y Redes De Comunicaciones. 2002, 462 p.

GOMEZ VIEITES, Álvaro.Enciclopedia de la seguridad informática. 2007,664 p.

HUIDOBRO MOYA, José Manuel. Comunicaciones en redes WLAN. 2005, 336 p.

KAARANEN, Heikki.Redes UMTS: arquitectura, movilidad y servicios. 2006, 584 p.

KUROS, James F y ROSS Keith W.Redes de computadores: un enfoque descendente basado a internet. 2004, 740 p.

ROLDAN David; HUIDOBRO MOYA, José Manuel.Redes y Servicios de banda ancha. 2003, 432 p.

RAYA CABRERA, José Luis. Redes Locales. 2005, 352 p.

TANENBAUM, Andrew S. Redes de computadoras. 2003, 912 p.

ANEXOS

Girardot, 16 de Marzo de 2011

Señores(a) Colegio Cooperativo Espíritu Santo

Mediante la presente queremos pedir el debido permiso para realizar un proyecto llamado SISTEMA DE SEGURIRDAD INFORMATICO PARA LAS INSTITUCIONES EDUCATIVAS DEL MUNICIPIO DE GIRARDOT el cual consta de instalar y probar un software especializado llamado "FIREWALL" para la seguridad interna de la red del colegio el cual permitirá mantener a los estudiantes controlados en cuanto a las páginas que visitan en la red, hasta el bloqueo de la misma ya que los estudiantes sabes distintos medios de como entrar a páginas como: FACEBOOK, YOUTUBE, MESSENGER, PAGINAS XXX, ETC; Sabiendo que hoy en día es una constante que afecta el rendimiento de los estudiantes en el municipio de Girardot y por ese motivo pretendemos realizar la prueba y funcionalidad por parte de los estudiantes de la CORPORACION UNIVERSITARIA MINUTO DE DIOS, VI SEMESTRE DE REDES DE COMPUTADORES Y SEGURIDAD INFORMATICA.

Muchas gracias por su atención otorgada a la presente

Cordialmente

EDGAR ANDRES BERMUDEZ SANMIGUEL

C.C 1070601779

DIEGO ALEJANDRO TAFUR TORRES

C.C 1070594620

Anexo A.

Ciber-Recarga

COMPUTADORES, TONNER Y CARTUCHOS
CENTRO DE SERVICIO

Puedes contar con Nosotros !

Señor(a) :

COLEGIO COOPERATIVO ESPIRITU SANTO

Girardot, 28 de Abril 2011

Combo Computador de Mesa

Athlon 64 LE-1660 AM2 2.8Ghz 1Mb 65NM45W FSB 2000Mhz Oem DDR2 2048Mb 128x64 PC2 6400 800Mhz Twin KBox, PSU 250w, Span Kbd, Opt Mouse, w/ Card Reader 18.5" LG TFT Svga LCD Wide Monitor, DVD-RW 22X Interna SATA Black H.Disk 1000Gb 7200RPM SATA 32MB

PRECIO: $876.000

Precio con descuento $788.400

10% DESCUENTO Pago contado En Efectivo

CORDIALMENTE

Monica Osorio.

Monica Osorio Toledo
Ciber-Recarga
Cra 12 No 21-77 B/ Sucre
TEL 8350544-8353767 - 3153176330

Cra 12 No 21-77 B/ Sucre Tels (571) 8350544-8353767

Girardot - Cundinamarca

Anexo B.

SUN COMPUTER
Tecnología sin limites...

Puedes contar con Nosotros !

QBEX

Señor(a) :

COLEGIO COOPERATIVO ESPIRITU SANTO

Girardot, Mayo de 2011

AMD Athlon 64

COMPUTADOR QBEX TWIN ATHLON

TWIN **Procesador Athlon LE1660** 2.8GHZ 65NM 45W 2800Mhz RAM **DDR2 DE 2GB** 128x64, Disco Duro H.Disk **1000Gb,** 7200 rpm Sata 32 MB. Unidad Quemador de DVDRW (DVDRW), T.Red 10/100, Teclado, Mouse Optico, Monitor LCD 18.5" LG o Samsung, 7 puertos usb, Lector multitarjetas. Linux Operating System

PRECIO: $867.500

Precio con descuento **$737.400**

15% DESCUENTO Pago contado En Efectivo

CORDIALMENTE

CAMILO TRUJILLO

Sun Network Systems Ltda
Cra 12 No 21-39 B/ Sucre
TEL 8353520- 8352726

Cra 12 No 21-39 B/ Sucre Tels (571) 8353520 – (571) 8352726
msn: ventas1.sun@hotmail.com
Girardot - Cundinamarca

Anexo C.