ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y
TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN
DEL TÍTULO EN INGENIERÍA

IMPLEMENTACIÓN DE UNA RED SEGURA PARA LOS LABORATORIOS DEL DEEE UTILIZANDO UN DISPOSITIVO UTM

Cristian Guerra C.

SANGOLQUÍ – ECUADOR

2011

AGRADECIMIENTO

Agradezco a Dios por haberme dado la fuerza, dedicación y tiempo necesarios para cada día ir cumpliendo mis objetivos.

A mi familia, en especial a mi madre por darme ánimos a cada momento, a mi padre que desde siempre, hasta siempre y desde cualquier lugar me va a dar ese empuje en momentos de flaqueza y a mis hermanos por darme ese motivo para seguir adelante.

A los Ingenieros, Carlos Romero y Darwin Aguilar por la guía y apoyo que recibí en el desarrollo del presente proyecto de grado; sus observaciones y recomendaciones hicieron que el objetivo planteado inicialmente se cumpliera a cabalidad.

Cristian D. Guerra C.

PRÓLOGO

Este proyecto de grado proporciona a la red del Departamento de Eléctrica y Electrónica seguridades a nivel de capa de aplicación en el stack de modelo TCP/IP, filtrado web, reconocimiento de usuarios, funcionalidades de red en capa 2, informes de eventos diarios gestionados por el Administrador de la red y recuperación ante falla unificados en un solo software UTM (Unified Threat Management) con interfaz web al cual se puede acceder por cualquiera de las direcciones públicas asignadas a las interfaces del servidor y por el puerto 443/TCP, usado para la transferencia segura de páginas web HTTPS/SSL.

Se incluyen estudios de vulnerabilidades actuales y clásicos que atacan las redes principalmente de las universidades, considerando el hecho de que la mayoría de intrusiones a cualquier red provienen de los mismos usuarios; también se desarrolla un estudio de la mayoría de protocolos usados internamente y así determinar cuáles son los destinos que generan mayor consumo de red, de esta manera se pueden establecer medidas de restricción a páginas consideradas como fraudulentas o a su vez no necesarias dentro de un recinto universitario y estudio.

Para el desarrollo del proyecto se cuenta con un estudio de la red del DEEE tanto físico como lógico, en el que se verifican desempeños antes y después de la implementación del mismo, con el propósito de que el servidor sea adaptado a la topología actual de la red, añadiendo servicios y manteniendo los que actualmente se tienen levantados, gestionados por el administrador sobre una interfaz amigable y de fácil configuración, de tal manera que la actualización de los servicios y funciones puedan ser en cualquier momento actualizados.

ÍNDICE DE CONTENIDOS

CAPÍTULO III

SOLUCIONES GENERALES PARA DOTAR DE SEGURIDAD A LA RED DEL DEEE

CAPÍTULO IV

INSTALACIÓN DE LOS UTMs EN LA RED DEL DEEE

CAPÍTULO V

PRUEBAS DE OPERACIÓN, CONCLUSIONES Y RECOMENDACIONES

ANEXOS

ÍNDICE DE FIGURAS

CAPÍTULO I

CAPÍTULO II

CAPITULO IV

CAPITULO V

ÍNDICE DE TABLAS

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

CAPÍTULO I

SEGURIDAD EN REDES

1.1. INTRODUCCIÓN

Hoy en día, tal y como se presentan los avances tecnológicos, así mismo se presentan los ataques a redes tanto públicas como privadas, al punto de que no existen redes seguras sino simplemente redes fiables. Entendiéndose como red fiable a toda aquella red que se supone responderá tal y como el planeador de la misma espera que lo haga; es decir, al menos cumplirá con una política de seguridad actualizada y que no sea fácilmente vulnerada.

A breves rasgos, se tiene entendido que una red fiable debe poseer 3 aspectos: confidencialidad, disponibilidad e integridad. Confidencialidad porque a la red sólo deberán acceder aquellas personas autorizadas a hacerlo y que se entiende, no compartirán dichos privilegios con entidades externas al sistema. Disponibilidad porque cada una de los

elementos pertenecientes a una red deberán estar accesibles y la gran parte del año. Por último, integridad porque estos elementos de la red sólo podrán ser modificados[1] por quienes son autorizados a hacerlo. Como se ve claramente, cada uno de estos tres elementos depende el uno del otro, y son los que hacen de una red robusta ante ataques.

Lo que ese pretenderá hacer en el presente proyecto es integrar en un solo dispositivo de red a la mayoría de los elementos de protección con los que hoy en día se puede contar para una red, como son: Antispam - Antiphishing - Filtro de contenidos - Antivirus - Detección/Prevención de Intrusos (IDS/IPS); mismos que serán implementados en una red ya estructurada y que se encuentra operando. De tal manera que ésta red (red del Departamento de Electrónica de la ESPE) quede operando al finalizar dicho propósito con las tres características ya expuestas anteriormente (Disponibilidad, Confidencialidad e Integridad).

Los tres elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos. Por hardware entendemos el conjunto formado por todos los elementos físicos de un sistema informático, como CPUs, terminales, cableado, medios de almacenamiento secundario (cintas, CD-ROM) o tarjetas de red. Por software entendemos el conjunto de programas lógicos que hacen funcional al hardware, tanto sistemas operativos como aplicaciones, y por datos el conjunto de información lógica que manejan el software y el hardware, como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos. Aunque generalmente en las auditorías de seguridad se

[1] MODIFICAR, se entiende por escribir, modificar, editar o borrar.

habla de un cuarto elemento a proteger, los fungibles[2]. En el presente proyecto no tomaremos en cuenta la seguridad ni de éstos fungibles ni del hardware, sin embargo si se los tomarán en cuenta ya que para la implementación de un dispositivo UTM, se requiere saber de las capacidades con las que cuenta un servidor o el elemento de red donde será implementado, así como también la dimensión de la red a proteger y el tipo de información que posee. Indudablemente los datos constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar.

Adicionalmente, y como parte de una política de seguridad se va a citar otras medidas de seguridad que se pueden tomar en cuenta al instalar una red, y que es el tipo de sistema operativo con el que va a operar la misma. Actualmente, los sistemas corriendo en LINUX se sabe que son los que sufren una cantidad de amenazas mucho menor que los que corren en WINDOWS. Por lo que implementar una red a base de LINUX es un muy buen comienzo. Así como también aislar los servidores, routers, switches, etc., y protegerlos de un corte de energía o de la falla de uno de ellos (para lo cual se deberá tomar en cuenta tener redundancia).

[2] FUNGIBLES, elementos que se gastan o desgastan con el uso continuo, como papel de impresora, tóners, cintas magnéticas.

1.2. CONCEPTOS BÁSICOS

En el mundo de las redes, y según los conceptos que se manejan hoy en día, existen a manera general de ver las cosas, cuatro tipos de vulnerabilidades, representados en la ***Figura 1.1.***

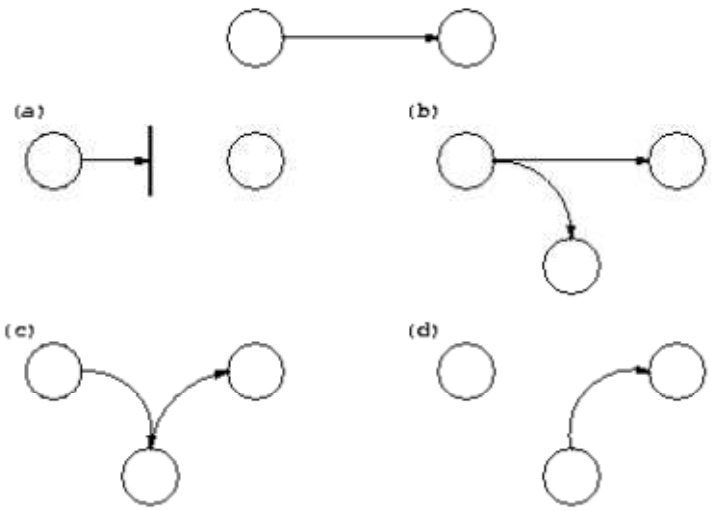

Figura1.1 Flujo normal de información entre emisor y receptor y posibles amenazas: (a) interrupción, (b) interceptación, (c) modificación y (d) fabricación.

Como se puede apreciar en el gráfico, hay cuatro tipos de amenazas con los que se puede atacar a una red, Interrupción, Interceptación, Modificación y Fabricación, todos referidos a los datos. Interrupción se refiere a cuando un objeto del sistema se pierda, quede inutilizable o no disponible. Interrupción, si es que un elemento no autorizado consigue

acceso a cualquier objeto del sistema. Modificación es cuando éste elemento no autorizado, además de conseguir entrar en el sistema, puede modificarlo, alterarlo o dañarlo. Finalmente, es un ataque de fabricación cuando se trata de una modificación destinada a conseguir un objeto similar al atacado de tal manera que sea casi imperceptible la distinción entre el objeto original y el "fabricado".

En la gran mayoría de publicaciones relativas a la seguridad informática en general, tarde o temprano se intenta clasificar en grupos a los posibles elementos que pueden atacar nuestro sistema. Con frecuencia, especialmente en las obras menos técnicas y más orientadas a otros aspectos de la seguridad, se suele identificar a los atacantes únicamente como personas; esto tiene sentido si hablamos por ejemplo de responsabilidades por un delito informático. Pero en este trabajo es preferible hablar de elementos y no de personas: aunque a veces lo olvidemos, nuestro sistema puede verse perjudicado por múltiples entidades aparte de humanos, como por ejemplo programas, catástrofes naturales, etc., la cuestión es que si un usuario pierde un trabajo importante a causa de un ataque, poco le importará que haya sido un intruso, un gusano o un simple error del administrador que haya abducido un disco duro.

Sin embargo, para el presente proyecto se identificarán plenamente en primera instancia, cuáles son los factores que vulneran una red. Es así que, la mayoría de ataques a un sistema van a provenir de personas que, intencionada o inintencionadamente, pueden causarnos enormes pérdidas. Generalmente se trataría de "piratas" que intentan conseguir el máximo nivel de privilegio posible aprovechando alguno de los riesgos lógicos de los que se hablará a continuación, especialmente agujeros de software, para lo cual, acciones como permanecer atento a vulnerabilidades de éstos, restricción de servicios o utilización de

cifrado de datos, hacen que estas intromisiones se minimicen. Los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para nuestros sistemas; generalmente se dividen en dos grandes grupos: los atacantes pasivos, aquellos que entran al sistema pero no lo modifican o destruyen, y los activos, aquellos que dañan el objetivo atacado, o lo modifican en su favor. Generalmente los curiosos y los crackers realizan ataques pasivos (que se pueden convertir en activos), mientras que los terroristas y ex-empleados realizan ataques activos puros; los intrusos remunerados suelen ser atacantes pasivos si nuestra red o equipo no es su objetivo, y activos en caso contrario, y el personal realiza ambos tipos indistintamente, dependiendo de la situación concreta.

- **Personal.-** Las amenazas a la seguridad de un sistema provenientes del personal de la propia organización rara vez son tomadas en cuenta; se presupone un entorno de confianza donde a veces no existe, por lo que se pasa por alto el hecho de que casi cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática puede comprometer la seguridad de los equipos. Aunque los ataques pueden ser intencionados, lo normal es que más que de ataques se trate de accidentes causados por un error o por desconocimiento de las normas básicas de seguridad: un empleado de mantenimiento que corta el suministro eléctrico para hacer una reparación puede llegar a ser tan peligroso como el más experto de los administradores que se equivoca al teclear una orden y borra todos los sistemas de ficheros; y en el primer caso, el atacante ni siquiera ha de tener acceso lógico ni físico a los equipos, ni conocer nada sobre seguridad.
- **Ex-empleados.-** Otro gran grupo de personas potencialmente interesadas en atacar nuestro sistema son los antiguos empleados del mismo, especialmente los que no abandonaron el entorno por voluntad propia (y en el caso de redes de empresas, los que pasaron a la competencia). Generalmente, se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema que conocen perfectamente para dañarlo como venganza por algún hecho que no consideran justo, pueden insertar troyanos, bombas lógicas, virus o simplemente conectarse al sistema

como si aún trabajaran para la organización (muchas veces se mantienen las cuentas abiertas incluso meses después de abandonar la universidad o empresa), conseguir el privilegio necesario, y dañarlo de la forma que deseen, incluso chantajeando a sus ex-compañeros o ex-jefes.

- **Curiosos.-** Junto con los crackers, los curiosos son los atacantes más habituales de cualquier red. Se recuerda que los equipos están trabajando en entornos donde se forma a futuros profesionales de la informática y las telecomunicaciones (gente que a priori tiene interés por las nuevas tecnologías), y recordemos también que las personas suelen ser curiosas por naturaleza; esta combinación produce una avalancha de estudiantes o personal intentando conseguir mayor privilegio del que tienen o intentando acceder a sistemas a los que oficialmente no tienen acceso. Y en la mayoría de ocasiones esto se hace simplemente para leer el correo de un amigo, enterarse de cuánto cobra un compañero, copiar un trabajo o comprobar que es posible romper la seguridad de un sistema concreto. Aunque en la mayoría de situaciones se trata de ataques no destructivos (a excepción del borrado de huellas para evitar la detección), parece claro que no benefician en absoluto al entorno de fiabilidad que podamos generar en un determinado sistema.
- **Crackers.-** Los entornos de seguridad media son un objetivo típico de los intrusos, ya sea para fisgonear, para utilizarlas como enlace hacia otras redes o simplemente por diversión. Por un lado, son redes generalmente abiertas, y la seguridad no es un factor tenido muy en cuenta en ellas; por otro, el gran número y variedad de sistemas conectados a estas redes provoca, casi por simple probabilidad, que al menos algunos de sus equipos (cuando no la mayoría) sean vulnerables a problemas conocidos de antemano. De esta forma un atacante sólo ha de utilizar un escáner de seguridad contra el dominio completo y luego atacar mediante un simple *exploit* a los equipos que presentan vulnerabilidades; esto convierte a las redes, a las de empresas, o a las de ISP en un objetivo fácil y apetecible para piratas con cualquier nivel de conocimientos, desde los más novatos (y a veces más peligrosos) hasta los expertos, que pueden utilizar toda la red para probar nuevos ataques o como nodo intermedio en un ataque a otros

organismos, con el consiguiente deterioro de imagen (y a veces de presupuesto) que supone para una universidad ser, sin desearlo, un apoyo a los piratas que atacan sistemas teóricamente más protegidos, como los militares.

- **Terroristas.-** Por *terroristas* no debemos entender simplemente a los que se dedican a poner bombas o quemar autobuses; bajo esta definición se engloba a cualquier persona que ataca al sistema simplemente por causar algún tipo de daño en él. Por ejemplo, alguien puede intentar borrar las bases de datos de un partido político enemigo o destruir los sistemas de ficheros de un servidor que alberga páginas web de algún grupo religioso. Típicos ataques son la destrucción de sistemas de prácticas o la modificación de páginas web de algún departamento o de ciertos profesores, generalmente por parte de alumnos descontentos.
- **Intrusos Remunerados.-** Este es el grupo de atacantes de un sistema más peligroso, aunque por fortuna el menos habitual en redes normales; suele afectar más a las grandes empresas o a organismos de defensa. Se trata de piratas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, que son pagados por una tercera parte[5] generalmente para robar secretos, el nuevo diseño de un procesador, una base de datos de clientes, información confidencial sobre las posiciones de satélites espía, etc., o simplemente para dañar la imagen de la entidad afectada. Esta tercera parte suele ser una empresa de la competencia o un organismo de inteligencia, es decir, una organización que puede permitirse un gran gasto en el ataque; de ahí su peligrosidad: se suele pagar bien a los mejores piratas, y por si esto fuera poco los atacantes van a tener todos los medios necesarios a su alcance. Aunque como hemos dicho los intrusos remunerados son los menos comunes en la mayoría de situaciones, en ciertas circunstancias pueden aprovechar nuestras redes como plataforma para atacar otros organismos.

1.3. TIPOS DE AMENAZAS LÓGICAS

Bajo la etiqueta de amenazas lógicas se encuentra todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (software malicioso o malware) o simplemente por error (bugs o agujeros). De aquí se clasifican las amenazas en:

- **Software incorrecto.-** Las amenazas más habituales a un sistema provienen de errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones. Una situación no contemplada a la hora de diseñar el sistema de red del kernel o un error accediendo a la memoria en un fichero setuidado pueden comprometer local o remotamente a cualquier sistema operativo. A estos errores de programación se les denomina bugs, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema, exploits. Como se ha dicho, representan la amenaza más común contra, ya que cualquiera puede conseguir un exploit y utilizarlo contra nuestra máquina sin ni siquiera saber cómo funciona y sin unos conocimientos mínimos de sistemas operaitvos; incluso hay exploits que dañan seriamente la integridad de un sistema (negaciones de servicio o incluso acceso root remoto) y están preparados para ser utilizados desde MS-DOS, con lo que cualquier pirata novato (comúnmente, se les denomina Script Kiddies) puede utilizarlos contra un servidor y conseguir un control total de una máquina de varios millones desde su PC sin saber nada del sistema atacado; incluso hay situaciones en las que se analizan los logs de estos ataques y se descubre que el pirata incluso intenta ejecutar órdenes de MS-DOS.
- **Herramientas de seguridad.-** Cualquier herramienta de seguridad representa un arma de doble filo. De la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos. La

conveniencia de diseñar y distribuir libremente herramientas que puedan facilitar un ataque es un tema controversial que incluso, expertos reconocidos como por ejemplo Alec Muffet (autor del adivinador de contraseñas **Crack**) han recibido enormes críticas por diseñar determinadas herramientas de seguridad para Unix. Tras numerosos debates sobre el tema, ha quedado bastante claro que no se puede basar la seguridad de un sistema en el supuesto desconocimiento de sus problemas por parte de los atacantes: esta política, denominada **Security through obscurity**, se ha mostrado inservible en múltiples ocasiones. Si los administradores no utilizan herramientas de seguridad que muestren las debilidades de los sistemas (para corregirlas), se tiene que estar seguro que un atacante no va a dudar en utilizar tales herramientas para explotar las debilidades encontradas; por tanto, se ha de agradecer a los diseñadores de tales programas el esfuerzo que han realizado en pro de sistemas más seguros.

- **Puertas traseras.-** Durante el desarrollo de aplicaciones grandes o de sistemas operativos, es habitual entre los programadores insertar *atajos* en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando. A estos atajos se les denomina puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos: por ejemplo, los diseñadores de un software de gestión de bases de datos en el que para acceder a una tabla se necesiten cuatro claves diferentes de diez caracteres cada una pueden insertar una rutina para conseguir ese acceso mediante una única clave, con el objetivo de perder menos tiempo al depurar el sistema. Algunos programadores pueden dejar estos atajos en las versiones definitivas de su software para facilitar un mantenimiento posterior, para garantizar su propio acceso, o simplemente por descuido; la cuestión es que si un atacante descubre una de estas puertas traseras (no importa el método que utilice para hacerlo) va a tener un acceso global a datos que no deberá poder leer, lo que obviamente supone un grave peligro para la integridad del sistema.
- **Bombas lógicas.-** Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de

una acción perjudicial. Los activadores más comunes de estas bombas lógicas pueden ser la ausencia o presencia de ciertos ficheros, la ejecución bajo un determinado UID (identificador único) o la llegada de una fecha concreta; cuando la bomba se activa va a poder realizar cualquier tarea que pueda realizar la persona que ejecuta el programa: si las activa el **root**, o el programa que contiene la bomba está **setuitado**[3] a su nombre, los efectos obviamente pueden ser fatales.

- **Canales cubiertos.-** Los canales cubiertos o canales ocultos, son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema; dicho de otra forma, un proceso transmite información a otros (locales o remotos) que no están autorizados a leer dicha información.
- **Virus.-** Un virus es una secuencia de código que se inserta en un fichero ejecutable denominado huésped, de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas. Todo el mundo conoce los efectos de los virus. Sin embargo, los virus existentes para entornos Unix, por ejemplo, son más una curiosidad que una amenaza real, en sistemas sobre plataformas IBM-PC o compatibles ciertos virus, especialmente los de **boot**, pueden tener efectos nocivos, como dañar el sector de arranque; aunque se trata de daños menores comparados con los efectos de otras amenazas, hay que tenerlos en cuenta.
- **Gusanos.-** Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando **bugs** de los sistemas a los que conecta para dañarlos. Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande: el mayor incidente de seguridad en Internet fue precisamente el **Internet Worm**, un gusano que en 1988 causó pérdidas millonarias al infectar y detener más de 6000 máquinas conectadas a la red. Se puede pensar que un gusano puede automatizar y ejecutar en unos segundos todos los pasos que seguiría un atacante humano para acceder a nuestro sistema, mientras que una

[3] SETUITAR, término usado en Linux, como abreviatura a SET USER ID o SET GROUP ID. También son permisos de acceso que pueden asignarse a archivos o directorios en un sistema operativo basado en UNIX.

persona, por muchos conocimientos y medios que posea, tardaría como mínimo horas en controlar una red completa (un tiempo más que razonable para detectarlo), un gusano puede hacer eso mismo en pocos minutos, de ahí su enorme peligro y sus devastadores efectos.

- **Caballos de Troya.-** Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario; como el Caballo de Troya de la mitología griega, al que deben su nombre, ocultan su función real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente. En la práctica, cuando un intruso consigue el privilegio necesario en el sistema, instala troyanos para ocultar su presencia o para asegurarse la entrada en caso de ser descubierto: por ejemplo, es típico utilizar lo que se denomina un **rootkit**, que no es más que un conjunto de versiones troyanas de ciertas utilidades para conseguir que cuando el administrador las ejecute no vea la información relativa al atacante, como sus procesos o su conexión al sistema; otro programa que se suele suplantar es login, por ejemplo, al recibir un cierto nombre de usuario y contraseña proporcionando acceso al sistema..
- **Programas conejo o bacterias.-** Bajo este nombre se conoce a los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco), produciendo una negación de servicio. Por sí mismos no hacen ningún daño, sino que lo que realmente perjudica es el gran número de copias suyas en el sistema, que en algunas situaciones pueden llegar a provocar la parada total de la máquina. Hay ciertos programas que pueden actuar como conejos sin proponérselo; ejemplos típicos se suelen encontrar en los sistemas Unix destinados a prácticas en las que se enseña a programar al alumnado: es muy común que un bucle que por error se convierte en infinito contenga entre sus instrucciones algunas de reserva de memoria, lo que implica que si el sistema no presenta una correcta política de cuotas para procesos de usuario

pueda venirse abajo o degradar enormemente sus prestaciones. El hecho de que el autor suela ser fácilmente localizable no debe ser ninguna excusa para descuidar esta política.

- **Técnicas salami.-** Por técnica salami se conoce al robo automatizado de pequeñas cantidades de bienes (generalmente dinero) de una gran cantidad origen. El hecho de que la cantidad inicial sea grande y la robada pequeña hace extremadamente difícil su detección. Si de una cuenta con varios millones se roban unos céntimos, nadie va a darse cuenta de ello; si esto se automatiza para, por ejemplo, descontar un centavo de cada nómina pagada en la universidad o de cada beca concedida, tras un mes de actividad, seguramente se habría robado una enorme cantidad de dinero sin que nadie se haya percatado de este hecho, ya que de cada origen se ha tomado una cantidad ínfima. Las técnicas salami no se suelen utilizar para atacar sistemas normales, sino que su uso más habitual es en sistemas bancarios; sin embargo, como en una red con requerimientos de seguridad medios es posible que haya ordenadores dedicados a contabilidad, facturación de un departamento o gestión de nóminas del personal, su finalidad no sería nada difícil.

1.4. TIPOS DE PROTECCIONES EN UNA RED

En el diseño de una red, es esencial que se haga un análisis del tráfico que van a soportar cada uno de los elementos de la misma, para que luego con esos resultados establecer las políticas de seguridad en función de las potenciales amenazas a las que la red podría estar expuesta. Estas amenazas van en función de los servicios que se presten en la red o del tipo de información que se procese en la misma. Si eventualmente las protecciones implementadas en la red no fueron lo suficientemente robustas ante un ataque cualquiera, se deberá tener planificado un plan de contingencia, en el que exista un back up

de la red, tanto de energía como de datos (respaldo de la información). Este tipo de acciones previas a un ataque (llamados **mecanismos de seguridad**) son las que minimizan los efectos del mismo; es decir, hacen que la red no quede totalmente inoperable o que los datos se pierdan o sean dañados; además de que el restablecimiento de la misma no sería muy complicado ni tampoco tomaría mucho tiempo.

En función de lo ya expuesto, se determinan tres tipos de protecciones: de prevención, detección y recuperación. El primer tipo de protección es el de **prevención** ya que es el que aumenta el nivel de seguridad de la red durante su normal funcionamiento. Un ejemplo de esto es cuando los datos transmitidos son cifrados, previniendo así que éstos sean interceptados. Los de **detección** son aquellos que detectan violaciones o intentos de violaciones a la red. Finalmente, los de **recuperación** son los que, una vez que la red fue vulnerada, establecen las medidas de recuperación del sistema para volverle a este a su funcionamiento correcto. En sí, el proceso completo de esta protección es además de identificar la violación ocurrida, identificar el alcance que tuvo la misma en la red, las actividades que realizó y la puerta utilizada para entrar. Un ejemplo de esto es cuando se realizan copias de seguridad o redundancia. En la ***figura 1.2*** se muestra los procesos de protección y amenazas.

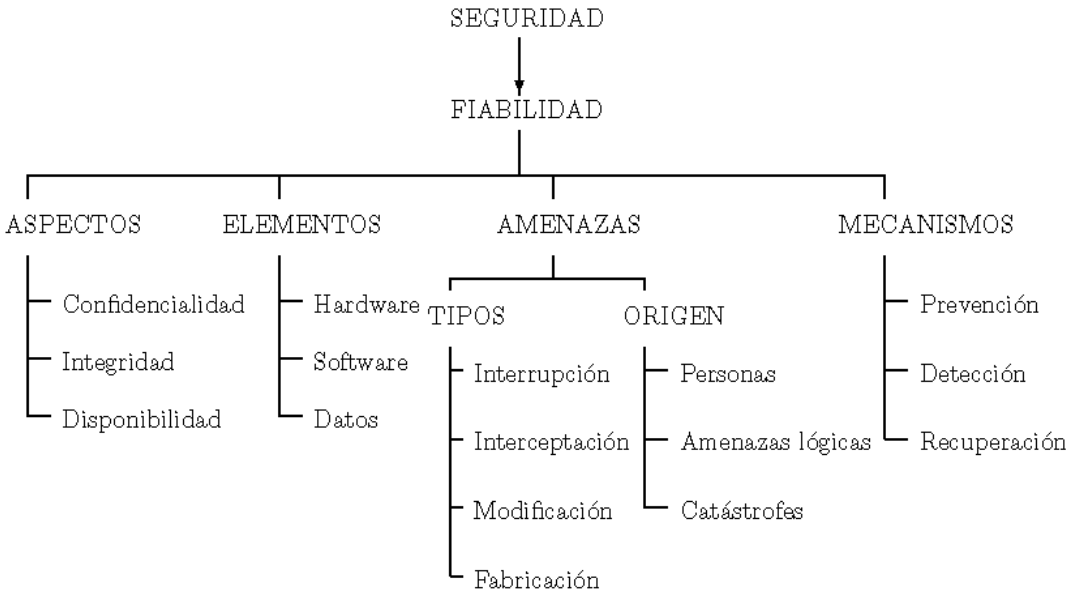

Figura1.2 Visión global de la seguridad informática

Los mecanismos de prevención más habituales en redes son:

- **Mecanismos de autenticación e identificación.-** Estos mecanismos hacen posible identificar entidades del sistema de una forma única para posteriormente autenticarlas. Son los mecanismos más importantes en cualquier sistema ya que forman la base de otros mecanismos. Un grupo especialmente importante de estos mecanismos son los denominados Sistemas de Autenticación de Usuarios.
- **Mecanismos de control de acceso.-** Cualquier objeto del sistema ha de estar protegido mediante mecanismos de control de acceso, que controlan todos los tipos de acceso sobre el objeto por parte de cualquier entidad del sistema.
- **Mecanismos de separación.-** Cualquier sistema con diferentes niveles de seguridad ha de implementar mecanismos que permitan separar los objetos dentro de cada nivel, evitando el flujo de información entre objetos y entidades de diferentes niveles, siempre

que no exista una autorización expresa del mecanismo de control de acceso. Los mecanismos de separación se dividen en cinco grandes grupos, en función de cómo separan a los objetos: separación física, temporal, lógica, criptográfica y fragmentación.

- **Mecanismos de seguridad en las comunicaciones.-** Es especialmente importante para la seguridad de nuestro sistema el proteger la integridad y la privacidad de los datos cuando se transmiten a través de la red. En las comunicaciones la mayoría se basan en la Criptografía (cifrado de clave pública, privada, firmas digitales). Aunque cada vez se utilizan más los protocolos seguros como SSH, aún es frecuente encontrar conexiones en texto no sólo entre máquinas de una misma subred, sino entre redes diferentes. Una de las mayores amenazas a la integridad de las redes es este tráfico sin cifrar, que hace extremadamente fáciles los ataques encaminados a robar contraseñas o suplantar la identidad de máquinas de la red.

1.5. DISPOSITIVOS UTM

1.5.1. Concepto y Generalidades

Un UTM (Unified Thread Management) es un dispositivo de red que presta servicios convencionales de un firewall convencional, también integra otras funciones tales como anti-spam, antivirus, detección de intrusos (IDS/IPS), malware y gestión de tráfico, todo eso a nivel de capa de aplicación. Este administrador de tráfico realiza los procesos a modo de proxy, analizando y permitiendo tráfico en función de las instrucciones implementadas en el dispositivo.

La finalidad de los equipos UTM es el de cada vez ir incrementando mas las capacidades de protección para una red en un solo equipo, sea esta el de una gran empresa o una red local pequeña. Sin embargo, este servicio puede ser de gran utilidad u obsoleto dependiendo de si hubo un estudio de planificación para el correcto uso del mismo.

Una de las últimas tendencias que van ganando campo entre los expertos informáticos es la protección en capas de una red, por lo que la utilización de UTMs es la manera más eficaz de hacerlo. Hay que tomar en cuenta que existen en el mercado muchas marcas que ofrecen al usuario diversas funciones que integran servicios según

las necesidades de cada organización, por lo que solo mediante una gestión de planificación, se podría dotar a la red de una excelente protección.

En la actualidad, el mercado UTM se encuentra en gran apogeo, y según datos publicados hace poco más de un año, éste copará más del 33,6% del negocio de seguridad de redes hasta antes del 2012. Según datos de Europa, solo durante el segundo trimestre del 2009, el mercado de dispositivos de seguridad cayeron aproximadamente un 9,6%, mientras que los dispositivos UTM cayeron hasta el segundo trimestre del año anterior tan sólo un 0,6%, dejando ganancias por sobre los 113 millones de euros.[4]

Tan buenas son las cifras estadísticas, que la mayoría de las empresas están cada vez más interesadas en la integración de cada vez más servicios en un solo dispositivo. Empresas como: Juniper, Check Point, Watchguard, Netgear, Stonesoft, Crossbeam Systems y Astaro, Fortinet, Trend Micro, Secure Computing, Cisco, SonicWall, lideran el mercado y compiten para ofrecer mejores servicios.

En el insaciable deseo de conseguir cada vez un mayor conjunto de prestaciones y cubrir con las necesidades de seguridad de las empresas en cuanto a capacidad de red, movilidad, tráfico y acceso remoto, se plantea alcanzar un XTM (eXtensive Thread Management), que como su nombre lo indica, es un UTM potenciado a dar muchos más servicios, como una gestión centralizada mediante interfaces gráficas para actualizaciones y licencias, monitorización y correlación de eventos. Fortinet, una

[4] "**El mercado de appliances de seguridad volverá a crecer con fuerza en 2010" asegura IDC, AZLANEWS**, edición N10, Febrero/Abril 2010.

de las empresas líderes en este mercado, en Noviembre del 2008 introdujo en el mercado un equipo capaz de segmentar sus redes para una mayor granularidad de la política y aislamiento de eventos. Según el administrador de productos de XTM de la empresa WatchGuard, "los accesorios XTM del futuro estarán capacitados para operar procesos automáticamente como control de acceso, protección basada en un historial, correlación de eventos, gestión de vulnerabilidades y control de acceso a la red".

En general, a un UTM, además de lo ya expuesto, también se le suman protecciones como: control de tráfico, rendimiento y latencia y gestión del ancho de banda; y funcionalidades como protección robusta, capacidad de conectividad mejorada y mayor flexibilidad en la administración. Adicionalmente, si integran más capacidades de gestión de red, incluyendo integración de tecnologías de redes, optimización de las redes WAN, alta disponibilidad que suministre redundancia y software de gestión que permita control one-touch.

Una tendencia adicional del mercado UTM es la reciente adquisición de Woven Systems para utilizar su conmutación de alta velocidad y desarrollada tecnología en la gestión de tráfico para mejorar el rendimiento de la seguridad. Un ejemplo de esta adquisición es la que hizo últimamente la empresa Fortinet, con el objetivo de obtener una mayor potencia de conmutación en lo productos basados en chasis, aumentando la velocidad de las comunicaciones dentro y entre las hojas de seguridad, una opción que ofrece a sus clientes una mayor escalabilidad y el rendimiento en general.

1.5.2. Características

Un UTM debe incluir:

- ✓ Firewall/VPN y filtrado antivirus
- ✓ Antispam
- ✓ Filtrado de URL
- ✓ Detección de intrusiones
- ✓ Prevención de intrusiones
- ✓ Bloqueo de spyware
- ✓ Protección de VoIP

Cómo funciona:

- ✓ El tráfico entrante se desencripta, si es necesario, en el módulo correspondiente antes de que se inicie la inspección en el módulo de cortafuegos.
- ✓ El dispositivo de análisis de datos relaciona las inspecciones realizadas por los distintos módulos y dispositivos UTM, descartando cualquier tráfico que suponga una amenaza.
- ✓ El dispositivo de análisis vuelve a unir las cargas útiles de los paquetes para que el dispositivo antivirus y los módulos de filtrado y Antispam analicen el contenido.
- ✓ Cualquier tráfico sospechoso se descarta.
- ✓ El módulo de encriptación reencripta el tráfico VPN y otros del mismo tipo que vayan cifrados.

- ✓ Todos los retos se reportan al módulo de logging e informes, dedicados a activar alertas en condiciones determinadas y para realizar un análisis forense.

Un dispositivo UTM presta muchas ventajas en una red, no solo con el ahorro de espacio físico y lógico en la misma, sino también porque en un solo dispositivo o software se da una protección global a gran escala; es decir, a nivel de servidores. Adicionalmente se tiene una instalación simplificada y recurrentemente se pueden mantener actualizados todos los servicios que integra un UTM.

Cuando se evalúa el desempeño, la mayoría de los ejecutivos de las empresas tienen una complicación común al no acordar en una metodología para probar o describir un dispositivo UTM. Las tradicionales formas de gestionar estas mediciones son basadas en tasa de conexión, throughput, latencia y límites de conexión; sin embargo los vendedores tienden a jugar con sus cifras más atractivas, sin proveer suficientes detalles y así comparar características similares entre marcas, ni tampoco ofreciendo suficientes escenarios para comprobar la robustez del manejo de seguridad en sus equipos. Un verdadero test UTM sería el de aplicar el equipo en una red real que corra con un procesamiento real de datos a lo largo de la misma. Cuando un equipo UTM es correctamente diseñado, llega a ser igualmente útil sin importar donde es ubicado, por ejemplo, mientras un dispositivo de borde sólo necesitaría dos o tres interfaces para la red interna y externa, un Firewall interno necesitará muchas más interfaces, una por cada grupo de servidores (tantos como VLANs se tengan) para soportar tantas zonas de seguridad como sean necesarias.

Los administradores de red usan protocolos de enrutamiento dinámico para simplificar las configuraciones y proveer servicios más robustos frente a los cambios que existen en las topologías y cortes de servicio. Los dispositivos UTM de clase empresarial deben integrar en sí compatibilidad con los actuales protocolos y servicios de enrutamiento que grandes compañías tienen corriendo en sus redes privadas (por ejemplo OSPF). Cuando se le considera a un dispositivo UTM para ser utilizado en una red de una compañía, es crítico y de gran importancia el dar soporte a los protocolos de enrutamiento de la red, a los tipos de interfaz como la fibra óptica o cobre de gigabit con capacidades de VLAN, y a los requisitos de escalabilidad (tal como un balanceo de carga).

Adicionalmente, para obtener flexibilidad en el enrutamiento y con las interfaces, cualquier recurso de red crítico, tal como un Firewall actúa como un cuello de botella entre las diferentes zonas de una red, un punto de despliegue de un dispositivo UTM debe ser diseñado tanto para afrontar la disponibilidad de componentes defectuosos como para el inevitable incremento o actualización de cargas en la red.

Alta disponibilidad puede significar muchas cosas, pero la manera más simple de definirla y en función de una red segura, significa que el fallo de una parte de un dispositivo UTM, ya sea hardware o software, no debe interrumpir el flujo de tráfico a través de de la red. Así mismo, la disponibilidad trae consigo mismo otro punto de vista, la posibilidad de escalabilidad de un dispositivo UTM. Así como una gran red de producción crece día a día, los dispositivos UTM deben tener la habilidad de escalar en rendimiento sin interrumpir el servicio. Esto lleva a pensar que estos dispositivos deben poderse maniobrar en caliente (hot swap) o tener redundancia. En

sí, lo que caracteriza a un dispositivo UTM es la "Integración" de servicios, tales como los actuales sistemas de administración de escritorio, anti-virus de más alta eficacia, sistemas de prevención de intrusos y los sistemas de detección de intrusos. En otras palabras, un dispositivo UTM está diseñado específicamente para integrar una red adecuadamente en cualquier parte de ella; o sea, es un dispositivo de red y un dispositivo de seguridad al mismo tiempo (***Figura 1.3***).

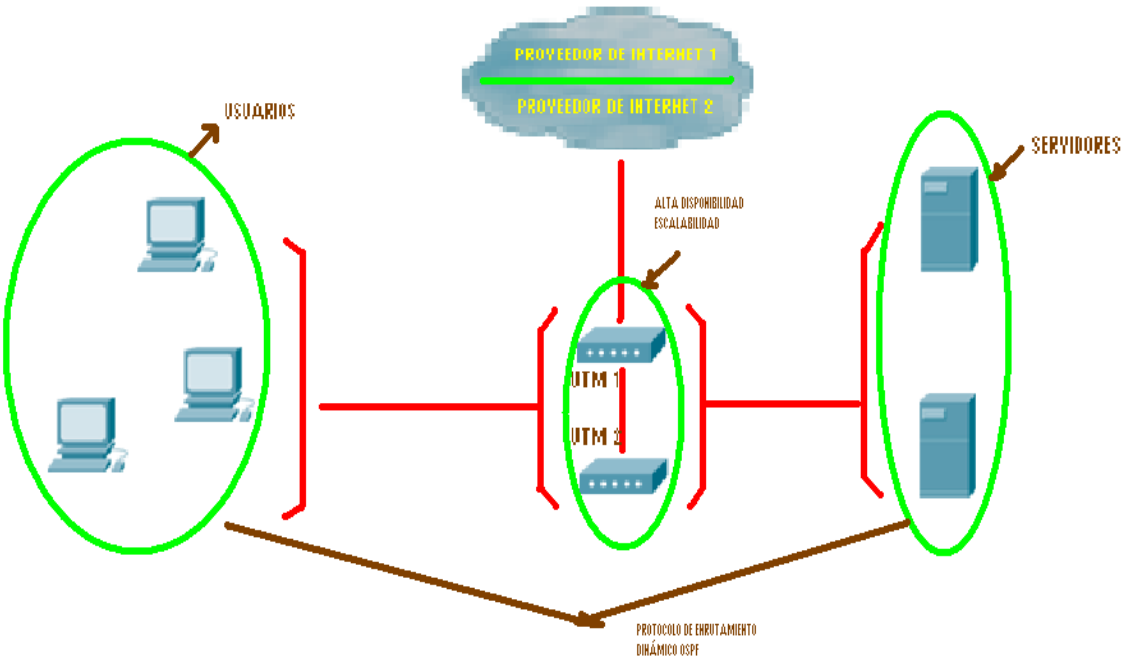

Figura1.3 Dispositivo UTM en la red

1.5.3. Prestaciones

Firewall.- Un firewall es un parte de un sistema de red que bloquea el ingreso de elementos no autorizados a la misma o que en su caso permite el ingreso o el establecimiento de comunicaciones autorizadas. El criterio que se maneja es que en base a lineamientos establecidos por el administrador de la red, un firewall es capaz de permitir, bloquear, descifrar o limitar el tráfico tanto de elementos externos a la red como de internos, cuando se tiene el caso de que ciertos grupos de personas tienen el acceso restringido a ciertas partes en la red.

Estos dispositivos pueden ser implementados tanto en hardware como en software y el uso más usual que se les da es para gestionar el ingreso o no de usuarios del internet a una red local o privada cualquiera. Todo mensaje que provenga del internet, será analizado y dependiendo de que cumpla o no con los criterios de seguridad establecidos en la administración de la red, este tráfico o usuario será permitido o negado. En la ***figura 1.4*** se muestra de forma grafica como se integra este servicio a una red.

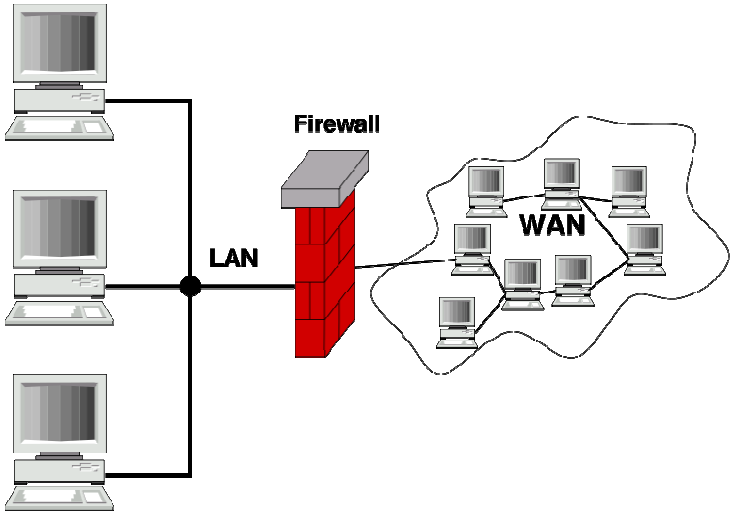

Figura1.4 Firewall en una red

Tipos de Firewall

- **Nivel de aplicación de pasarela**

  Este mecanismo de seguridad se aplica a servidores FTP y TELNET.

- **Circuito a nivel de pasarela**

  Este se aplica a conexiones establecidas de TCP o UDP. Permite que una sesión se establezca, aun si esta fue hecha desde una zona de mayor seguridad hacia una de menor seguridad.

- **Cortafuegos de capa de red o de filtrado de paquetes**

  Opera a nivel de la capa de red (tomados del modelo TCP/IP) como filtro de paquetes IP. Se realizan los filtros en función de los campos de los paquetes IP, como son dirección IP origen, dirección IP destino, tipos de datos transmitiéndose. En algunos dispositivos firewall también se realizan filtrados según los campos de

nivel de la capa de transporte o a nivel de la capa de enlace de datos (dirección MAC). A éste cortafuegos se le considera uno de los más eficaces para la protección de una red contra intrusos.

- **Cortafuegos de capa de aplicación**

  Como su nombre mismo lo dice, este tipo de firewall trabaja en la capa 7 de aplicación del modelo OSI, como por ejemplo trafico HTTP realizando filtrado según la URL a la que se intenta acceder. A este tipo se le denomina PROXY y oculta las direcciones de red para gestionar los accesos en una organización al internet o desde el internet.

- **Cortafuego personal**

  Este es el más común de los firewall. Es el que se instala en un computador individual cualquiera y cumple la función principal, filtrar el acceso de elementos no autorizados a una red.

SPAM.- O también llamado correo basura, se le denomina a todo tipo de mensajes de correo electrónico que no es solicitado o deseado. El propósito de este tipo de correo es el de enviar masivamente publicidad a un sinnúmero de direcciones y que en la mayoría de los casos puede perjudicar de alguna manera al receptor o a los receptores. Sin embargo este tipo de correo, hoy en día ya no está afectando solamente a los correos electrónicos vía internet, sino que también ya se está distribuyendo vía sms y sistemas de mensajería instantánea.

Antivirus.- Los antivirus nacieron como una herramienta simple cuyo objetivo era detectar y eliminar virus informáticos. Su comportamiento normal se basa en contar con una lista de virus conocidos y sus formas de reconocerlos. Sin embargo actualmente se cuenta con un proceso de detección de virus heurístico, que es una

técnica para reconocer virus o código malicioso que no se encuentren dentro de la base de datos que ya se incluye en un antivirus.

Con el transcurso del tiempo, con la aparición de sistemas operativos más avanzados y el Internet, los antivirus evolucionaron hacia programas más avanzados que no sólo detectan virus informáticos, sino que también los bloquean, desinfectan y previenen una posible infección.

El principal objetivo de un antivirus es el de detectar la mayor cantidad de amenazas que puedan dañar o afectar a un ordenador y bloquearlas antes de que pueda cumplir con su objetivo, o a su vez eliminarlo tras la infección. Los métodos de contagio son más que conocidos por la colectividad, usualmente son adquiridos al bajarse un programa del internet de una dirección o servidor no seguro o cuando por ejemplo, por medio de publicidad y atrayendo a la gente por lo que se dice en la misma, se ven incentivados a seguir las instrucciones que se le recomienda, con el fin de ganar un premio o beneficiarse de alguna manera.

Malware.- Un malware es todo software que tiene como finalidad dañar cualquier sistema operativo, es por eso que a estos programas se los identifica como hostiles, intrusivos o molestos. Un malware incluye a todos los tipos de programas peligrosos antes descritos.

Tipos de Malware

- **Spyware.-** Estos programas son los que se instalan de forma paralela a programas deseados por el usuario, sin que éste se dé cuenta, con el fin de recopilar información y transmitirla a centros publicitarios o empresas específicas que utilizan lo recopilado para diferentes propósitos. Una manera legal en la que estas

empresas utilizan dicho propósito es cuando el usuario instala un programa gratis, y en los términos de contrato o licencia se establece de forma confusa y oculta la forma en que el spyware actuara en la computadora. El usuario confundido o sin si quiera leer lo que dice dicho contrato acepta las condiciones del mismo, dejando libre el paso.

- **Adware**.- Éstas son las famosas ventanas emergentes o pop-up que se muestran de forma intrusiva y molestosa al usuario, es decir, aparecen sin ser requeridos A pesar de las acciones ya descritas, por muchas personas se dice que los Adware no deberían ser considerados como un tipo de malware, pero por otras, se establece más bien que por lo que los programas que se instalan no establecen de forma clara y precisa lo que en si llevan y adicionalmente se instalara en el ordenador, si deberían ser considerados como tales.

- **Hijackers.-** Estos son programas que reconfiguran el navegador web, haciendo que la página de inicio del mismo, por ejemplo, se cambie a una de interés específico o en el peor de los casos, estos cambian los resultados de búsqueda, direccionándolos a paginas donde se puede realizar phishing bancario[5].

- **Diales.-** Estos programas son los que mediante el tono de llamado, introducen un número para conectarse telefónicamente hacia un lugar específico, dejando la llamada abierta constantemente y consecuentemente la cuenta de teléfono incrementándose exponencialmente.

- **Botnets.-** Son todas las computadoras infectadas que son utilizadas para diferentes objetivos. Por ejemplo, pueden ser usadas por personas que hacen ataques a

[5] **Phishing.-** Término informático que denomina un tipo de delito que se comete por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria. El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso con llamadas telefónicas.

diferentes organizaciones y que porque utilizan a estas computadoras como medio para sus propósitos, no pueden ser rastreados ni sometidos a persecución policial.

1.6. Consideraciones a tomarse en cuenta para instalar un UTM

1.6.1. Planificación y Despliegue

Para pymes u organizaciones de mayor tamaño, para un UTM o XTM, cuando la opción de seguridad a desplegarse es un enfoque unificado, se deben tener muchos factores en cuenta antes de decidirse por un producto y configuración concretos. Las cuestiones más importantes a considerarse son: la manera en la que se integra la seguridad en la arquitectura general de la empresa, identificar las fronteras de la red, el personal y cuántos darán soporte al despliegue, el personal interno, y si es que se puede confiar en el soporte del suministrador y en sí todas las cuestiones comunes a cualquier solución de seguridad. Cuando se elige un enfoque UTM se ha de tener en cuenta también cuestiones como el nivel de integración y fiabilidad de las distintas funciones, y cómo éstas impactarán en el rendimiento de la red. Las funciones de firewall, VPN y detección de intrusiones no son particularmente intensivas en computación, pero son sensibles a la latencia. Por el contrario, las funciones de antivirus, filtrado de URL y otras similares, sí son intensivas en computación aunque mucho más tolerantes a la latencia. Mezclando las dos clases de servicios en la red puede tener como efecto la ralentización de las aplicaciones más sensibles a los retardos.

Antes de buscar productos en el mercado, se debe determinar las necesidades de seguridad específicas de la empresa, pues los dispositivos UTM combinan varias funciones en un único sistema, y no todos de la misma manera. Los múltiples productos UTM en el mercado varían ampliamente en cuanto a características, capacidad y precio, y no todas las organizaciones requerirán determinadas prestaciones y capacidades, mismas que podrían encarecer innecesariamente el coste total de la tecnología, además de incrementar la complejidad de la solución.

Como recomienda IDC, cuando se va a evaluar una caja UTM, hay que comenzar por lo básico: necesidades, tamaño exacto de la compañía, si es que la empresa crece o no, etc., lo que hace posible que la lista de productos potenciales se recorte en dos tercios.

1.6.2. Investigar y Probar

Muchas empresas, usualmente las más pequeñas, no tienen ni tiempo ni recursos para probar productos internamente, aprovechan los test publicados por los medios especializados y usan los servicios de prueba de organizaciones como ICSA Labs (International Computer Security Association). Las empresas más grandes, muy por el contrario realizan sus propios test, seleccionan tres o cuatro suministradores y prueban sus soluciones en un laboratorio. IDC sugiere realizar dos tipos de test. El que consiste

en someter a prueba el rendimiento de los productos contra la configuración que la empresa plantea usar y aquellas funciones específicas que utilizará. Y el que se trata de probar los productos con todas las características que ofrece un UTM, lo que dará una idea del rendimiento necesario cuando se capaciten más aplicaciones de las elegidas en un primer momento. Otras cuestiones a considerar es la comprobación de que los dispositivos UTM evaluados trabajan sin problemas con el múltiple hardware instalado en la empresa. Asimismo, también los test se deberían aplicar a las actualizaciones, pues si bien no deberían implicar cambios sustanciales, en los productos UTM se puede tratar de cambios de tipos de patrones de tráfico o de filtrado, lo que puede afectar al tráfico legítimo. Los expertos aconsejan al respecto probar previamente las actualizaciones, porque, de lo contrario y al menos potencialmente, podrían provocar la desactivación de uno o varios segmentos de la red".

1.6.3. Coste vs. Escalabilidad.

Cuando se selecciona un producto, hay que tomar en consideración distintos factores: coste, escalabilidad, gestión centralizada y soporte del suministrador. Por otra parte, la interfaz de gestión debería ser tan unificada como el dispositivo en sí. La escalabilidad y distribución son otras consideraciones clave, puesto que las empresas con muchas sucursales necesitan asegurarse de que un dispositivo UTM es capaz de soportar usuarios remotos y lo más importante, cuántos remotos es capaz de brindar el servicio eficientemente, por lo que aquí es donde entra en juego la escalabilidad y el rendimiento con cientos o miles de usuarios. Es también crítico e importante el evaluar la consola de gestión o interfaz de usuario para comprobar si se dispone de SIEM (Security Information Event Management), si permite habilitar fácilmente aplicaciones

y cuáles son las que permite o hacer cambios y configuraciones de política universales. Con un UTM, estos factores son tan importantes como las propias prestaciones de la caja, sobre todo cuando se ha de dar servicio a un gran número de usuarios. Los sistemas UTM no deberían tener consolas separadas para cada función, más bien, los perfiles de protección que definen URL, IPS y firmas de antivirus para aplicar en función de un grupo específico de usuarios, deberían estar integrados con un gestor de reglas de cortafuegos. Las actualizaciones deberían además ser fáciles de llevarse desde una consola de gestión centralizada a múltiples dispositivos. También hay que considerar el alcance y cómo va a llegar el soporte y mantenimiento al sistema UTM, un factor que puede cambiar la decisión del cliente, muy especialmente cuando se cuenta con presencia internacional. En estos casos, y si es que la empresa que vende el producto está localizado en un país extranjero, hay que garantizar que éste disponga de canales de distribución en el o los países donde la empresa está presente. Así, se garantiza la disponibilidad de una plataforma integrada capaz de proporcionar los mismos servicios de seguridad en todas las filiales, sucursales y delegaciones de la corporación repartidas por todo el mundo.

1.6.4. Grandes redes

Si en las pymes, el despliegue de soluciones UTM puede estar más que justificado desde un primer momento, por cuestiones de rentabilidad, algunas personas responsables del manejo de la red de grandes empresas, con redes de múltiples ubicaciones, son reacios al confiar todas sus herramientas de seguridad a un único proveedor. No obstante, se puede soslayar este inconveniente instalando un UTM en forma redundante con propósitos de failover, lo que ofrece mayores niveles de disponibilidad para la red.

Además, como en las redes de gran tamaño, la capacidad de proceso real es una cuestión crítica, a menudo se prefiere distribuir la protección contra retos en vez de centralizarla, simplemente para reducir la probabilidad de que se produzca un cuello de botella en el rendimiento de la red. El estilo y calidad de las características de mitigación de vulnerabilidades que proporcionan los dispositivos UTM no siempre cubren las necesidades de las grandes empresas, especialmente en lo que se refiere a las funciones Antispam y antivirus, cuando no fueron diseñadas para ser adaptadas desde un inicio al software y hardware de la empresa. En cualquier caso, son muchos hoy los expertos que defienden las ventajas de un UTM sobre todo por cuanto aportan a una menor complejidad, una gestión más sencilla y una mayor flexibilidad.

Los administradores de grandes redes incluyen en la planificación de la seguridad, soluciones de protección contra vulnerabilidades, especialmente en cuanto

a IDS/IPS, tanto en el núcleo como en la frontera de la red. Sin embargo, la complejidad de instalar cajas IDS/IPS hace desistir a muchos de ellos. Construir un "firewall sándwich," con balanceadores de cargas rodeando un núcleo de cortafuegos en cluster, es una solución común y bien conocida, pero intentar escalar ese sándwich con otra capa de protección incrementa enormemente la complejidad de la red y añade inestabilidad al abrir la puerta a fallos y problemas. Por el contrario, las soluciones UTM para grandes empresas con funciones IDS/IPS integradas aportan una seguridad adicional en la red sin la complejidad añadida que implica instalar dispositivos IPS/IDS.

1.6.5. Gestión Simplificada

Por otra parte, aunque los equipos de seguridad de las empresas suelen ser sistemas de gestión diferentes a la plataforma común del resto de recursos de la empresa, disponer de un cierto nivel de integración de gestión en la seguridad ayuda a simplificar el tratamiento de todas estas diferentes funciones, minimizando errores humanos y los que surgen por concepto de la comunicación entre ellos. Este enfoque de gestión integrada es especialmente valiosa cuando los cortafuegos, redes privadas virtuales e IDS/IPS son considerados conjuntamente, puesto que las tres funciones intervienen en una misma política. Cada una de ellas cumple con una cierta función en la topología de la red, además de determinar que grupos de aplicaciones están corriendo en cada servidor y qué puede hacer cada grupo de usuarios. Una gestión completamente separada de estas tres funciones dificulta la coordinación de las políticas. Por el contrario, trabajar con una única consola de gestión preparada para soportar un UTM, permite optimizar las políticas a través de las tres funciones,

incrementando la seguridad global. Finalmente, si bien los que están al frente de la seguridad de las grandes empresas acostumbran a elegir lo mejor del mercado en cada área a proteger, en vez de confiar en un UTM, habría situaciones concretas en que hacerlo puede aportar un enorme beneficio. Disponer de características de seguridad adicionales constantes en los firewalls, da al administrador de la red mayores niveles de flexibilidad. Si, por ejemplo, el dispositivo de antivirus deja de funcionar, el Firewall podrá asumir esa función. Aunque esas características del Firewall son usadas raramente, lo cierto es que brindan un refuerzo de seguridad que incrementa la flexibilidad de todo el sistema.

CAPÍTULO II

ANÁLISIS DE LA RED DEL DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA (DEEE)

1.1. DESCRIPCIÓN GENERAL

El departamento de Eléctrica y Electrónica de la Escuela Politécnica del Ejército cuenta con una red grande que comprende entre otras cosas con servidores de FIREWALL y correo, tanto para profesores como para estudiantes, y un servidor DNS que está en la frontera de la red.

1.2. ANÁLISIS DE LA RED LAN

La manera en que los diferentes equipos se comunican dentro de la red es mediante VLANS. La configuración de VLANS está dada de la siguiente manera.

Tabla2.1 **Información VLANs por cada Switch**

VLAN ID	NAME	IP ADDRESS
1	**adminEspe**	
2	**Masters**	**10.1.30.0/24**
3	**Pupils**	**10.1.29.0/24**
4	**Redes**	
10	**Intranet**	**10.10.0.0/24**
11	**Antigua**	
50	**NBX**	
100	**OUTNET**	

El DEEE está compuesto en la frontera con la parte WAN por un servidor FIREWALL, mismo que tiene los servicios en la parte LAN activos:

- IPTABLES.- tiene registro de VLANS, ROUTES, NAT y FORDWARDING
- DNS.- Domain Name System, configurado con el dominio deee.espe.edu.ec.
- NTOP.- Network TOP, que es la utilidad de la red que permite monitorear en tiempo real los usuarios y aplicaciones que consumen en tiempo real en un instante específico.
- DHCP, Dynamic Host Configuration Protocol, mismo que se encuentra configurado:

a) Red de profesores: 10.1.30.0/24
b) Red alumnos: 10.1.29.0/24

En el servidor FIREWALL, se encuentra instalado el sistema operativo Linux Centos versión 5.4, kernel 2.6.18-164.e15, con una memoria de 515740 Bytes, estando ocupado 181956 bytes y un espacio libre de 333784 bytes. Tiene 3 tarjetas de red:

- Eth0: IP: 10.1.28.2
  Máscara: 255.255.252.0
  Mac: 00:0C:76:5C:61:43

Ésta interfaz, a la vez tiene 4 sub-interfaces:

Tabla2.2 **Sub-interfaces de la tarjeta eth0**

eth0:1	**10.1.28.3/22**
eth0:2	10.1.28.4/22
eth0:3	10.1.28.5/22
eth0:4	10.1.28.6/22

- Eth1: MAC: 00:13:F7:48:60:6F

Posee cuatro sub-interfaces:

Tabla2.3 **Sub-interfaces, interfaz eth1**

Eth1:2	**10.1.30.1/24**	**Red de Profesores**
Eth1:3	10.1.29.1/24	Red de Alumnos
eth0:3	10.10.0.1/24	Red de Servidores
eth0:4	192.168.1.1/24	Pruebas de Red

- Eth2: IP: 201.234.84.173
  Máscara: 255.255.255.252
  Mac: 00:13:F7:48:6C:47 (GIGABIT ETHERNET)

Otro de los servicios con los que cuenta el DEEE (kyo.deee.espe.edu.ec), es el servidor WEB, con un sistema operativo Linux Centos versión 5.4, kernel 2.6.18-164.e15, una memoria total de 12297884 bytes, misma que tiene ocupada una capacidad de 4964224 bytes y libre 7338660. Éste servidor tiene instalado una tarjeta de red que tiene las siguientes características:

- Eth2: IP: 10.10.0.2
  Máscara: 255.255.255.0
  Mac: 00:25:B3:AD:75:BE
  Sub-interfaz: 192.168.58.54/24

2.3. ANÁLISIS DE LA TOPOLOGÍA FÍSICA DE LA RED

La Topología Física de la red LAN en el departamento de Eléctrica y electrónica, consta de un servidor conectado en estrella a los diferentes terminales. En la figura 2.1 se indica la distribución de los equipos conectados.

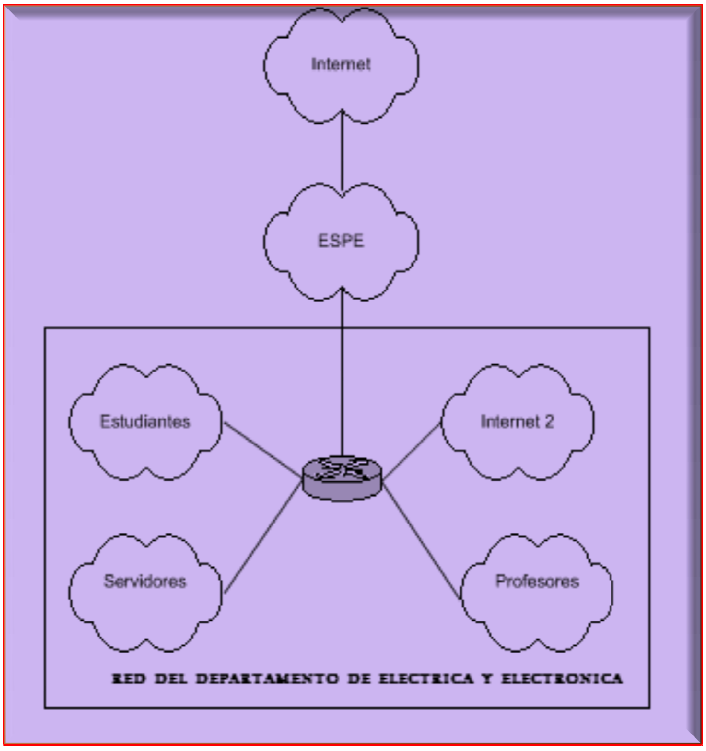

Figura2.1 **Topología Física del DEEE**

La red física del Departamento de Eléctrica y Electrónica está divida en diferentes bloques. Los laboratorios de Electrónica contarán con cinco bastidores, uno por cada planta, cuyas identificaciones son A1, B1, B2, C1 y C2 respectivamente. La identificación de bastidores se muestra en la figura:

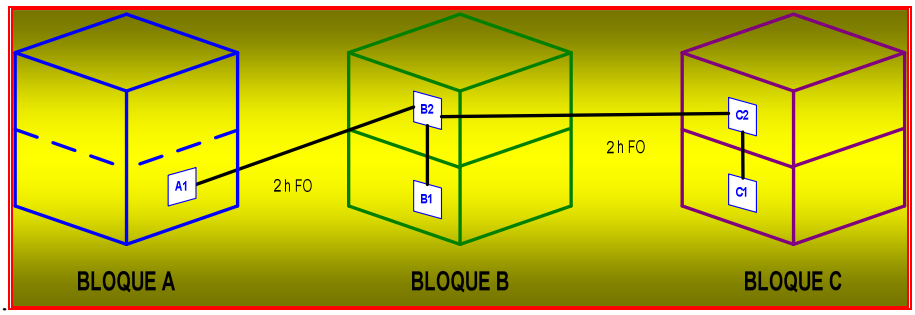

Figura2.2 **Identificación de Bastidores**

A continuación de detalla la distribución de cada rack que componen la red del DEEE, se muestra un esquema con todos los elementos que pertenecen a los rack, además se detalla cómo se encuentran interconectados cada uno de sus elementos.

- **Bloque A:**

  La conexión entre los elementos está dispuesta de la siguiente manera:

Tabla2.4 **Interconexion de Equipos del Rack A1 (Id: 2201-2224)**

Patch Panel	Id de Canal	Swicth HP2524	Hub 3Com
1	2201	13	
2	2202	14	
3	2203	15	
4	2204	17	
5	2205	16	
6	2206	18	
7	2207	19	
8	2208	20	
9	2209	21	
10	2210	22	
11	2211	23	
12	2212	Libre	
13	2213		6
14	2214		5
15	2215		13
16	2216	Libre	
17	2217		10
18	2218		7
19	2219		14
20	2220		9
21	2221		8
22	2222	Libre	
23	2223	Libre	
24	2224	Libre	

Tabla2.5 **Interconexión de Equipos del Rack A1 (Id: 2301-2324)**

Patch Panel	Id de Canal	Swicth HP2524	Hub 3Com
1	2301		
2	2302		
3	2303		
4	2304		
5	2305		
6	2306		
7	2307		
8	2308		
9	2309	12	
10	2310		12
11	2311		11
12	2312		
13	2313	2	
14	2314	3	
15	2315	4	
16	2316	5	
17	2317	6	
18	2318	7	
19	2319	8	
20	2320	9	
21	2321		
22	2322		
23	2323		
24	2324	10	

Tabla2.6 **Interconexión de Equipos Rack A1**

Swicth HP2524	Hub 3Com
11	1

- **Bloque B1**

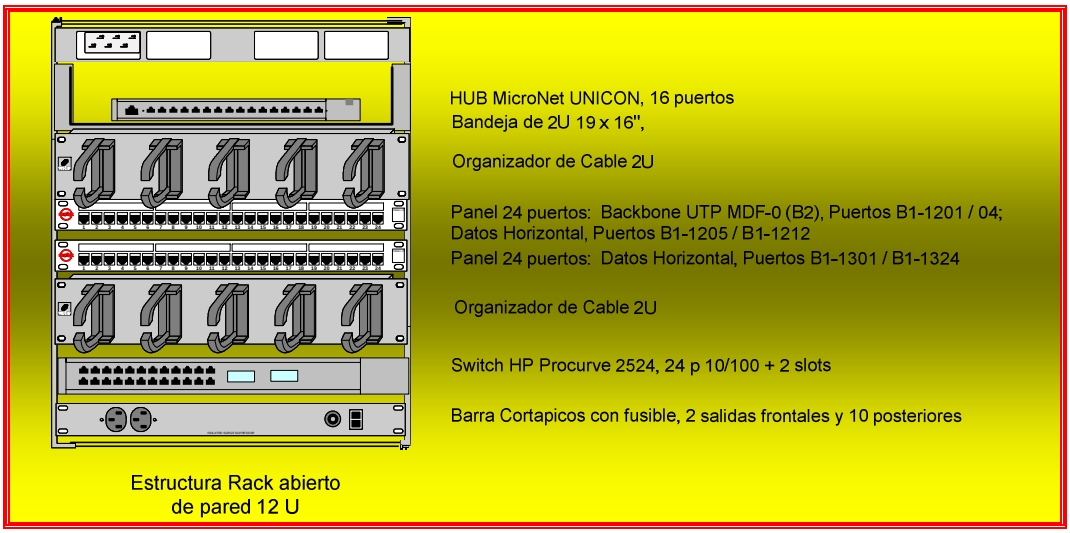

Figura2.3 **Rack B1**

La conexión entre los elementos está dispuesta de la siguiente manera:

Tabla2.7 **Interconexión de Equipos Rack B1 (Id: 1201-1224)**

Patch Panel	Id de Canal	Swicth HP2524
1	B1 1201	21
2	B1 1202	22
3	B1 1203	23
4	B1 1204	24
5	B1 1205	10
6	B1 1206	13
7	B1 1207	14
8	B1 1208	15
9	B1 1209	16
10	B1 1210	17
11	B1 1211	19
12	B1 1212	20
13	B1 1213	
14	B1 1214	
15	B1 1215	
16	B1 1216	
17	B1 1217	
18	B1 1218	
19	B1 1219	
20	B1 1220	
21	B1 1221	
22	B1 1222	
23	B1 1223	
24	B1 1224	

Tabla2.8 **Interconexión de Equipos Rack B1 (Id: 1301-1324)**

Patch Panel	Id de Canal	Swicth HP2524	Hub 3Com
1	B1 1301	1	
2	B1 1302	2	
3	B1 1303	3	
4	B1 1304	4	
5	B1 1305	5	
6	B1 1306	7	
7	B1 1307	8	
8	B1 1308	9	
9	B1 1309	12	
10	B1 1310		
11	B1 1311		
12	B1 1312		
13	B1 1313		
14	B1 1314		2
15	B1 1315		3
16	B1 1316		4
17	B1 1317		5
18	B1 1318		6
19	B1 1319		7
20	B1 1320		
21	B1 1321		8
22	B1 1322		9
23	B1 1323		11
24	B1 1324		

Tabla2.9 **Interconexión de Equipos Rack B1**

Swicth HP2524	Hub 3Com
11	Uplink

- **Bloque B2**

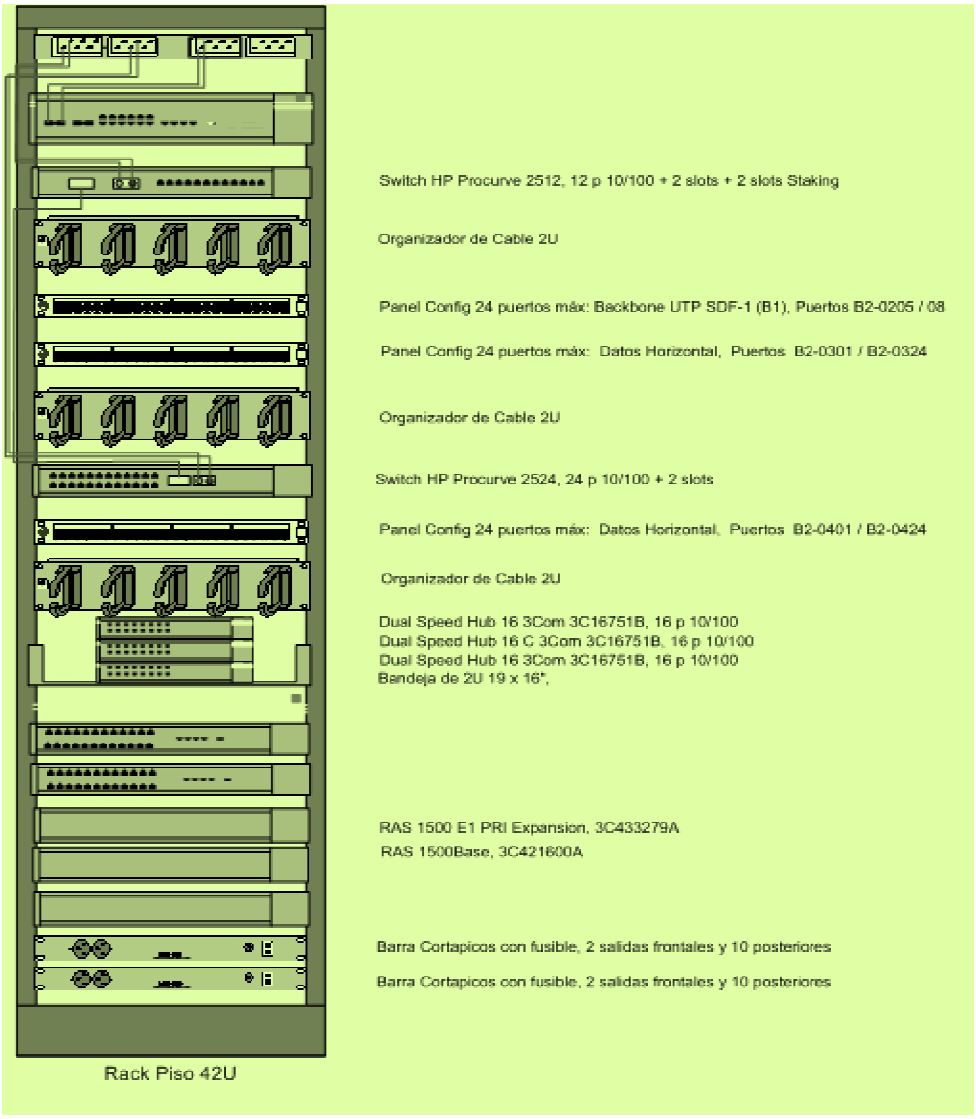

Figura2.4 **Rack B2**

La conexión entre los elementos está dispuesta de la siguiente manera:

Tabla2.10 **Interconexión de Equipos Rack B2 (Id: 2201-2224)**

Patch Panel	Id de Canal	Swicth 3Com 4050	Switch HP 2512	Switch HP 2524
1	B2 201	11		
2	B2 202			
3	B2 203			
4	B2 204			
5	B2 205			21
6	B2 206			22
7	B2 207			23
8	B2 208			24
9	B2 209			
10	B2 210			
11	B2 211			
12	B2 212			
13	B2 213			
14	B2 214			
15	B2 215			
16	B2 216			
17	B2 217			
18	B2 218	8		
19	B2 219	7		
20	B2 220	9		
21	B2 221	17		
22	B2 222		4	
23	B2 223			
24	B2 224	13		

Tabla2.11 **Interconexión de Equipos Rack B2 (Id: 2301-2324)**

Patch Panel	Id de Canal	Switch HP 2524	Hub 2	Hub 3
1	B2 301			1
2	B2 302			2
3	B2 303			3
4	B2 304			4
5	B2 305			5
6	B2 306			6
7	B2 307			7
8	B2 308			8
9	B2 309			9
10	B2 310			10
11	B2 311			11
12	B2 312			
13	B2 313			
14	B2 314			
15	B2 315			
16	B2 316			
17	B2 317		1	
18	B2 318		2	
19	B2 319		3	
20	B2 320			
21	B2 321	19		
22	B2 322	20		
23	B2 323		13	
24	B2 324		15	

Tabla2.12 **Interconexión de Equipos Rack B2 (Id: 2401-2424)**

Patch Panel	Id de Canal	Switch HP 2524	Switch 3Com 4050	Hub 2
1	B2 401	1		
2	B2 402	2		
3	B2 403	3		
4	B2 404	4		
5	B2 405	5		
6	B2 406	6		
7	B2 407	7		
8	B2 408	8		
9	B2 409	9		
10	B2 410	10		
11	B2 411	11		
12	B2 412	12		
13	B2 413			
14	B2 414			
15	B2 415			
16	B2 416			12
17	B2 417			11
18	B2 418	14		
19	B2 419	13		
20	B2 420		2	
21	B2 421	15		
22	B2 422	16		
23	B2 423	17		
24	B2 424	18		

Tabla2.13 **Interconexión de Equipos Rack B2**

Swicth 3Com 4050	Switch HP 2512	RAS	Switch 1 3Com 4500	Switch 2 3Com 4500
10			27	
11	12			
12				27
	6	LAN		

- **Bloque C1**

Figura2.5 **Rack B1**

La conexión entre los elementos está dispuesta de la siguiente manera:

Tabla2.14 **Interconexión de Equipos Rack C1 (Id: 5201-5224)**

Patch Panel	Id de Canal	Hub MicroNet	Switch HP 2512
1	C1 5201	7	
2	C1 5202		11
3	C1 5203		
4	C1 5204		
5	C1 5205		1
6	C1 5206		2
7	C1 5207		6
8	C1 5208	15	
9	C1 5209	14	
10	C1 5210		12
11	C1 5211		4
12	C1 5212	13	
13	C1 5213	12	
14	C1 5214	11	
15	C1 5215	10	
16	C1 5216		5
17	C1 5217		3
18	C1 5218		
19	C1 5219		
20	C1 5220		7
21	C1 5221		
22	C1 5222		8
23	C1 5223		
24	C1 5224		9

Tabla2.15 **Interconexión de Equipos Rack C1**

Swicth HP2512	Hub 3Com
10	Uplink

- **Bloque C2**

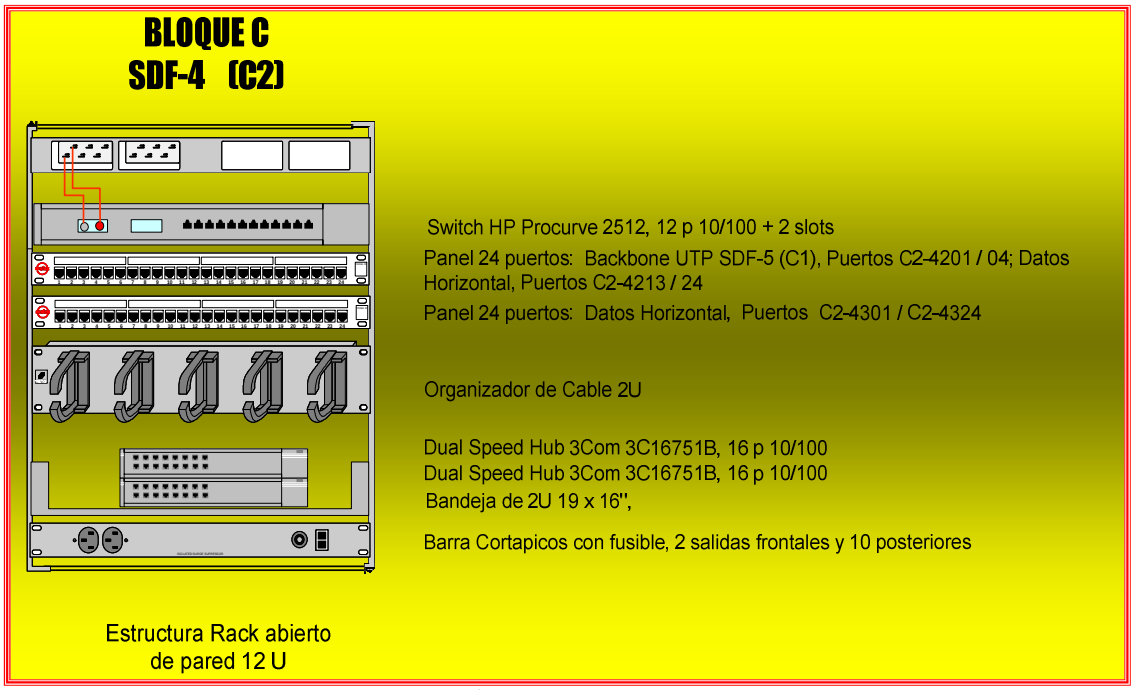

Figura2.6 **Rack B1**

Tabla2.16 **Interconexión de Equipos Rack C2 (Id: 4201-4224)**

Patch Panel	Id de Canal	Switch HP 2512
1	C2 4201	
2	C2 4202	
3	C2 4203	
4	C2 4204	
5	C2 4205	12
6	C2 4206	11
7	C2 4207	
8	C2 4208	
9	C2 4209	
10	C2 4210	
11	C2 4211	
12	C2 4212	
13	C2 4213	1
14	C2 4214	2
15	C2 4215	3
16	C2 4216	4
17	C2 4217	5
18	C2 4218	6
19	C2 4219	7
20	C2 4220	8
21	C2 4221	
22	C2 4222	
23	C2 4223	
24	C2 4224	

Tabla2.17 **Interconexión de Equipos Rack C2 (Id: 4301-4224)**

Patch Panel	Id de Canal	Hub 1	Hub 2
1	C2 4301		1
2	C2 4302		2
3	C2 4303		3
4	C2 4304		4
5	C2 4305		5
6	C2 4306		6
7	C2 4307		7
8	C2 4308		8
9	C2 4309		11
10	C2 4310		9
11	C2 4311		12
12	C2 4312		
13	C2 4313	4	
14	C2 4314	3	
15	C2 4315	2	
16	C2 4316	1	
17	C2 4317	15	
18	C2 4318	14	
19	C2 4319	11	
20	C2 4320		
21	C2 4321	13	
22	C2 4322	10	
23	C2 4323	12	
24	C2 4324	9	

Tabla2.18 **Interconexión de Equipos Rack C2**

Swicth HP2512	Hub 1	Hub 2
9		16
10	16	

2.4. Análisis del tráfico de la Red.

La medición de tráfico de datos se realizó utilizando el software Fluke Networks Optiview Protocol Expert. El software fue instalado en el host 10.1.30.132 conectado al puerto 2 del Switch 1, 3Com 4050 del rack B2, para realizar la captura del trafico de toda la red el Switch fue configurado como Port Mirroring (es una configuración que podemos establecer en un switch, con el fin de que éste envíe una copia de todos los paquetes que pasan por uno o más puertos a otro puerto concreto que llamamos monitor-port, ó a otro switch), el puerto 2 fue configurado de monitor-port y el puerto 20 como mirroring-port además que se agregaron todas la VLANS para con esto poder conectar el punto que pertenece al servidor que brinda todos los servicios.

Las siguientes figuras obtenidas mediante el software Fluke Networks nos permiten determinar las especificaciones del tráfico que circula por la red. La figura 2.7, nos permite conocer el porcentaje de tráfico en frames, por cada protocolo. Se puede observar que el

mayor tráfico que circula por la red es OTHERS (consiste en otros protocolos como CDP[6], ETHERNET, NMB[7], etc.). A continuación de OTHERS, el protocolo que más circula por la red es el HTTP.

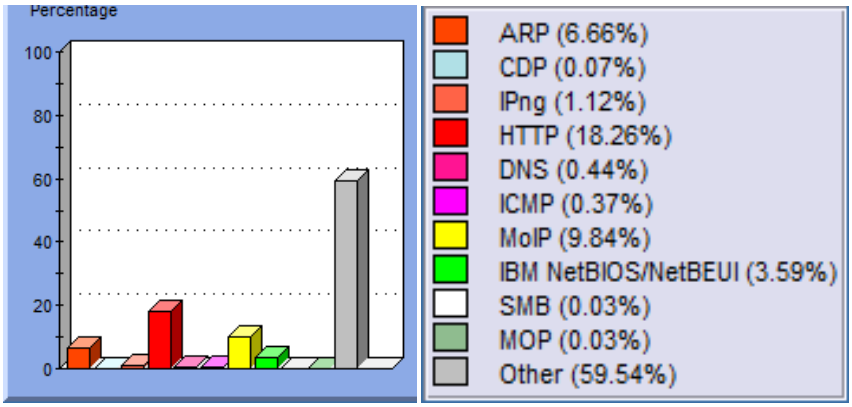

Figura2.7 **Captura de la Distribución por Protocolo**

En la figura 2.8 se puede observar el tamaño de los paquetes, en bytes, que más circulan en la red, es entre 1024 -1516 kbps.

[6] CDP.- Protocolo creado por CISCO. Obtiene información de routers y switches que están conectados localmente.
[7] NMB. - Protocolo de enlace de datos.

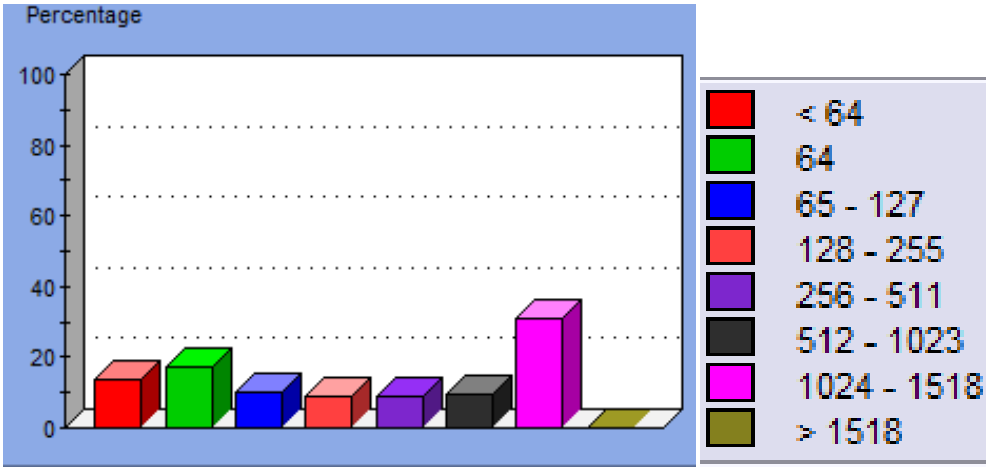

Figura2.8 **Tamaño de la Distribución de Paquetes**

En la figura 2.9, muestra los 10 equipos que reciben la mayor cantidad de tráfico, en frames, dentro de la red. Aquí se puede determinar que el equipo que recibe mayor tráfico es el 10.1.30.196, que pertenece a la red de profesores. El siguiente equipo que recibe mayor cantidad de frames, es el 10.1.0.112 que corresponde al servidor de nombre serverisa.espe.int. La figura 2.10 muestra, los mismos equipos pero indicando el respectivo tipo de aplicación:

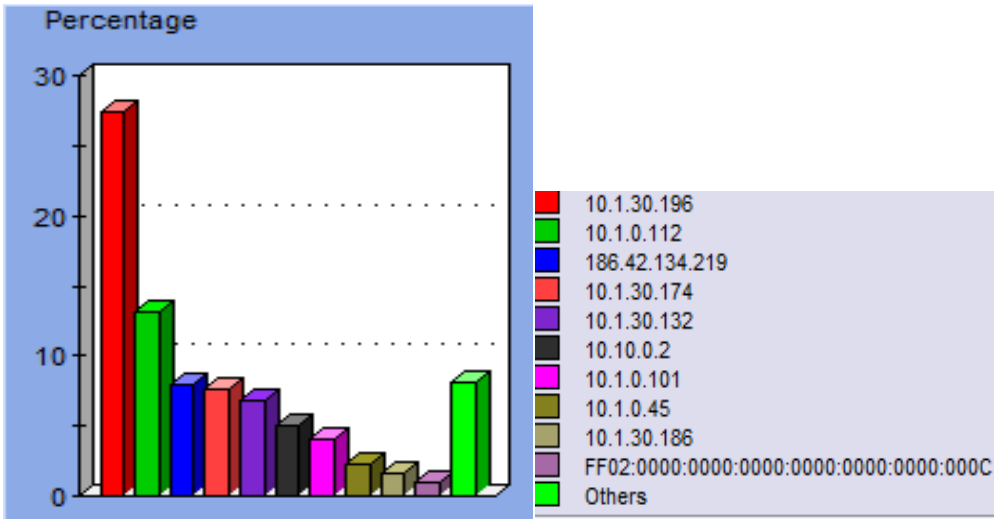

Figura2.9 **Equipos que reciben la mayor cantidad de tráfico en frames.**

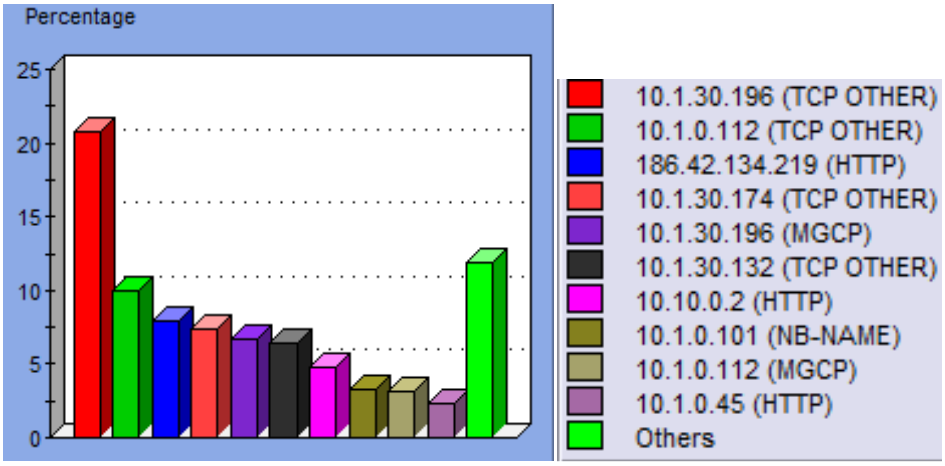

Figura2.10 **Equipos que reciben la mayor cantidad de tráfico y su aplicación.**

En la figura 2.11 se puede apreciar que los equipos que más tráfico comparten, son el host 10.1.30.196 y el servidor 10.1.0.112, que anteriormente fueron descritos. La figura 2.12 permite observar qué tipo de aplicación es la que se manejan entre estos equipos.

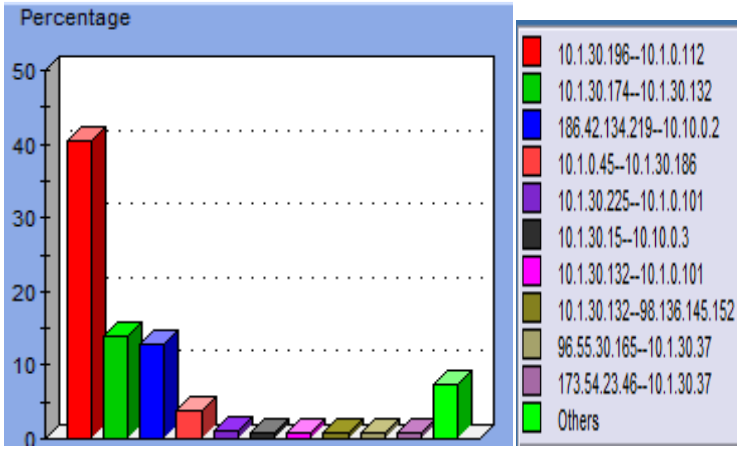

Figura2.11 **Equipos que comparten más tráfico.**

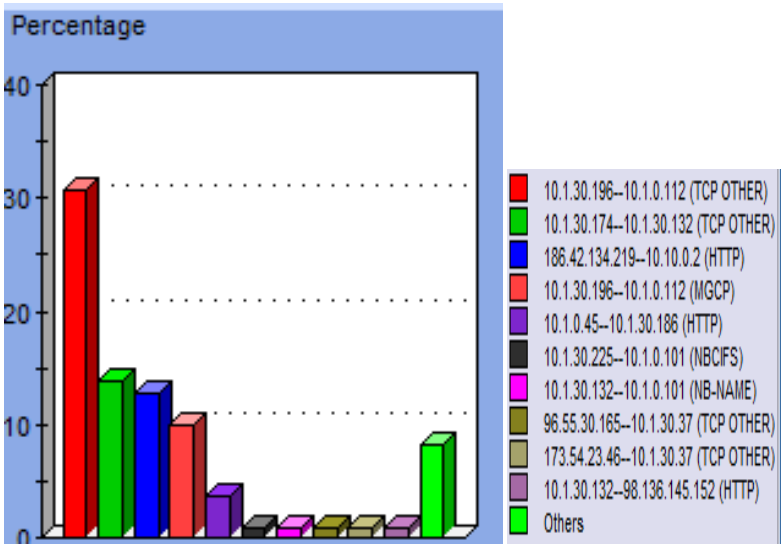

Figura2.12 **Equipos que comparten más tráfico y su aplicación.**

2.5. Tipo de Topología Física y Lógica

- **BLOQUE A1**

  SWITCH1-A1 (Mayo)
  IP: 10.10.0.250
  GW: 10.10.0.1

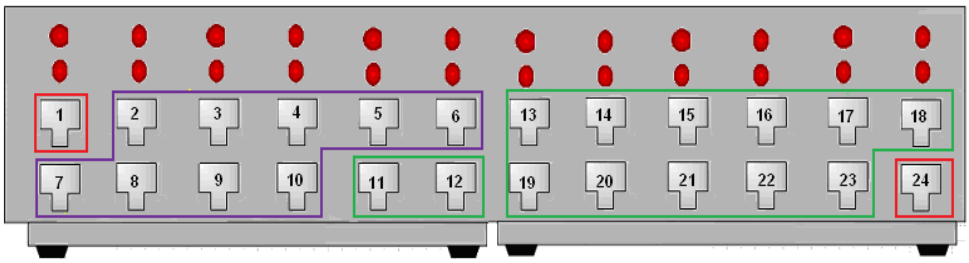

Figura2.13 **Switch 1 Rack A1 Vlans**

Tabla2.19 **Distribución de VLANs switch 1 Rack A1**

1. –
2. A1-2313
3. A1-2314
4. A1-2315
5. A1-2316
6. A1-2317
7. A1-2318
8. A1-2319
9. A1-2320
10. A1-2324
11. Hub 3Com (Puerto 1)
12. A1-2309
13. A1-2201
14. A1-2202
15. A1-2203

16. A1-2205
17. A1-2204
18. A1-2206
19. A1-2207
20. A1-2208
21. A1-2209
22. A1-2210
23. A1-2211
24. –

VLANS

Profesores
Alumnos A1
Todas las VLAN

- **BLOQUE B1**

SWITCH1-B1 (Julio)
IP: 10.10.0.251
GW: 10.10.0.1

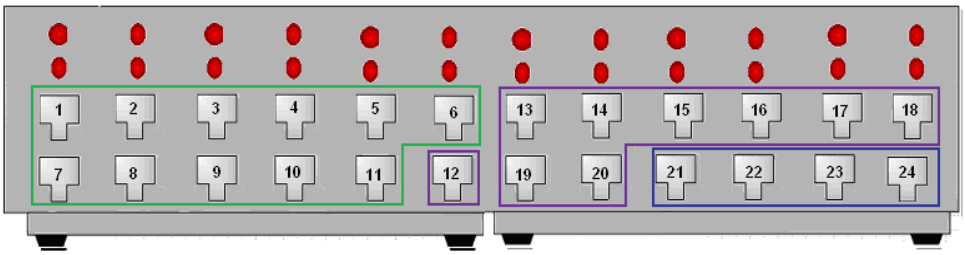

Figura2.14 **Switch 1 Rack B1 Vlans**

Tabla2.20 **Distribución de VLANs switch 1 Rack B1**

VLANS
1. B1-1301
2. B1-1302
3. B1-1303
4. B1-1304
5. B1-1305
6. –
7. B1-1306
8. B1-1307
9. B1-1308
10. B1-1205
11. Hub Uplink
12. –
13. B1-1206
14. B1-1207
15. B1-1208
16. B1-1209
17. B1-1210
18. –
19. B1-1211
20. B1-1212
21. B1-1201
22. B1-1202
23. B1-1203
24. B1-1204

Profesores
Alumnos B1
TRK al B2

- **BLOQUE B2**

SWITCH2-B2 (Enero)
IP: 10.10.0.254
GW: 10.10.0.1

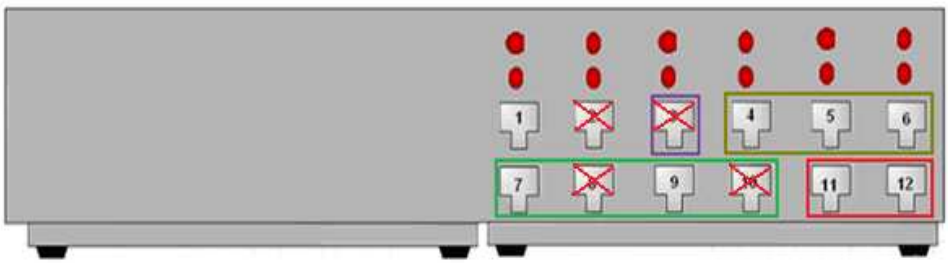

Figura2.15 **Switch 2 Rack B2 Vlans**

Tabla2.21 **Distribución de VLANs switch 2 Rack B2**

1. Switch 3Com (Puerto 12)	
2.-	
3.-	Profesores
4. B2-0222	Intranet
5. –	
6. RAS	
7. Hub3-B2 (Puerto 16)	Alumnos B2
8. –	
9. Hub2-B2 (Puerto 16)	
10. -	
11. B2-0201	Todas las VLANs
12. B2-0220	

VLANS

SWITCH3-B2

IP: 10.10.0.253
GW: 10.10.0.1

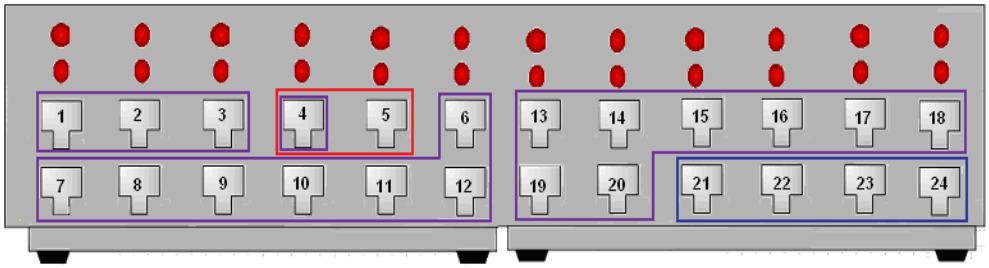

Figura2.16 **Switch 3 Rack B2 Vlans**

Tabla2.22 **Distribución de VLANs switch 3 Rack B2**

1. B2 0401	20. B2 0322
2. B2 0402	21. B2 0205
3. B2 0403	22. B2 0206
4. B2 0404	23. B2 0207
5. B2 0405	24. B2 0208
6. B2 0406	
7. B2 0407	
8. B2 0408	
9. B2 0409	
10. B2 0410	
11. B2 0411	VLANS
12. B2 0412	
13. B2 0419	
14. B2 0418	
15. B2 0421	
16. B2 0422	
17. B2 0423	Profesores
18. B2 0424	TRK al B1
19. B2 0321	Todas las VLANs

SWITCH4-B2

IP: 10.10.0.247
GW: 10.10.0.1

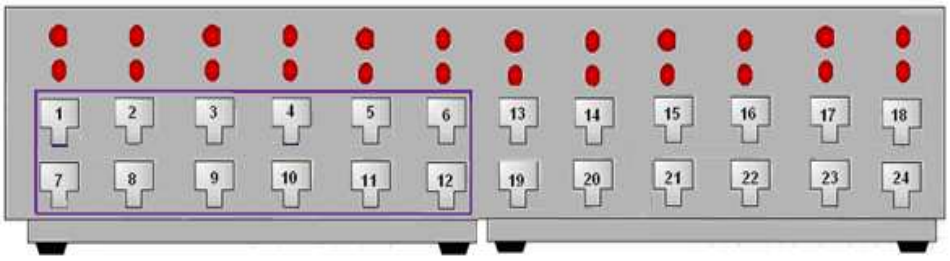

Figura2.17 **Switch 4 Rack B2 Vlans**

SWITCH5-B2

IP: 10.10.0.253
GW: 10.10.0.1

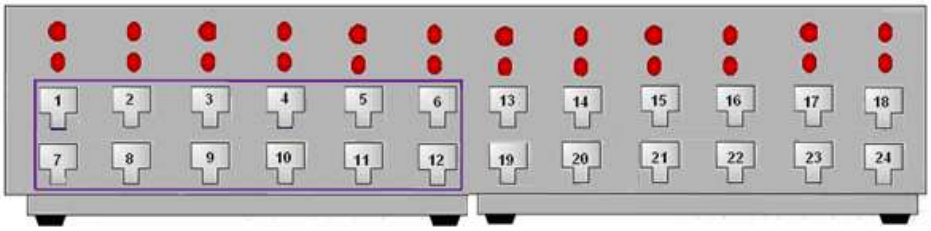

Figura2.18 **Switch 5 Rack B2 Vlans**

- **BLOQUE C1**

  SWITCH1-C1

  IP: 10.10.0.249
  GW: 10.10.0.1

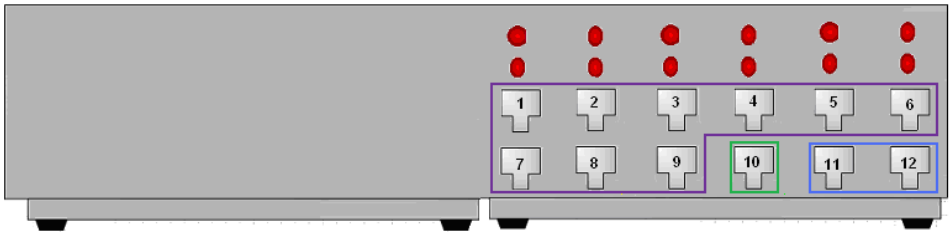

Figura2.19 **Switch 1 Rack C1 Vlans**

Tabla2.23 Distribución de VLANs switch 1 Rack C1

1. C1-5205	VLANs
2. C1-5206	
3. C1-5217	
4. C1-5211	
5. C1-5216	
6. C1-5207	
7. C1-5220	Profesores
8. C1-5222	Alumnos C1
9. C1-5224	TRK al C2
10. Hub Uplink	
11. C1-5202	
12. C1-5210	

2.6. Requerimientos de Seguridad

2.6.1. Seguridad que emplea la red

El Departamento de Eléctrica y Electrónica emplea un mecanismo de prevención para la seguridad de la red que permiten el control de acceso y la autenticación. Los mecanismos que se encuentran implementados en la red son:

- VLANs.- Las VLANs mejoran el rendimiento de la red y aumentan la seguridad, separando sistemas que tienen datos sensibles del resto de la red.

- Firewall.- Establece un enlace controlado, protege la red local de ataques generados en el Internet proporcionando un solo punto de protección. Todo el tráfico ya se proveniente de la red o desde afuera de esta debe pasar por el firewall. Además solo al tráfico autorizado (definido por una política de seguridad local) se le permitirá pasar
- ACL: son reglas que, según se requiera, permiten filtrar tráfico, permitiendo o denegando el tráfico de la red.
- Servidor de Backup:

Actualmente en la red del DEEE no se utilizan ninguna herramienta ni mecanismo que nos permita detectar ataques en la red.

2.6.2. Puntos Críticos

Este apartado comprende el análisis de la importancia de los servicios que presta la red del DEEE de la universidad, así como de los equipos que solicitan mayormente y aquellas que prestan dichos servicios. En el segmento de la red que analizamos, podemos definir servicios críticos basándonos en la necesidad de ellos para los usuarios; ellos son: DHCP, DNS, WEB, Correo. Por tanto estos son los servicios que se van a implementar en la red con el nuevo servidor UTM. El propósito es incluir el servidor pero adaptándolo totalmente a lo que actualmente se tiene implementado en el DEEE. La criticidad de cada servicio, su importancia, cantidad de usuarios, servicios, define la importancia de cada uno.

Basándose en la figura 2.17, se puede apreciar que el protocolo HTTP es uno de los más usados, por tanto el servicio web es uno de los que más tráfico genera dentro de la red, además del tráfico generado por el uso de internet mediante el servidor proxy 10.1.0.112. Otro punto crítico es el servidor DNS que es una de las aplicaciones con más tráfico. Tomando en cuenta la cantidad de usuarios que gestiona cada servidor y el mayor tráfico generado, está el servidor 10.10.0.2 que es el servidor web. Otro punto de criticidad es el servidor DHCP, dado que cualquier usuario para tener conectividad dentro de la red, y poder acceder a los diferentes servicios, requiere de asignación de direccionamiento de red, entonces el servidor DHCP es otro de los puntos críticos. Cabe resaltar además que el servidor firewall es el que proporciona todos los servicios, además de las peticiones al resto de la red por medio de su direccionamiento. Por ende los servicios que se encuentran en este servidor son esenciales, y este servidor es un punto crítico ya que de sufrir algún problema, la red dejaría de funcionar.

Teniendo en cuenta que el servidor Firewall es el más importante dentro de la red, se extraen los problemas de seguridad que aparecen en los datos proporcionados por los propios administradores, además, se realiza una búsqueda online de las vulnerabilidades conocidas sobre el sistema operativo y sobre los servicios implementados en cada servidor.

CAPÍTULO III

SOLUCIONES GENERALES PARA DOTAR DE SEGURIDAD A LA RED DEL DEEE

3.1. DESCRIPCIÓN

En este capítulo se requiere el estudiar qué software UTM que se encuentre en el mercado se adapte completamente al DEEE, así como también el desenvolvimiento que tienen todos los elementos de hardware del servidor en estado operativo, es decir, se analizan las funciones de cada uno para que el software que se instale opere óptimamente.

3.2. CLEAROS UTM

3.2.1. Requerimientos Mínimos

Tabla 3.1 Requerimientos Mínimos para que opere bien un CLEAROS UTM.

Hardware	
Memoria RAM	Mínimo 512 MB
Disco Duro	Mínimo 2 Gb
CD-ROM Drive	Solo se requiere para la instalación
USB	Solo se requiere para la clave de instalación
Video Card	Cualquier tarjeta de vídeo
Floppy Drive	No se requiere
Sound Card	No se requiere
Periféricos	
Mouse	No se requiere
Monitor y Keyboard	Sólo se requiere para la instalación
Red	
Banda ancha	Ethernet, cable, DSL
Tarjetas de Red	Se requiere una sola tarjeta, pero dos para el modo Gateway

3.2.2. Requerimientos de Hardware

Lo que se va a describir a continuación, son líneas de estimación para lo que sería el hardware necesario y correcto en un sistema para la utilización del ClearOs UTM, tomando en cuenta de que el hardware requerido depende de cómo se utiliza el software, es decir, una gran utilización del mismo requerirá más potencia del sistema del que se necesitaría para correr un simple Firewall.

Tabla 3.2 Capacidades para usuarios y Disco Duro para un CLEAROS UTM.

RAM y CPU	5 usuarios	5-10 usuarios	10-50 usuarios	50-200 usuarios
Processor/CPU	500 MHz	1 GHz	2 GHz	3 GHz
Memoria RAM	512 MB	1 GB	1.5 GB	2 GB
Hard Disk	La instalación y Logs requieren de 1 Gb. Si se quiere guardar toda la información recopilada por el dispositivo, depende de cada uno.			
RAID	Recomendado para sistemas críticos			

Cuando se utilizan los siguientes parámetros del UTM, se requiere más potencia del sistema:

- Intrusion Detection and Prevention (IDS/IPS)
- Content Filtering
- Webmail
- Antispam
- Antivirus

3.3. ENDIAN FIREWALL

La comunidad de Endian Firewall, es una línea de distribución de seguridad en Linux transforma cada sistema operativo a un dispositivo de seguridad con todas las funciones unificadas contra amenazas, características de un UTM. El software ha sido diseñado pensando en el usuario, es decir, es fácil de instalar, de gestionarlo pero sin perder flexibilidad. Entre las características más importantes está que incluyen un firewall de inspección de paquetes, proxies a nivel de la capa de aplicación para los distintos protocolos (HTTP, FTP, POP3, SMTP) con el apoyo de antivirus, virus y spamfiltering para el tráfico de correo electrónico (POP y SMTP), filtrado de contenido de tráfico web, y

una solución VPN. La ventaja de este dispositivo UTM es que es de código abierto, pero patrocinado por Endian.

Tabla 3.3 Detalles del ENDIAN UTM

	Características del Hardware					Características en Software	
General	Oficina/ Industrial	Mini	Mediana	GrandeX1	GrandeX2	5-10 Usuarios	25+ Usuarios
Número sugerido de usuarios	N/A	<25	<100	<250	250+	5-10	25+
Soporte directo de ENDIAN	x	x	x	x	x	x	x
Seguridad en la Red	Oficina/ Industrial	Mini	Mediana	GrandeX1	GrandeX2	5-10 Usuarios	25+ Usuarios
Firewall	X	X	X	X	X	X	X
Prevención contra intrusos (Snort)	X	X	X	X	X	X	X
Múltiples IPs públicas	X	X	X	X	X	X	X
Manejo de la calidad de servicio y ancho de banda	X	X	X	X	X	X	X
Soporte SNMP	X	X	X	X	X	X	X
Soporte VoIP/SIP	X	X	X	X	X	X	X
Escaneo de puertos	X	X	X	X	X	X	X
Prevención de flujos SYN/ICMP	X	X	X	X	X	X	X
Protección contra suplantación de identidad	X	X	X	X	X	X	X
Seguridad Web	Oficina/ Industrial	Mini	Mediana	GrandeX1	GrandeX2	5-10 Usuarios	25+ Usuarios
Proxies HTTP & FTP	N/A	X	X	X	X	X	X
Anti-virus	N/A	X	X	X	X	X	X
Soporte transparente del proxy	N/A	X	X	X	X	X	X
Análisis y filtrado de contenidos	N/A	X	X	X	X	X	X
Autenticación: Local, RADIUS, LDAP, Directorio activo	N/A	X	X	X	X	X	X
Seguridad de Correo	Oficina/ Industrial	Mini	Mediana	GrandeX1	GrandeX2	5-10 Usuarios	25+ Usuarios
Proxies SMTP & POP3	N/A	X	X	X	X	X	X
Auto aprendido de Spam	N/A	X	X	X	X	X	X
Reenvío de correo transparente (BCC)	N/A	X	X	X	X	X	X

X= Sí, x= Opcional, N/A = No Aplica

3.4. Astaro UTM

3.4.1. Especificaciones Técnicas

- Firewall con filtro de paquetes de inspección de estado profundo.
- Proxies transparentes para HTTP, FTP, SMTP, POP3, DNS y SOCKETS.
- Protección contra inundaciones DoS o DDoS, escaneo de puertos y gusanos.
- Actualizaciones diarias.
- Acceso remoto con SSL y VPN.
- Soporta VoIP: H.323, SIP.
- Autenticación vía Directorio Activo.
- Muestreo del tráfico de la red, dentro y fuera de la misma.
- Balanceo de carga.

3.5. UNTANGLE UTM

3.5.1. Especificaciones Técnicas

Untangle es una empresa privada que ofrece una pasarela de red (network gateway) de código abierto para pequeñas empresas. Untangle ofrece muchas aplicaciones como el bloqueo de correo electrónico no solicitado (spam), bloqueo de software malicioso (malware), filtrado de web, protección contra robo de información sensible (phishing), prevención de intrusiones, y más sobre la Plataforma Untangle Gateway.

Untangle fue fundada en 2003 como Metavize, Inc. por John Irwin y Dirk Morris. Metavize lanzó oficialmente en 2005 un Demo@15!. En 2006, Metavize recaudó $10.5 Millones de dólares a través de una financiación por parte de las empresas CMEA Ventures y Canyon Ventures y Asociados, nombró a Bob Walters como CEO (Presidente de la compañía), y cambió su nombre a Untangle, Inc. En 2007, Untangle lanzó la Plataforma Untangle Gateway de código abierto (Open Source) bajo la licencia GPL (versión 2). En 2007, Untangle también experimentó un crecimiento significativo y superó 100.000 usuarios repartidos en 2000 organizaciones.

Tabla 3.4 Requerimientos Mínimos de UNTANGLE

Recurso	Processor	Memory	Hard Drive	NICs	Notes
Mínimo	Intel/AMD-compatible Processor (800+ Mhz)	512 MB	20 GB	2	
1-50 usuarios	Pentium 4 igual o mayor	1 GB	80 GB	2 o más	
51-150 usuarios	Dual Core	2 GB	80 GB	2 o más	
151-500 usuarios	2 o más Cores	2 o más GB	80 GB	2 o más	
501-1500 usuarios	4 Cores	4 GB	80 GB	2 o más	64-bit
1501-5000 usuarios	4 o más Cores	4 o más GB	80 GB	2 o más	64-bit

La herramienta firewall multi-funcional de UNTANGLE simplifica y consolida muchos productos de red y seguridad que las organizaciones necesitan bajo las siguientes características:

- Accesible.- en código abierto se convierte en una herramienta de muy bajo precio al integrar muchos servicios en un solo software.
- Amplio.- maneja todo lo que es filtrado web, spam, control de red, administración de usuarios y ancho de banda, políticas de calidad QoS.

- Flexible.- permite el añadir y eliminar aplicaciones en función del crecimiento o requerimientos de la empresa.
- Garantizado.- actualmente protege 1.7 millones de personas in más de 30.000 organizaciones alrededor.

3.6. Zentyal UTM

Zentyal es una aplicación web que usa el servidor web Apache con lenguaje de programación Perl orientado a objetos que incluye algunas mejoras visuales con Javascript. Su diseño incorpora técnicas de programación modernas como:

- Patrones de diseño: un patrón de diseño observador usado principalmente para integrar diferentes módulos en Zentyal. Por ejemplo, cada servicio informa sobre que puertos necesitan que estén abiertos. Además, un patrón Singleton que se usa para almacenar la configuración y comportamiento global.
- Desacoplamiento de la lógica y presentación: la interfaz de usuario usa CSS (Cascading Style Sheets, lenguaje usado para definir la presentación de un documento estructurado escrito en HTML o XML) y AJAX (Asynchronous JavaScript And XML, técnica de desarrollo web que crea aplicaciones interactivas. Éstas aplicaciones se ejecutan en el cliente mientras se mantiene una comunicación asíncrona con el servidor en segundo plano, es decir, se pueden hacer cambios sobre las páginas sin necesidad de recargarlas), e incluye varios componentes Mason, como una tabla genérica usada para configurar servicios. La lógica del programa reside en los paquetes de las bibliotecas y en el código CGI (Common Gateway Interface, permite a un cliente solicitar datos de un programa ejecutado en el servidor web).
- Tolerancia a fallos: los errores y avisos se manejan a través de excepciones software, yendo desde el núcleo hasta la rutina.

- También ofrece la arquitectura para la búsqueda de errores, integrando la distribución de la pila de ejecución del intérprete de Perl 5.
- Cada proceso de cada servicio es monitoreado y si uno muere, éste relanzado automáticamente.

Características Generales.- Zentyal 2.0 (publicado en septiembre 2010) dispone de las siguientes características:

- Gestión de redes
- Cortafuegos y encaminamiento
- Filtrado de tráfico
- NAT y redirección de puertos
- VLAN 802.1Q
- Soporte para múltiples puertas de enlace PPPoE y DHCP
- Reglas para múltiples puertas de enlace, balanceo de carga y auto-adaptación ante la pérdida de conectividad
- Moldeado de tráfico (soportando filtrado a nivel de aplicación)
- Monitorización gráfico de tráfico
- Sistema de detección de intrusos en la red
- Cliente dinámico DNS
- Infraestructura de red
- Servidor DHCP
- Servidor NTP
- Servidor DNS
- Actualizaciones dinámicos mediante DHCP
- Servidor RADIUS
- Soporte de redes privadas virtuales
- Autoconfiguración de rutas dinámicas
- Proxy HTTP

- Caché
- Autenticación de usuarios
- Filtrado de contenido
- Antivirus transparente
- Delay pools
- Sistema de detección de intrusos
- Servidor de correo
- Dominios virtuales
- Recuperación de cuentas externas
- POP3 e IMAP con SSL/TLS
- Filtro de Spam y Antivirus
- Listas blancas, negras y grises
- Filtro transparente de POP3
- Catch-all account
- Webmail
- Servidor web
- Dominios virtuales
- Autoridad de Certificación
- Trabajo en grupo
- Gestión centralizada de usuarios y grupos
- Soporte maestro/esclavo
- Sincronización con un controlador de dominio Windows Active Directory
- Controlador Primario de Dominio (PDC) de Windows
- Política de contraseña
- Soporte para clientes de Windows 7
- Compartición de recursos
- Servidor de archivos
- Antivirus
- Papelera
- Servidor de impresión
- Groupware: Compartición de calendarios, agendas, webmail, wiki, etc.

- Servidor VoIP
- Buzón de voz
- Salas de conferencias
- Llamadas a través de un proveedor externo
- Transferencia de llamadas
- Aparcamiento de llamadas
- Música de espera
- Colas de llamadas
- Registros
- Salas de conferencias
- Rincón del Usuario de Zentyal
- Informes y monitorización
- Dashboard para centralizar la información de los servicios
- Monitorización del CPU, carga, espacio del disco, temperatura, memoria
- Estado del RAID por software e información del uso de disco duro
- Informes completos y resumidos de sistemas
- Notificación de eventos vía correo, subscripción de noticias (RSS) o Jabber/XMPP
- Actualizaciones de software
- Copias de seguridad (backup de configuración y remoto de datos)

Tabla 3.5 Requerimientos Mínimos de ZENTYAL

Perfil de Zentyal	Usuarios	CPU	Memoria	Disco	Tarjetas de red
Puerta de acceso	<100	P4 o equivalente	2G	80G	2 ó más
	100 ó más	Xeon Dual core o equivalente	4G	160G	2 ó más
UTM	<100	P4 o equivalente	1G	80G	1
	100 ó más	Xeon Dual core o equivalente	2G	160G	1
Infraestructura	<100	P4 o equivalente	1G	80G	1
	100 ó más	P4 o equivalente	1G	160G	1
Oficina	<100	P4 o equivalente	1G	250G	1
	100 ó más	Xeon Dual core o equivalente	2G	500G	1
Comunicaciones	<100	Xeon Dual core o equivalente	4G	250G	1
	100 ó más	Xeon Dual core o equivalente	8G	500G	1

3.7. SOLUCIÓNES ELEGIDAS QUE CUMPLA CON LOS REQUERIMIENTOS EN SOFTWARE Y HARDWARE

Según lo hasta ahora estudiado, se determina que los UTMs UNTANGLE y Zentyal son lo que mejor se adaptarían a la topología de red del DEEE. Todos los que hasta ahora se ha estudiado tienen prácticamente los mismos estándares mínimos en hardware para su implementación, sin embargo ClearOS, Endian y Astaro tienen la mayor parte de sus appliances licenciadas, de manera contraria, UNTANGLE y ZENTYAL se desarrollaron en lenguaje OPEN SOURCE. Adicionalmente éstos dos manejan una interfaz gráfica más amigable y tienen en sus propias páginas troubleshooting o atención a sus usuarios según los problemas más frecuentes, así como también foros en los que se pueden hacer consultas gratuitas del manejo de sus software.

3.8. PROCESAMIENTO EN LÍNEA

El procesamiento en línea implica que los programas se ejecuten de tal forma que los datos se actualicen de inmediato en los archivos de la computadora. En el caso del software a instalarse, el procesamiento en línea se refiere a que cada que se ingrese algún parámetro en la interfaz de usuario, éste se modifique en tiempo real en la base de datos del servidor. El tiempo es el que determina cuán rápido puede procesar un computador cierta información y esto va a depender de los siguientes parámetros:

3.8.1. Procesador.- Los procesadores se describen en términos de su tamaño de palabra, su velocidad y la capacidad de RAM asociada.

- **Tamaño de la palabra** que es el número de bits que se maneja como una unidad en un sistema de computación en particular. Normalmente, el tamaño de palabra de las microcomputadoras modernas es de 32 bits; es decir, el bus del sistema puede transmitir 32 bits (4 bytes de 8 bits) a la vez entre el procesador, la RAM y los periféricos.
- **La Velocidad del procesador** se mide en diferentes unidades según el tipo de computador, MHz (Megahertz) para microcomputadoras. La velocidad del procesador de una micro se mide por su frecuencia de oscilación o por el número de ciclos de reloj por segundo. El tiempo transcurrido para un ciclo de reloj es 1/frecuencia. Para estaciones de trabajo, la velocidad del procesador se mide en MIPS (Millones de instrucciones por segundo). Las supercomputadores son medidas en FLOPS *(floating point operations per second*, operaciones de punto

flotante por segundo). Hay supercomputadoras para las cuales se puede hablar de GFLOPS (Gigaflops, es decir 1.000 millones de FLOPS).

- **Capacidad de la RAM** que se mide en términos del número de bytes que puede almacenar. Habitualmente se mide en KB y MB, aunque ya hay computadoras en las que se debe hablar de GB.

3.8.2. Canales, puertos y ranuras de expansión

- **Canales:** Grupos de cables a través de los cuales viaja la información entre los componentes del sistema. Tienen 8, 16 o 32 cables y este número indica la cantidad de bits de información que puede transmitir al mismo tiempo. Los canales más anchos pueden transmitir información con más rapidez que los canales angostos.
- **Ranuras de expansión:** Se conectan al bus eléctrico común. Algunos canales están conectados a ellas en la caja del computador. Los usuarios pueden personalizar sus máquinas insertando tarjetas de circuitos (o *tarjetas*) de propósito especial en estas ranuras. Existen tarjetas de expansión de RAM, adaptadores de color y de gráficos, fax módem, puertos, coprocesadores (procesadores adicionales que incrementan la capacidad o velocidad de procesamiento del sistema).
- **Puertos:** Son puntos de conexión en la parte exterior del chasis de la computadora a los que se conectan algunos canales. El puerto permite una conexión directa con el bus eléctrico común de la PC. Los puertos pueden ser Puertos Series, que permiten la transmisión en serie de datos, un bit a la vez. Este tipo de puertos permiten una interfaz con impresoras y módems de baja velocidad. Puertos paralelos, que permiten la transmisión paralela de datos, es decir que se transmiten varios bits simultáneamente. Permiten la interfaz con dispositivos tales como

impresoras de alta velocidad, unidades de cinta magnética de respaldo y otras computadoras.

3.8.3. El Bus del Sistema

El bus del sistema conecta a los elementos que forman una computadora. Existen tres buses principales: el bus de datos, el bus de direcciones y el bus de control. Un bus es un conjunto de alambres por los que pasan señales eléctricas entre los componentes de un sistema, estos buses varían en cada procesador, sin embargo cada bus transporta información equivalente para todos los procesadores.

- **El Bus de Datos.-** Los procesadores utilizan el bus de datos para intercambiar información entre los diferentes componentes del sistema. El tamaño de éstos buses es variable dependiendo del tipo de procesador, por esta razón es común pensar en el tamaño del bus como una medida del "tamaño" del procesador, puede haber buses de datos de 8, 16, 32 ó 64 líneas. En cada línea del bus de datos se transmite un bit de información pero un sistema no está limitado a manejar información de acuerdo al tamaño del bus de datos, es decir, un bus de 32 bits no está limitado a trabajar con tipos de datos máximos de 32 bits. El tamaño del bus de datos por otro lado si limita el número de bits que el sistema puede manejar por cada ciclo de memoria de tal manera que un sistema de 16 bits necesita dos ciclos de memoria para manejar un tipo de dato de 32 bits, naturalmente pero no necesariamente, un sistema de 32 bits es el doble de rápido que un sistema de 16 bits, la limitación es porque existen otros factores que influyen en el rendimiento de un sistema.

- **El bus de direcciones.-** El bus de direcciones es el encargado de diferenciar las ubicaciones físicas de cada elemento de un sistema de cómputo, sea memoria ó elemento de E/S, cuando un programa necesita tener acceso a un elemento determinado del sistema coloca su dirección en el bus de direcciones, los circuitos electrónicos asociados sea con la memoria ó con un dispositivo de E/S son los encargados de reconocer ésta dirección y consecuentemente colocar los datos correspondientes en el bus de datos. Con una sola línea de dirección es posible tener acceso a dos elementos diferentes, con n líneas de dirección se puede acceder a 2n direcciones diferentes, por lo tanto el número de bits de un bus de direcciones determina la cantidad máxima de direcciones de memoria que un sistema puede acceder.
- **El Bus de Control.-** El bus de control es una colección de líneas que transportan un conjunto de señales cuyo propósito es la sincronía de todas las operaciones efectuadas por el CPU con los diferentes subsistemas de un equipo de cómputo, destacan las líneas para escritura (write) y lectura (read) de datos, el reloj del sistema, líneas de interrupción, líneas de estado.
- **Bus Local PCI.-** El bus local PCI (Peripheral Component Interconnect) es un bus de alta perfomance de 32 o 64 bits con líneas de dirección y de datos multiplexadas. Su uso se orienta como mecanismo de interconexión entre controladores de periféricos altamente integrados, placas periféricas de expansión y sistemas procesador/memoria. Se ha definido como meta principal establecer un estándar industrial, con una arquitectura de bus local de alta perfomance que ofrezca bajo costo y permita diferenciación. El punto fundamental es permitir nuevos valores en cuanto a precio y perfomance de los sistemas actuales, pero también es importante que el nuevo estándar se acomode a los requerimientos de sistemas futuros y sea aplicable a múltiples plataformas y arquitecturas. Por otro lado, mientras que las estructuras de bus local iniciales se centraban en aplicaciones para los sistemas de escritorio low-end hasta high-end, el bus PCI también comprende los requerimientos de sistemas móviles (Laptops) hasta servidores departamentales. El bus local PCI ofrece beneficios adicionales a los usuarios. Registros de configuración se especifican para los componentes y placas

de expansión PCI. Con esto se logran sistemas con software de auto-configuración automática incluido, el que es corrido durante el encendido, evitándole al usuario la tarea de configurar el sistema manualmente (Plug & Play).

- **Capacidades y beneficios del bus local PCI.-** El bus local PCI fue especificado para establecer un estándar de bus local de alta perfomance para varias generaciones de productos. Las especificaciones proveen una selección de cualidades que permiten alcanzar múltiples puntos de perfomance/precio y puede habilitar funciones que permitan diferenciación a nivel de componente. Las cualidades salientes pueden resumirse en:

Alta perfomance

- ✓ Upgrade transparente de 32 bits de datos a 64 bits a 33 MHz (132 MB/s a 264 MB/s pico) y de 32 a 64 bits a 66 MHz (264 MB/s a 528 MB/s pico).
- ✓ Variable lenght linear and caché line wrap mode bursting tanto para lectura como para escritura, que mejora la perfomance gráfica dependiente de escritura.
- ✓ Accesos aleatorios de baja latencia (60 nseg para 33 MHz y 30 para 60 MHz de latencia de acceso para escritura desde un máster que ocupa el bus y un registro esclavo).
- ✓ Capaz de soportar concurrencia total con el subsistema procesador/memoria. Bus sincrónico con operación hasta 33 o 66 MHz.
- ✓ Arbitraje central oculto (solapados).

Bajo costo

- ✓ Optimizado para interconexión directa (no necesita lógica de conexión). Las especificaciones eléctricas, para drivers y frecuencia se obtienen con tecnologias ASIC estándar y otros procesos típicos.

- ✓ La arquitectura multiplexada reduce el número de pines (47 para esclavos y 49 para maestros) y el tamaño de los encapsulados o permite implementar funciones adicionales en encapsulados de tamaño particular.
- ✓ Las placas de expansión simples PCI trabajan en sistemas ISA, EISA y MC. (Con cambios mínimos a los diseños de chasis existentes), reduciendo inventarios y minimizando la confusión para el usuario final.

Facilidad de uso

- ✓ Permite soporte completo para auto configuración de placas de expansión o componentes PCI. Los dispositivos PCI poseen registros con la información necesaria para esto.

Longevidad

- ✓ Por ser independiente del microprocesador soporta múltiples familias de estos como también lo hará con las futuras generaciones (mediante puentes o integración directa)
- ✓ Soporta direccionamiento de 64 bits.
- ✓ Entornos de 3,3 y 5 volts se han especificado. El camino de migración entre tensiones permite una transición gradual en la industria.

Interoperabilidad/confiabilidad

- ✓ Pequeño factor de tamaño en placas de expansión.
- ✓ La señalización actual permite que las fuentes de alimentación sean optimizadas para el uso esperado del sistema monitoreando placas de expansión que puedan sobrepasar la máxima potencia prevista para el sistema.

- ✓ Más de 2000 horas de simulación eléctrica SPICE con validación de modelos en hardware.
- ✓ Compatibilidad hacia adelante y atrás de 32 y 64 bits en placas de expansión y componentes.
- ✓ Compatibilidad hacia adelante y atrás de 33 y 66 MHz en placas de expansión y componentes.
- ✓ Confiabilidad incrementada y interoperabilidad de placas de expansión mediante la comprensión de los requerimientos de carga y frecuencia del bus local a nivel componentes, eliminando buffers y lógica de pegado.
- ✓ Conectores de expansión tipo MC.

Flexibilidad

- ✓ Capacidad total multi-maestro, permitiendo que cualquier maestro PCI pueda acceder puerto a puerto con cualquier esclavo PCI.
- ✓ Un slot compartido acomoda tanto a placas estándar ISA, EISA o MC como a placas de expansión PCI.

Integridad en los datos

- ✓ Provee paridad tanto en datos como en direcciones, y permite la implementación de plataformas robustas.

3.9. MODO PROMISCUO

Es aquel en el que una computadora conectada a una red compartida, tanto la basada en cable como la que usa tecnología inalámbrica, captura todo el tráfico que circula por ella. Este modo está muy relacionado con los sniffers (programa que tiene la capacidad de analizar el tráfico de una red) que se basan en este modo para realizar una tarea. En las redes, la información se transmite en una serie de paquetes con la dirección física o MAC de quien lo envía y quien lo tiene que recibir, de manera que cuando se transmite un fichero, éste se divide en varios paquetes con un tamaño predeterminado y el receptor es el único que captura los paquetes. En el modo promiscuo, una máquina intermedia captura todos los paquetes, que normalmente desecharía, incluyendo los paquetes destinados a él mismo y al resto de las máquinas. Resulta a destacar que las topologías y hardware que se usen para comunicar las redes, influye en su funcionamiento, ya que las redes en bus, redes en anillo, así como todas las redes que obliguen a que un paquete circule por un medio compartido, al cual todos tienen acceso, los modos promiscuos capturarán muchos más paquetes que si están en una red con topología en árbol. Para completar el modo, las máquinas en modo promiscuo suelen simplemente copiar el paquete y luego volverlo a poner en la red para que llegue a su destinatario real (en el caso de topologías que requieran de retransmisión). Los softwares UTM trabajan en modo promiscuo para de esta manera analizar cada paquete que es detectado como circulante.

CAPÍTULO IV

INSTALACIÓN DE LOS UTMs EN LA RED DEL DEEE

4.1.DESCRIPCIÓN

El presente capítulo implementa los dos softwares UTM elegidos como los que mejor se adaptan a las características de la red del DEEE. Se observará, analizará y probará el desempeño que tiene en sus modos de operación, así como también sus respuestas ante fallas. Éstos software, tal como se especifica en los manuales de cada fabricante, manejan su propio sistema operativo de libre distribución, lo que facilita la adquisición del o los appliances que se requieran en el tiempo según la demanda de servicios que necesite la red. Adicionalmente, se tratará de inyectar a las pruebas del laboratorio, tráfico considerado como malicioso, a fin de comprobar el desenvolvimiento del dispositivo, a más de, mediante capturas de tráfico, comprobar la forma en la que operan estos UTMs. Se considerará también un dimensionamiento en cuanto a número de usuarios por VLAN, servicios a los que podrán acceder, políticas de direccionamiento y ancho de banda.

4.2. IMPLEMENTACIÓN DEL UTM

4.2.1. Consideraciones de Implementación

Se ha diseñado un escenario similar a la topología de la red del DEEE, en el que se probarán los softwares UTM, de tal manera que al adaptarle el más idóneo, solo se requiera de un intercambio físico con el servidor actualmente operativo, mismo que constará de:

- 3 tarjetas de red, donde cada una de ellas cumplirá con funciones distintas.
- La primera tarjeta de red cumplirá con la función de troncal por dónde pasarán las VLANs y por la que se levantarán los servicios DHCP, DNS.
- La segunda tarjeta de red será GATEWAY para la conexión con el internet que provee la Universidad.
- La tercera tarjeta también será GATEWAY para la otra conexión del Departamento para la salida al internet y por donde solo ciertos usuarios de cada VLAN podrán acceder.
- Un switch de puerto GIGA, mismo que tendrá un puerto nativo y tres puertos designados para cada VLAN ya mencionadas anteriormente.
- Tres switches, cada uno de los cuales direccionará cada VLAN.

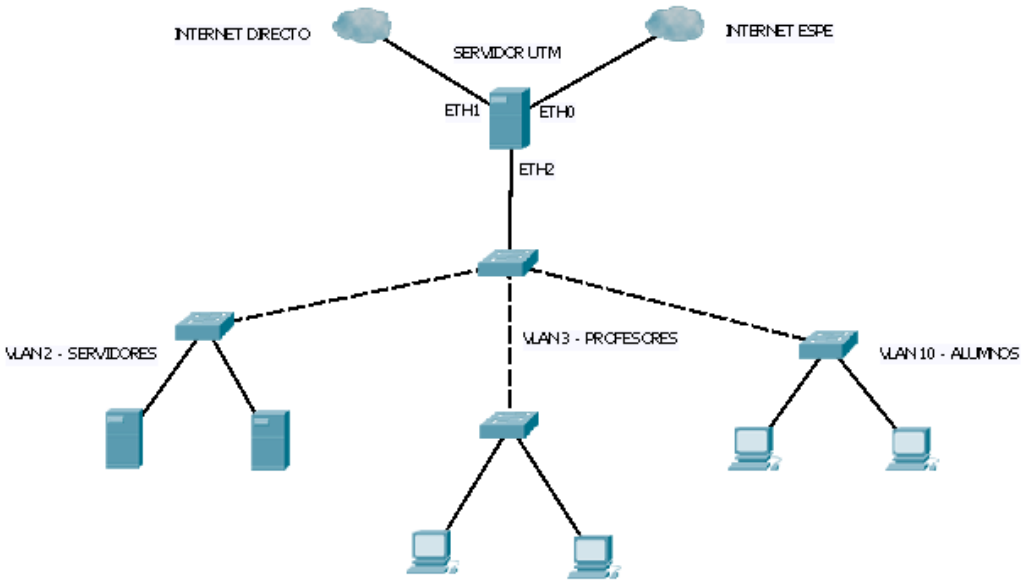

Figura4.1 Topología de la red de pruebas.

El servidor actúa como GATEWAY ante las dos salidas que se tiene al internet (FastEthernet 0, FastEthernet 1), que en modo de operación normal, por cada una los usuarios de las VLANs están saliendo constantemente dependiendo de cómo se lo determine, pero en caso de falla la una interfaz actúa como back up de la otra, es decir como FAILOVER. La interfaz FastEthernet 2 es por donde se levantarán los servidores DHCP y DNS por VLAN, como ya se lo mencionó anteriormente y se lo detalla en la siguiente tabla:

Tabla4.1 Configuración de VLANs

Interfaz	Red	Name	VLAN
Eth2:2	10.1.30.1/24	Red de Profesores	2
Eth2:3	10.1.29.1/24	Red de Alumnos	3
Eth2:10	10.10.0.1/24	Red de Servidores	10

4.3. Proceso de Instalación de los Software UTM

4.3.1. Untangle UTM

Untangle UTM es conocido en el mercado por su interfaz gráfica muy amigable con el usuario y versatilidad en cualquier topología, es decir, que éste software puede ser instalado en un servidor que tenga una sola tarjeta de red y actuará de la misma manera como que si tuviera 2 o 3. El inconveniente con esta topología es que se reduce la capacidad y velocidad de procesamiento datos, lo que se puede reducir al máximo con la implementación de un puerto GigabitEthernet o en el mejor de los casos 10GigabitEthernet. Por la calidad de la interfaz gráfica, éste UTM tiene requerimientos mínimos más exigentes que toda la competencia, pues presenta gráficamente al usuario el procesamiento de datos en tiempo real. El procedimiento de instalación se lo detalla a continuación:

a) Se procede a la instalación del CD en el servidor, cual si fuera un CD de inicio o de sistema operativo, para ello se debe poner al servidor como prioridad de lectura de boot al CD-ROOM
b) A continuación el programa va a pedir escoger algunas opciones para la instalación, comenzando desde el idioma, se selecciona el español.

Figura4.2 Selección del Idioma español

c) Ahora se selecciona el país (Ecuador) e idioma de distribución del teclado (español).

Figura4.3 País e Idioma de instalación

d) Luego se va a proceder a formatear el disco. UNTANGLE le pide únicamente el aprobar o no el formateo.

Figura4.4 Formateo de disco

e) La siguiente pantalla indica que UNTANGLE utiliza herramientas de sistema de GNU y combinación del núcleo o Kernel libre similar a Linux, es decir, que todo el código usado puede ser modificado y redistribuido libremente bajo los términos de la Licencia Pública General de GNU. El proyecto GNU en sí fue creado para mantener un espíritu de cooperación entre los usuarios. Es así que se establece una interacción entre el núcleo del sistema operativo y el usuario o los programas de aplicación. A éstas variantes se las denomina distribuciones, mismas que deben cumplir con las necesidades generales o específicas para aplicarlas en servidores o supercomputadoras, que es donde se tiene el nicho de mercado. Según cifras más exactas, IDC[8] informa que el 78% de los 500 servidores más importantes del mundo utilizan GNU/Linux.

[8] International Data Corporation (IDC), es una firma de mercado y análisis especializada en tecnologías de la información, telecomunicaciones y tecnología del consumidor.

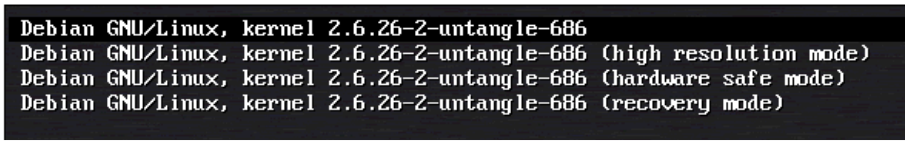

Figura4.5 Herramienta de sistema de GNU y combinación de núcleo kernel-Linux

f) Una vez iniciado el sistema operativo, aparecen las características de configuración global, es así que se comienza con el idioma. Se escogerá el español.

g) El siguiente paso es la configuración del password, esto con el fin de que solamente el administrador de la red pueda hacer cambios y gestionar el software de seguridad. Por default el nombre de administrador está configurado como admin, las contraseñas también se las registrará como admin. También se selecciona la zona horaria, se selecciona América/Guayaquil.

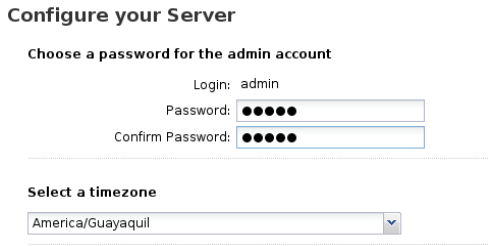

Figura4.6 El password es admin

h) El siguiente paso de configuración es el del nombre, apellido y mail del administrador de red. Hay que saber que el programa puede ser gestionado fuera de la red, puesto que todos los días (si es que así se lo programa) se envía el registro de logs de todos los ingresos o vulnerabilidades que tuvo la red, al mail que se ingrese en la siguiente parte. Adicionalmente se escoge el número de computadores que se van a administrar. Se determina que para las características del servidor y según lo

que determina el fabricante, se podrán administrar un máximo de 500 usuarios, pero en este caso se determinan 100 usuarios. Y finalmente, hay que determinar qué tipo de red se está administrando, es decir, para éste caso, se escoge School. La dirección de red se ha puesto para pruebas cristhian173@hotmail.com. Toda esta información se la observa en la siguiente imagen:

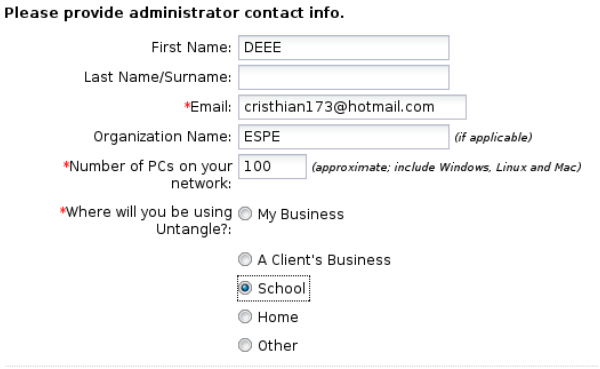

Figura4.7 Datos del administrador y de la red

i) En ésta siguiente parte, el servidor detectará las tarjetas de red que tiene el servidor, en este caso detecta tres y a cada una le asigna por default un nombre específico, mismos que pueden ser cambiados si así se lo requiere dentro de la configuración del servidor. Por ejemplo en la topología de red propuesta se cambiará el nombre DMZ por interfaz de usuarios. Posteriormente como proceso de instalación sólo se va a configurar la primera tarjeta de red que es la que se va a conectar al internet, y más adelante se va a configurarán las otras dos según lo explicado anteriormente.

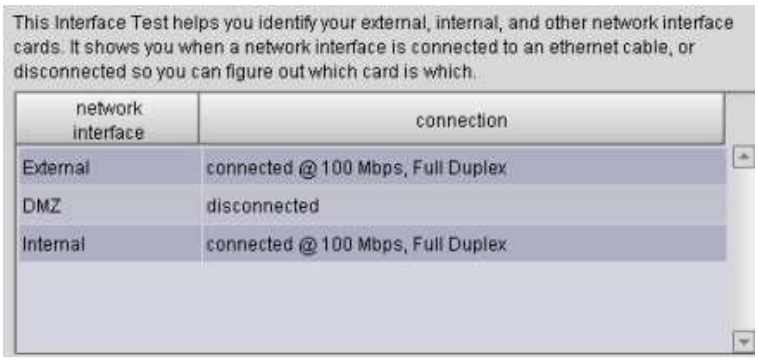

Figura4.8 Detección de las tarjetas y topología de red.

j) En la siguiente parte, el software determina la topología de la red, dando click en el botón actualizar, escogiendo previamente si es que la dirección de red se la obtiene por DHCP o enrutamiento estático. Si es que se escoge DHCP será porque se tiene un router o servidor que le proporciona al éste un direccionamiento dinámico. En éste caso se determina la configuración como DHCP y se recibe la dirección 10.0.2.15 provisionada por el actual servidor del DEEE.

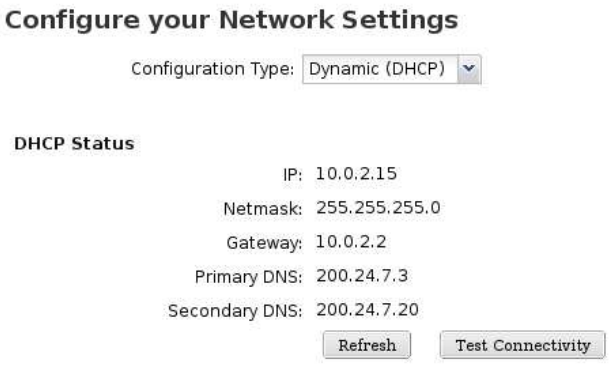

Figura4.9 Detección de características de red

k) Para comprobar si es que los datos del administrador son los correctos, UNTANGLE UTM, en el siguiente paso pide verificar si es que se quiere enviar un correo a la dirección de e-mail ingresada. Puede ser o no la dirección de correo electrónico configurada anteriormente en el ingreso de datos iniciales del administrador de red, en este caso es la misma. Se comprueba luego que el servidor envía un mail de prueba a la dirección de correo ingresada.

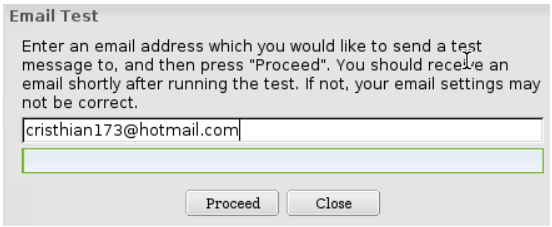

Figura4.10Completando proceso

l) Una vez ya completo el proceso de configuración, se ingresa al software.

Figura4.11 Ingreso al software

m) En ésta parte se determinan los servicios que se van a levantar en el servidor para la protección de la red. Es así que se escogen los siguientes:
    - Protección de la red de amenazas externas, como virus o malware.
    - Anti-spam, anti-phishing.
    - Control de actividad de la red, como ingreso a páginas web no apropiadas.
    - Acceso remoto.

n) Se deberán seleccionar algunas características adicionales, tales como:
    - Si se tiene o no ya un servidor Firewall instalado en la red. En este caso no se tiene.
    - Si se quiere protección de antivirus que trabaje en otra capa de la que lo hace el UTM. Para esto se requiere la instalación de un antivirus licenciado, lo cual no es nuestro caso.
    - Deja instalar un servidor de Active Directory. No se requiere.
    - Diferentes políticas de administración para diferentes usuarios.
    - Si se quiere o no sacar un respaldo del servidor diariamente.
    - Si se quiere o no asistencia remota de parte del fabricante.

o) Una vez establecidas todas las características de la red y servicios adicionales que se desean levantar en el servidor, se procede con la selección de los programas que se desea instalar. En este proceso, se empieza con la descarga de los programas seleccionados desde los servidores del fabricante.

p) Luego del proceso de selección y descarga de los servicios, se observa el llamado según el fabricante “rack”, que es donde se encuentran todos los servicios que se encuentran operando en la red.

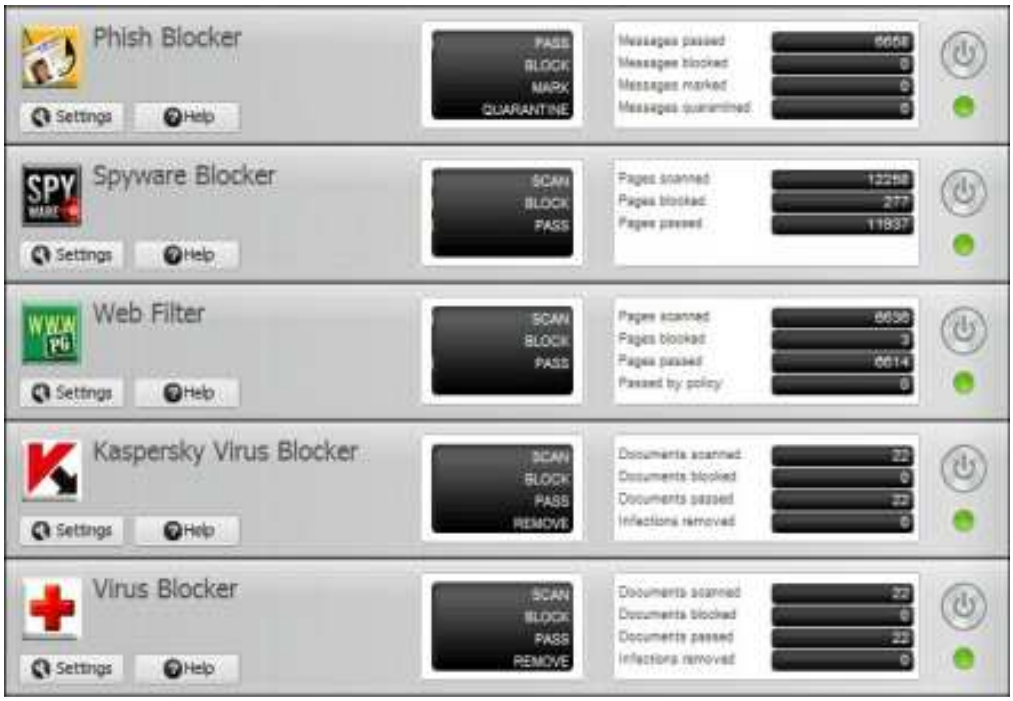

Figura4.12 Programas de protección instalados

q) A continuación se va a detallar el proceso de configuración de cada servicio, para lo cual se va a enfocar en los tipos de amenazas que podría recibir una universidad, mismos que fueron detallados en el capítulo 1, MARCO TEÓRICO.

El primer servicio es ANTIPHISHING, mismo que previene todo tipo de ataques o estafas cibernéticas mediante el uso de ingeniería social, es decir, mantener información confidencial mediante la manipulación de usuarios legítimos. Información que puede ser, contraseñas, claves, datos íntimos que pueden ser usados para fines ilegales, información detallada sobre tarjetas de crédito o cualquier información bancaria. Éste estafador o también llamado phisher toma la identidad de una persona o empresa cualquiera, procurando ganarse la confianza del cibernauta. Los principales medios que utilizan es el correo electrónico o cualquier sistema de mensajería instantánea.

El servicio que bloquea este tipo de ataques, muestra el proceso actual de protección, es decir, proyecta al administrador de red el número de paquetes que han sido bloqueados hasta la fecha, así como también los permitidos y analizados. Se explica cada uno a continuación:

- PERMITIR.- Son todos los mensajes o extensiones de archivos que han sido analizados, y dieron un resultado positivo, se los deja procesar en la red al destino final.
- DROP.- Cuando los mensajes no han sido analizados. Esto ocurre en la configuración del servicio, es decir, hay tipos de mensajes o extensiones de archivos que no se los configura para ser analizados porque son considerados como seguros, por lo tanto el tiempo de procesamiento de esos archivos se agilita.
- MARCAR.- Un mensaje se marca cuando se sospecha que éste puede causar algún tipo de daño en la red, pero en las firmas de seguridad del servicio no se tiene una que desinfecte los paquetes contaminados, por lo que se le envía luego a cuarentena.
- CUARENTENA.- Un archivo o paquete es enviado a cuarentena por dos razones. La primera es cuando no se tiene la vacuna, por así llamarlo para desinfectar a un cierto paquete, por lo que se lo envía a la central de análisis del antivirus y en la siguiente actualización de las firmas se puede desinfectar el archivo dañado. La segunda es porque a pesar de que se tenga la vacuna necesaria para desinfectar a un archivo, éste puede provocar que un proceso propio del sistema operativo quede inservible o dañado parcial o completamente, por lo que los siguientes pasos a seguir serán los mismos que en el anterior caso; es decir, se envía el archivo a cuarentena y luego a la central, para así, en la siguiente actualización desinfectarlo sin causar daño al sistema.

Seleccionando el botón de CONFIGURACIÓN, se ingresa a la siguiente pantalla.

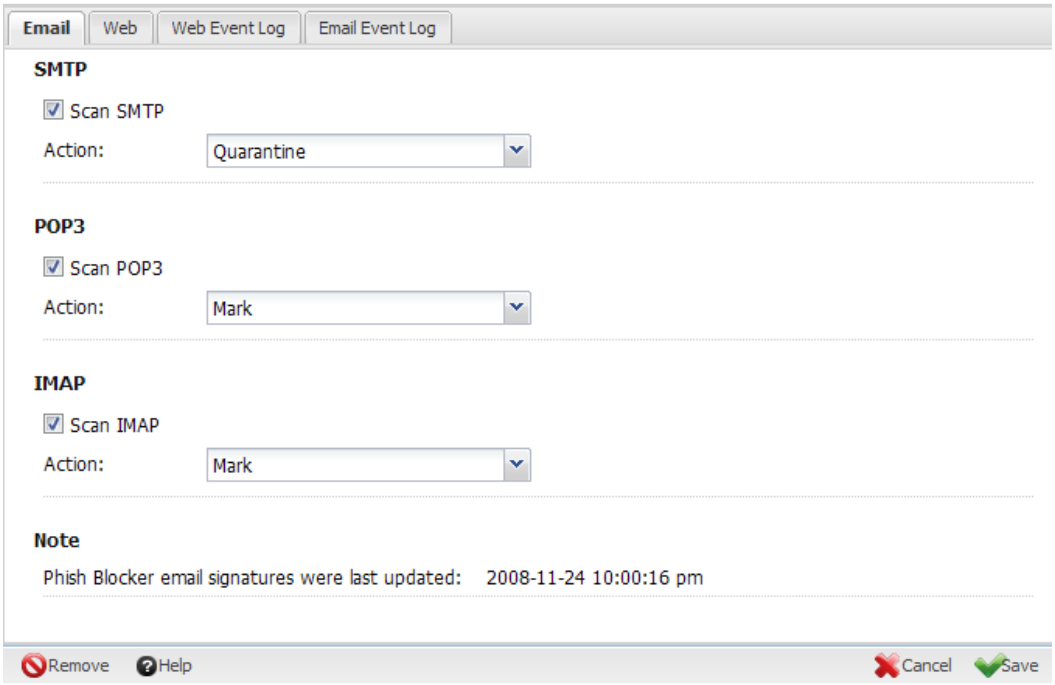

Figura4.13 Ventana de configuración des servicio ANTIPHISHING

Se toma cuarentena para el análisis de paquetes SMTP porque, como se sabe, son protocolos de transferencia de correo, mismos que en el peor de los casos, si es que se encuentran infectados, se los mantenga retenidos o continuamente analizándose hasta que, con una actualización se los pueda limpiar.

POP3 tendrá solo dos opciones, marcar o permitir. Se elegirá marcar por la misma razón que SMTP, se quiere que se analicen todos los paquetes y si es que uno está infectado, se lo marque para posterior análisis.

Marcar IMAP es muy importante, éste protocolo permite visualizar mensajes electrónicos de manera remota u obtenerlos desde cualquier servidor donde se encuentren.

r) Ahora se va a configurar el contenido WEB. La pantalla de inicio registrará los mismos parámetros que ANTIPHISHING, por lo que se saltarán esas descripciones. La ventana de configuración tiene los siguientes parámetros a determinarse en la pestaña de listas de bloqueo.

La primera opción es EDITAR CATEGORÍAS. Aquí se van a seleccionar todas los tipos de temas que no se deben abrir o mostrar al usuario.

Figura4.14 Opciones a ser filtradas

Como se puede apreciar, existen varias opciones que se pueden filtrar, entre las cuales unas ya se encuentran bloqueadas por defecto y las que se encuentran pintadas de color naranja son las que se seleccionaron para que también sean bloqueadas. En la siguiente tabla se va a mostrar las opciones que se pueden bloquean y están marcadas con una X.

Tabla4.2 Opciones que se seleccionaron para ser filtradas

FILTRADO WEB		
Categoría	Bloquear	Bandera (precaución)
Citas	■	■
Juegos de Azar	☒	☒
Agresión	☒	☒
Drogas	☒	☒
Trabajos	☒	☒
Pornografía	■	■
Sitios con Proxy	☒	☒
Compras	☒	☒
Redes Sociales	■	■
Deportes	■	■
Sin Categoría	■	■
Vacaciones	■	■
Violencia	■	■
Web Mail	■	■

Luego de aceptar y guardar los cambios hechos, se deberá configurar una siguiente opción que es la de EDITAR SITIOS. En ésta opción, hay que ingresar, si es que se tiene, las direcciones de los sitios que se presumen, con maliciosas o de contenido no apropiado para un recinto de estudio. Una vez que se han bloqueado las páginas, cuando se ingrese por ejemplo a playboy.com, aparecerá la siguiente página:

Figura4.15 Bloque de página

El siguiente botón de configuración es EDITAR TIPOS DE ARCHIVOS. Aquí se considerarán todas las extensiones de archivos que se considere, al momento de bajarse de una página web o de un servidor de mail, puedan vulnerar a la seguridad de la red. No se activó ninguno porque se considera que en una institución de estudios como una universidad, los estudiantes muchas veces requieren bajarse archivos por motivos de estudios con extensiones que pueden tener contenido vulnerable, pero no por esto se los debe bloquear necesariamente, puesto que se quedarían sin instrumentos necesarios de estudio. Las extensiones que se las puede bloquear son las siguientes: avi, bin, cab, com, cpt, dll, exe, gif, jpg, jar, mov, mp3.

También se puede bloquear por páginas específicas haciendo click en block lists y luego en Edit Sites. En la pantalla que aparece a continuación se ingresa la dirección de la página a ser bloqueada en este caso se pone como ejemplo espn.com y en descripción se pone el mensaje que salga en la página de bloque, se escribirá “dont go here”.

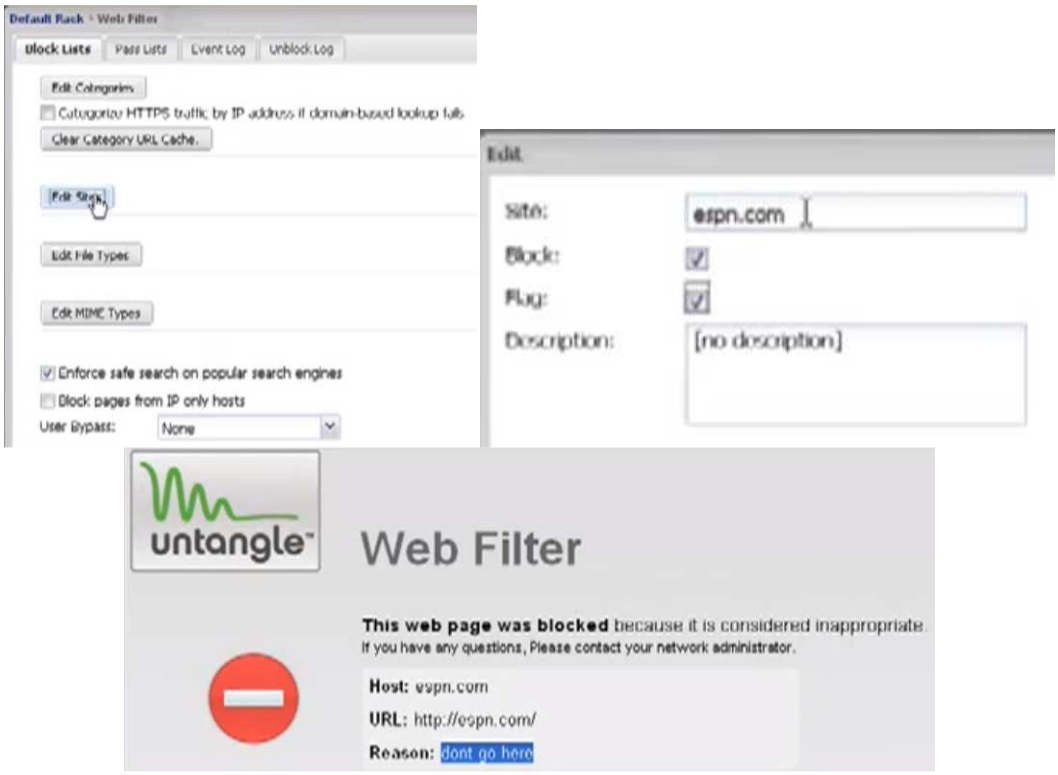

Figura4.16 Bloqueos específicos

En el reporte de este servicio, aparecerá la hora a la que se intentó acceder a un sitio prohibido, la página a la que se quiso acceder y la IP desde la que se originaron los paquetes.

Figura4.17 Reportes de eventos de WEB FILTER

s) El siguiente servicio a describirse es el de CONTROL DE PROTOCOLO. El software realiza el análisis en función de firmas que detectan los protocolos de tráfico de la red. Los puertos que se deben bloquear o a su vez analizar, se los registra dependiendo de las firmas cargadas en el software. En este servicio se analizarán y bloquearán de acuerdo a los puertos que maneje cada protocolo.

Figura4.18 Selección de protocolos a ser bloqueados

t) Finalmente se va a describir el servicio de FIREWALL. Aquí se ingresan las reglas de bloque en general o de permisos de acuerdo a direcciones IP o hosts para que accedan al internet.

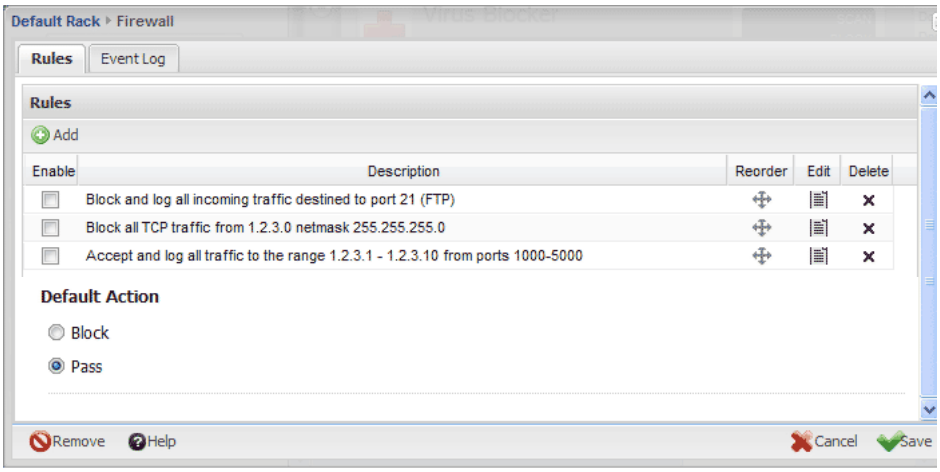

Figura4.19 Reglas de protección de Firewall

Lo que se observa en el gráfico es que todos los paquetes TCP entrantes van a ser bloqueados cuando estén destinados al puerto 21, sin embargo se la puede modificar para que o bien en lugar de que se bloquee, se permita o simplemente se analicen los paquetes que pueden ser TCP o UDP ICMP, etc., lo que en realidad va a depender de la siguiente regla creada. La segunda línea de la imagen indica un bloqueo TCP de acuerdo a la IP origen o bien a toda una red por ello se especifica la máscara. Finalmente, en este caso se establece una regla que permita o niegue todo un rango de direcciones o de hosts.

Todas estas reglas se las pueden editar o eliminar si es que se requiere o a su vez también agregar más, sin embargo se las deja como están puesto que por el momento. Más bien todas las reglas que se vayan añadiendo al servicio irán apareciendo en función del tiempo y de los problemas que se vayan detectando, es decir en función de los ataques que se vayan registrando.

4.3.1.1. Configuración de Red

Como se lo vio en el proceso de instalación del servidor, sólo se configuró una tarjeta de red puesto que era la única que se requería para la conexión a internet. En este caso se le puede dejar únicamente con esa tarjeta de red ya que UNTANGLE opera como un concentrador de tráfico, es decir, si es que tiene dos GATEWAYS de salida, basta que uno de ellos esté conectado al switch a donde se conecten los usuarios para que se analicen todos los paquetes. Se lo muestra en el siguiente gráfico:

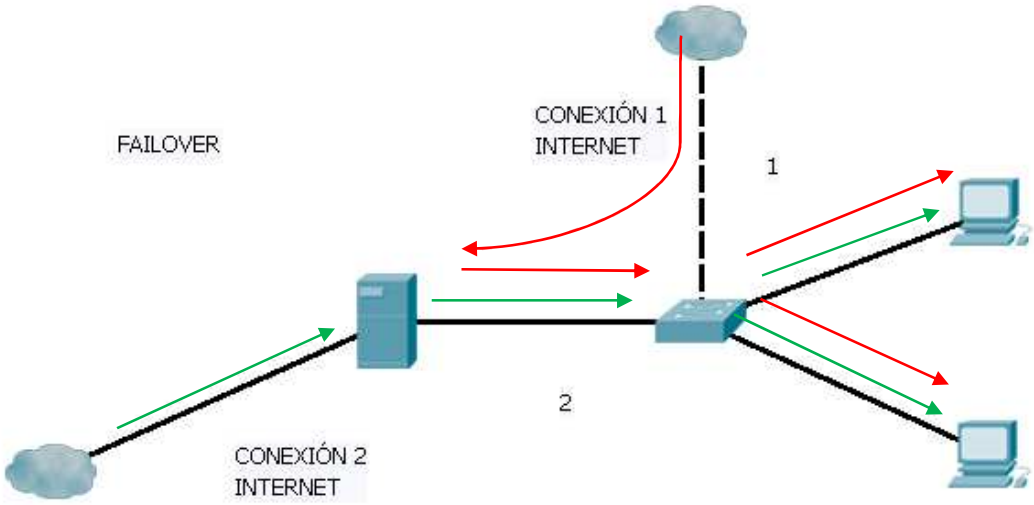

Figura4.20 Topología UNTANGLE con 1 y 2 tarjetas de red.

Se tienen dos procesos, según se puede apreciar en la figura. El proceso 1 (línea roja) que describe como puede operar este servidor con una tarjeta de red. Se tiene un comportamiento bastante simple, los paquetes que vienen del internet, ingresan

al servidor, se analizan y luego son distribuidos a la red en general, el servidor en este caso tiene una función de concentrador de tráfico. En el proceso 2 (línea verde), se tendría el mismo procedimiento pero con dos tarjetas de red en las que, la primera sigue el comportamiento del anterior proceso, si es que se configura para que también se salga al internet por ésta y la segunda es la que distribuirá los paquetes a sus respectivos destinos dependiendo de en qué VLAN se encuentren. En un caso de falla, bajo la configuración FAILOVER, todos los datos se enrutarían en una sola tarjeta de red, es decir, se tendría la configuración de concentrador de tráfico. En la siguiente figura se muestra la configuración de las dos tarjetas de red.

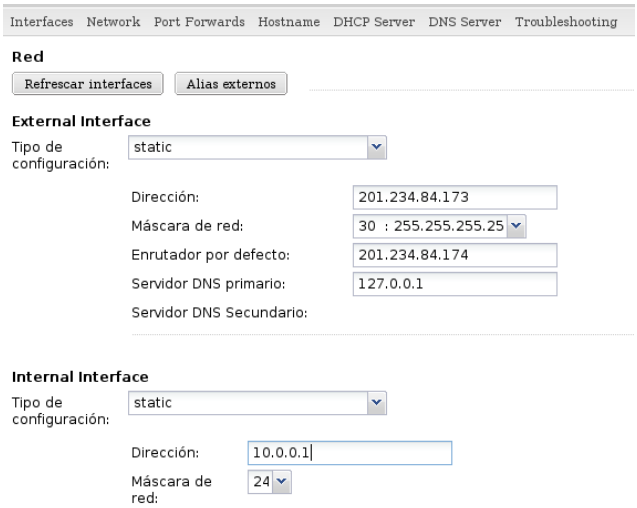

Figura4.21 Configuración de las tarjetas de red

En la interfaz interna se requiere configurar las VLANs, pero UNTAGLE UTM no dispone del protocolo 802.1Q, por lo que se requiere el bajarse un feature que permita ésta configuración pero a bajo nivel. El propósito de la instalación de éste software es el de configurar todo sobre una interfaz gráfica y en la que se pueda acceder vía HTML y desde cualquier lugar. En consecuencia, se procede a instalar el siguiente software, Zentyal UTM.

4.3.2. Zentyal UTM

Como se lo vio en el anterior apartado, el proceso de instalación de este sistema operativo tiene el mismo procedimiento que el ya visto, puesto que está construido bajo la misma plataforma Linux, cambiando la interfaz de usuario y prestaciones que ofrece, mismas que se las va a analizar paso a paso según se vaya avanzando.

Figura4.22 Logotipo de Zentyal

Luego del proceso de instalación, aparecerá la siguiente pantalla de inicio; en la que se ingresa tanto el usuario como la contraseña. En el caso de ésta implementación, la clave será: **servidorutm** y la contraseña: **espeadmin.** Cabe recalcar que la interfaz es en modelo web y el puerto de entrada al mismo es el **443.**

Figura4.23 Ingreso de claves

En la siguiente pantalla se procederá con la instalación de los servicios ya definidos como indispensables dentro de la red a protegerse, lo cual depende de la topología de la red y de lo que se requiere controlar. En este caso se instalan todos los servicios excepto VoIP. Cabe recalcar que todos los servicios que no se instalen desde un inicio o actualizaciones posteriores a éste proceso, pueden ser descargados desde la página del fabricante gratuitamente. En el gráfico se observa los íconos representativos de cada servicio, encerrados en círculos; al hacer clic en éstos, empieza la descarga. Los que fueron escogidos cambian de color.

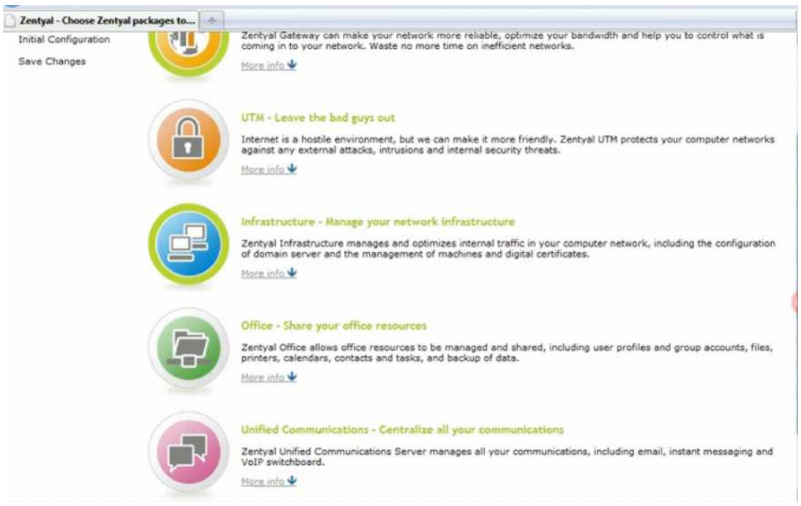

Figura4.24 Instalación de los servicios

En la siguiente pantalla aparece, como en todo servidor UTM, la configuración de red. En este caso, y con el propósito de tener acceso inicialmente sólo al internet,

se configura la IP que se observará en la siguiente imagen. Luego, cuando se implemente en la red del DEEE, las IP que están tanto en las interfaces externas como internas, se cambiarán a las que se adaptan a la topología actual y con la cual está operando actualmente la red. Se le configura como red estática teniendo así un enlace P2P con una de las salidas de de internet del DEEE.

Figura4.25 Red WAN

La siguiente pantalla es la interfaz que se muestra al usuario, en donde constan, en la parte izquierda la configuración de los servicios instalados en el servidor, en la parte central está el monitoreo de las interfaces configuradas, tanto externas, como internas (internas son las que usualmente manejan VLANs en las redes); éste monitoreo sólo será de ancho de banda consumido a tiempo real, y finalmente, en la parte derecha aparece el estado de los servicios que se encuentran tanto levantados y operando, como los que están temporal o totalmente parados. Se dice parcialmente parados a los servicios que por consumo del procesador del servidor en horarios de alta demanda, se los puede desactivar, como por ejemplo el de reportes al administrador de red.

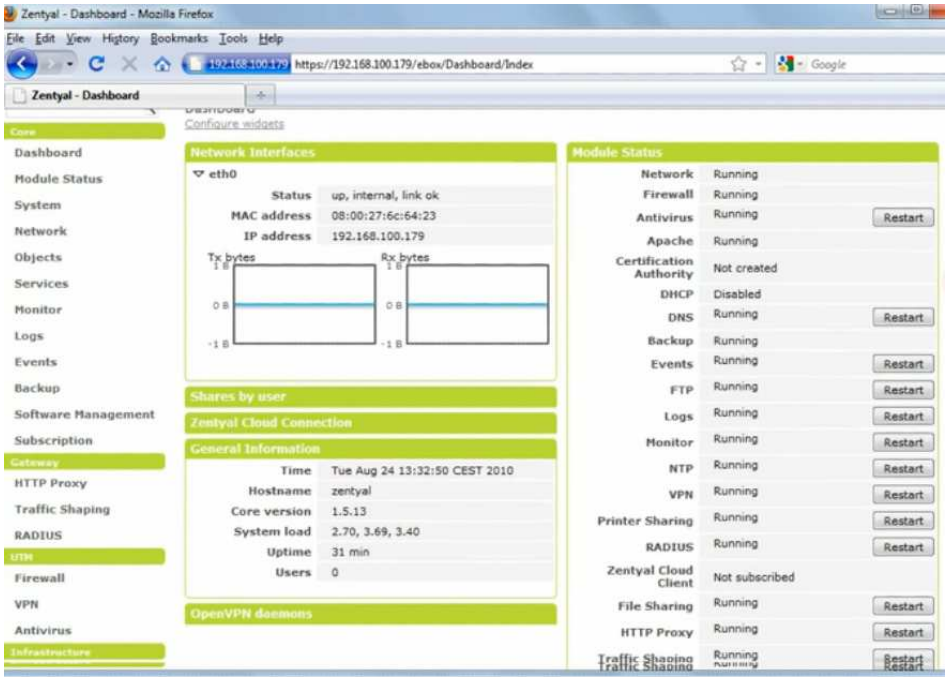

Figura4.26 Pantalla principal del servidor

Desde este momento y en adelante, como ya se tiene instalados todos los servicios, se va a proceder a configurar toda la parte de la red concerniente a la topología del DEEE, y como ya se lo vio en el capítulo 2.

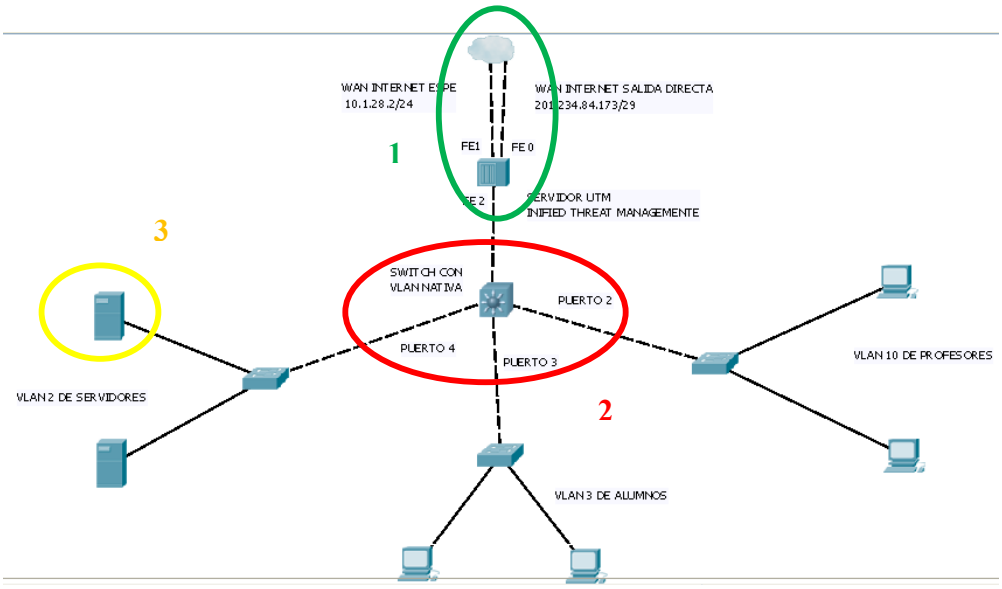

Figura4.27 Topología de la Red del DEEE

El círculo identificado como 1 es la configuración de GATEWAYS y FAILOVER. Se tienen dos interfaces establecidas como externas y ambas son Gateway de todas las redes internas de la red, ésta es una regla de configuración para que se pueda tener recuperación ante fallas o FAILOVER. Usualmente a éste término se le relaciona el concepto de tener don interfaces redundantes y una de ellas en modo standby con el propósito de que ante fallas, la una opere como back up de la otra; sin embargo, en ésta implementación se tiene a las dos interfaces operando simultáneamente y cada una con diferentes políticas, sin descuidar el que si una de las dos provoca un corte de servicio, automáticamente todo el enrutamiento pasa a ser manejado por la otra, es decir, un FAILOVER.

En el círculo identificado como 2, se describe el funcionamiento de la red interna dividida en dos partes fundamentales, la primera en la que la tercera interfaz del servidor maneja DHCP por las tres VLANs de la red, y la segunda en la que un switch capa 2 opera con una VLAN nativa y tres puertos asignados a cada VLAN

del DEEE que distribuyen los paquetes a sus respectivos usuarios. Esto se lo verá en detalle más adelante.

El círculo identificado como 3, es aquel que describe en parte cómo el servidor administrará a los usuarios; es decir, se crean reglas para cada VLAN, usuario o servidor, de tal manera que si una VLAN está saliendo por el Gateway 1, y se requiere que un usuario en particular salga por el 2, se pueda establecer la respectiva regla para éste caso en particular de acceso a internet. Por ejemplo, véase la siguiente figura:

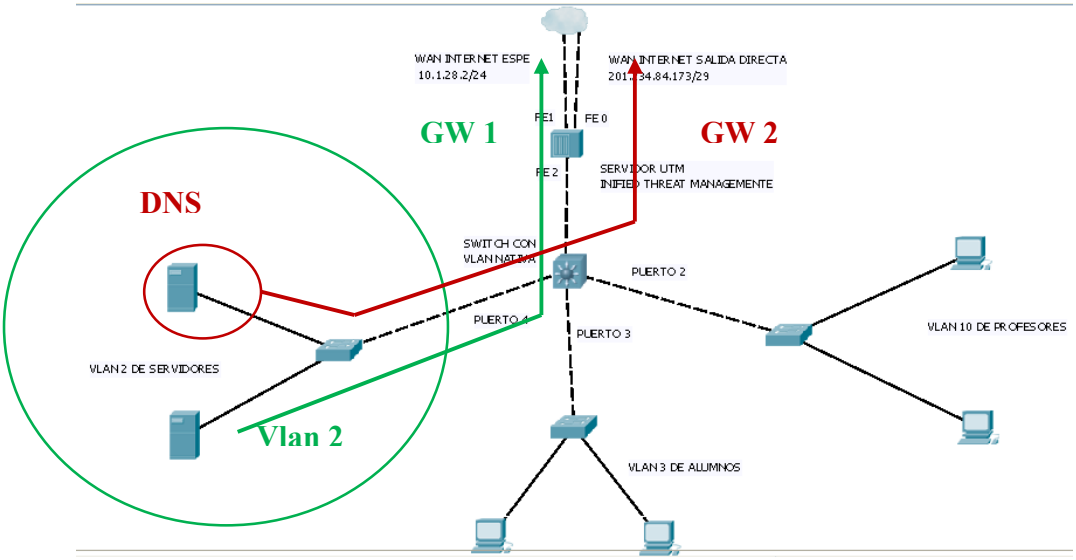

Figura4.28 Reglas de Salida a Internet

En este ejemplo se observa que toda la red de la VLAN 2 (color verde),que es la red de los servidores, tiene acceso a internet por la salida del GATEWAY 1, sin embargo, con una regla en el Firewall del UTM se logra que uno de los servidores,

el de DNS, salga por el GATEWAY 2. Esto se hace con el propósito de que ciertos usuarios tengan más velocidad o ancho de banda para tráfico IP o que a su vez tengan ciertos privilegios de navegación que las demás usuarios no lo tienen, es así que a un usuario específico se le puede permitir navegar a cualquier página de internet, mientras que los demás se regirán a las reglas de accesibilidad global, en las que destinos del tipo pornográfico o apuestas, etc., estarán bloqueados.

En la siguiente parte se procede con la configuración de la red del DEEE, iniciando con las dos interfaces externas ya definidas anteriormente como GATEWAY, y finalizando con la interfaz interna, misma que manejará 802.1Q. Ésta primera imagen es la interfaz externa que tiene una conexión directa de internet con el proveedor de la ESPE. El nombre con el que se le identificará a esta conexión es **INTERNET ESPE,** tiene una asignación estática de dirección de red, se le identifica como Externa (WAN) y la dirección, que está dentro del estudio realizado en el Capítulo 2, es la **10.1.28.2** con máscara **/24.** A esta interfaz no se le agrega ninguna VLAN.

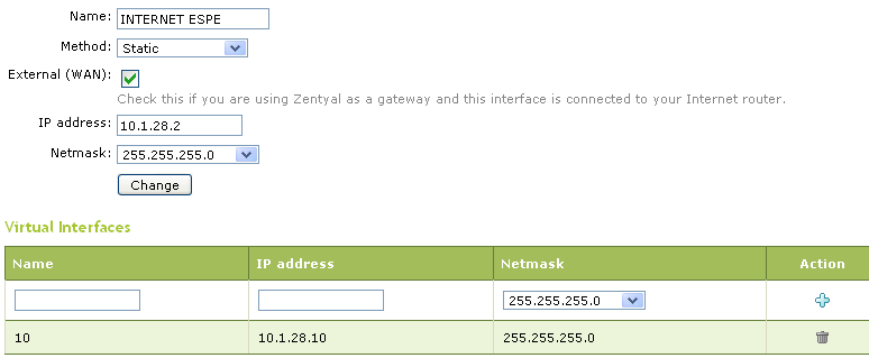

Figura4.29 Interfaz por la cual el DEEE recibe internet de la ESPE.

El siguiente paso a configurarse es la otra interfaz externa definida porque no sale a través de la conexión de la ESPE. El identificativo de ésta interfaz es **INTERNET DIRECTO,** tiene una asignación estática de dirección de red y se selecciona a ésta interfaz como Externa (WAN), y la dirección de red es la **201.234.84.173,** con una máscara **/29.**

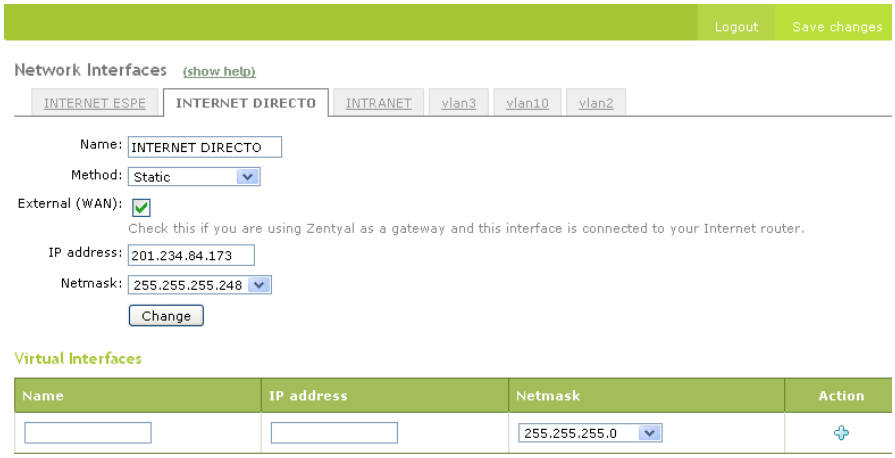

Figura4.30 Interfaz por la cual el DEEE recibe directamente de un proveedor el internet

Finalmente, la última interfaz a ser configurada es la interna, en la que se levanta el servicio de DHCP, 802.1Q y DNS. A esta red se le identifica como **RED INTERNA,** y el método de encapsulación será **Trunk 802.1Q.** Aquí es donde se le añaden las VLAN que se requiere para levantar la topología de red del DEEE. Para establecer esta configuración, en **VLAN List** se da click en el signo "+" de color azul para agregar una nueva VLAN, a continuación se activan 2 espacios en blanco a ser llenados, el primero en el que pide el identificativo de la VLAN y el segundo en el que pide el nombre que se le va a asignar y con el cual se le conocerá en el software, por lo que se agregan 3: VLAN **3 MASTERS**, **10 PROFESORES** y **2 ESTUADIANTES.** Para terminar, se da click en el botón **Enviar Datos** y luego **Guardar Datos.** Cabe recalcar que si solo se envían datos, se podrán seguir

haciendo modificaciones en el servidor y se retiene la información en la memoria virtual del mismo, mientras que cuando se da click en el botón guardar datos, el servidor se reinicia con los cambios realizados y empieza a operar con estos. Para guardar los datos en el servidor, siempre va a ser necesario primero enviar los datos al mismo. Si es que se requiere la eliminación de alguna configuración cualquiera, Zentyal tiene el ícono de un basurero y tan solo dando click en éste, el servidor la descarta.

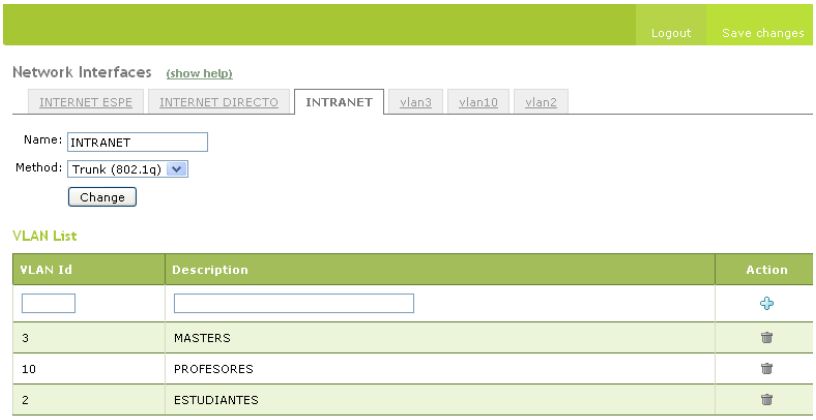

Figura4.31 Ésta es la interfaz interna, donde se configuran las VLANs del DEEE.

Se agrega primero la VLAN 3 que corresponde a los **MASTERS**. Su identificativo es **vlan3,** tiene una asignación estática de direccionamiento, la cual es **10.1.29.1** con máscara **255.255.255.0.** No se le configura como externa, puesto que como ya conocemos, todas las VLANs están en la interfaz interna. Para guardar los cambios, se da click en **Change.**

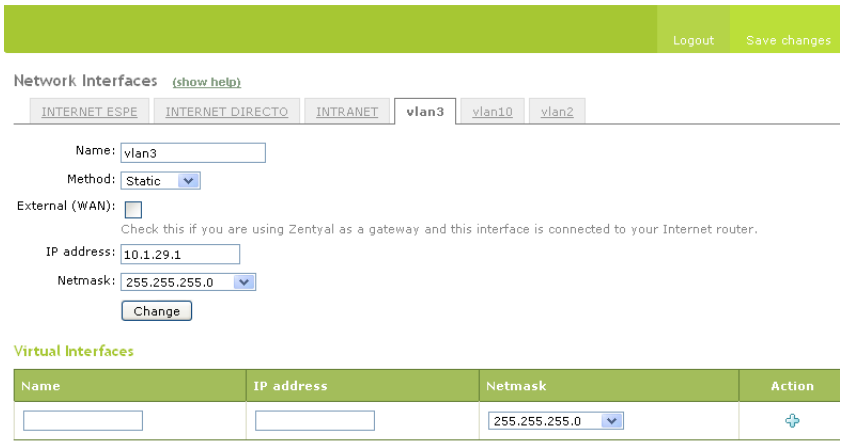

Figura4.32 Vlan de masters

La siguiente VLAN es la 10 correspondiente a **PROFESORES**. Hay que recordar que el nombre que se le asigne en esta parte de la configuración a las VLAN no es con el que se les identificará sino que solo es una asignación interna. En nombre se le configura como **vlan10.** El método de direccionamiento es estático, no es una interfaz externa y la ip: **10.10.0.1** con máscara: **255.255.255.0.**

Figura4.33 Vlan de Profesores

La última VLAN a ser asignada a la configuración de red es la 2 correspondiente a la VLAN de **ESTUDIANTES.** Prácticamente sigue el mismo patrón que las dos anteriores pero con diferente IP. En este caso la IP es: **10.1.30.1** con máscara de red: **255.255.255.0.** En ninguna de las interfaces se configuraron interfaces virtuales.

Figura4.34 Vlan de Estudiantes y laboratorios en general

Como se pudo apreciar, las dos primeras interfaces, que son la Eth0 y Eth1, son configuradas como WAN porque están conectadas directamente a las interfaces de dónde se provee el internet. Adicionalmente se requiere de la implementación de otras características, como son Failover, políticas de FIREWALL, balanceo y las dos serán GATEWAY. En la siguiente imagen se identifican a las 3 tarjetas de red y su ubicación en el servidor.

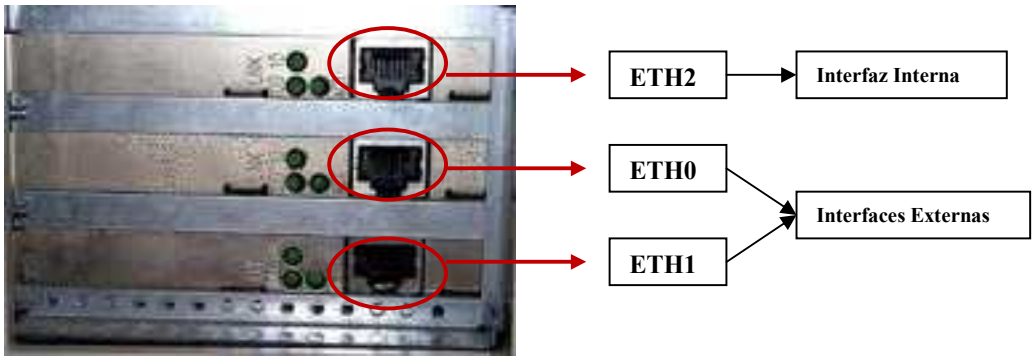

Figura4.35 Posición de las tarjetas de red

La tercera interfaz Eth2, es por la cual se va a administrar todo el tráfico LAN; es decir, es donde se implementaron las VLAN de administración del sistema, para lo cual se deberán adicionar políticas en el Firewall para que ciertos servidores de la red, y que fueron estudiados y nombrados en el capítulo 2 también, puedan salir por la WAN de la DIRECTA, ya que todas las VLANs van a salir por la WAN con la que la ESPE provee internet. Todas estas configuraciones se las verán más adelante.

En la siguiente parte se configuran los DNS que se darán a los hosts dinámicamente por la VLANs. Para añadir una dirección de DNS, se da click en el botón Añadir y se ingresa la dirección del servidor que resuelve los nombres de dominio, en el primer caso es el 200.31.6.34. Éste servidor es gratuito y lo provee el IMPSAT, se lo configura en nuestra red como back up por si el de la ESPE tiene algún problema. Luego, las direcciones de los servidores del DEEE son: **10.1.0.101** y **10.1.0.104.** A la derecha de cada servidor se encuentran unas flechas de color azul apuntando para arriba o abajo, esto es porque se pueden ordenar los servidores por prioridad, siendo el mayor el que se encuentra primero. El nombre del dominio es **espe.edu.ec.**

Figura4.36 Direcciones DNS

Como se dijo anteriormente, y para que el servidor tenga dos interfaces WAN y que una de ellas actúe como back up, se debe configurar las dos direcciones IP como GATEWAY, para luego poder establecer políticas en el FIREWALL tanto para los hosts como para los servidores, con el propósito de facilitar el direccionamiento de hosts, servidores o VLANs por cualquiera de los dos GATEWAYS. Primero se da click en el botón añadir nuevo y se ingresa los datos de cada interfaz. Para la interfaz ETH0 se da el nombre a proveedor al que está conectado, **INTERNET ESPE,** la dirección de red, **10.1.28.1** y en weight se le da el peso que quiere que tenga, es decir la prioridad o importancia en la red, a ésta dirección se le da un peso de 10, pues es la interfaz por donde saldrá la mayor cantidad de usuarios, en consecuencia será la salida **Default**. Para la interfaz ETH1, el nombre será **INTERNET DIRECTO,** la dirección de red con la que fue configurada, **201.234.84.169** y tendrá un peso de 5. A las dos interfaces se les habilita el visto en la casilla de **ENABLED,** pues las dos estarán en operación.

En esta parte también se puede configurar un password y una clave para las conexiones WAN que requieran de un proxy, es decir para que se pueda establecer la comunicación con el servidor se requiere de un ingreso restringido, esto por medidas de seguridad. En el caso de la red del DEEE no se configuran estas opciones.

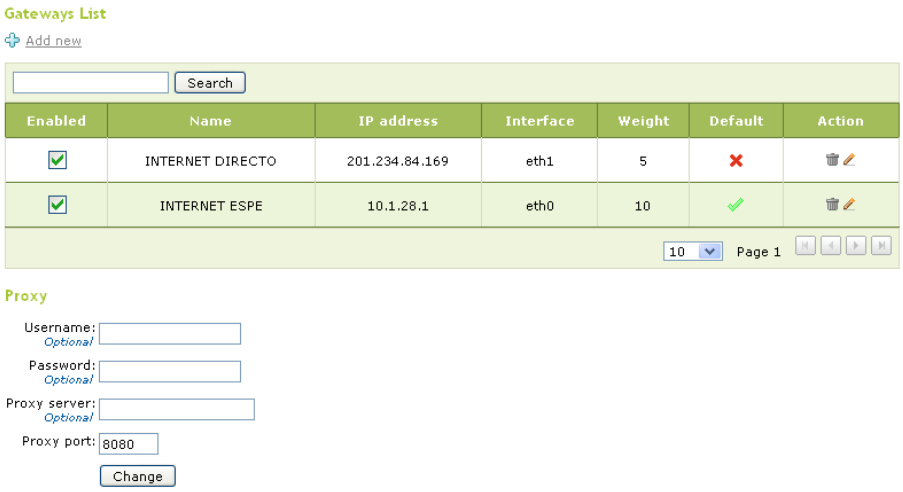

Figura4.37 Configuración de las Puertas de Enlace Predeterminadas

En la siguiente figura se muestra la **política de balanceo** utilizada, en la cual a todas las interfaces apuntan a la WAN del internet de la ESPE, mientras que la VLAN de profesores por el proveedor que contrata el DEEE. Para esto primero se habilita el visto en **Traffic Balancing.** Luego se da click en añadir nuevo, se pone la interfaz a ser configurada, luego la dirección origen, a donde los paquetes van dirigidos, el servicio o tipo de paquetes que se transmite y el GATEWAY por dónde saldrán. Asimismo con las flechas de la derecha, se elegirá la prioridad de la regla. Por ejemplo, inicialmente se requiere que todas las VLANs salgan por el **INTERNET DIRECTO,** sin embargo, sólo la VLAN2 se quiere que salga por el **INTERNET ESPE.** Gráficamente se tiene lo siguiente:

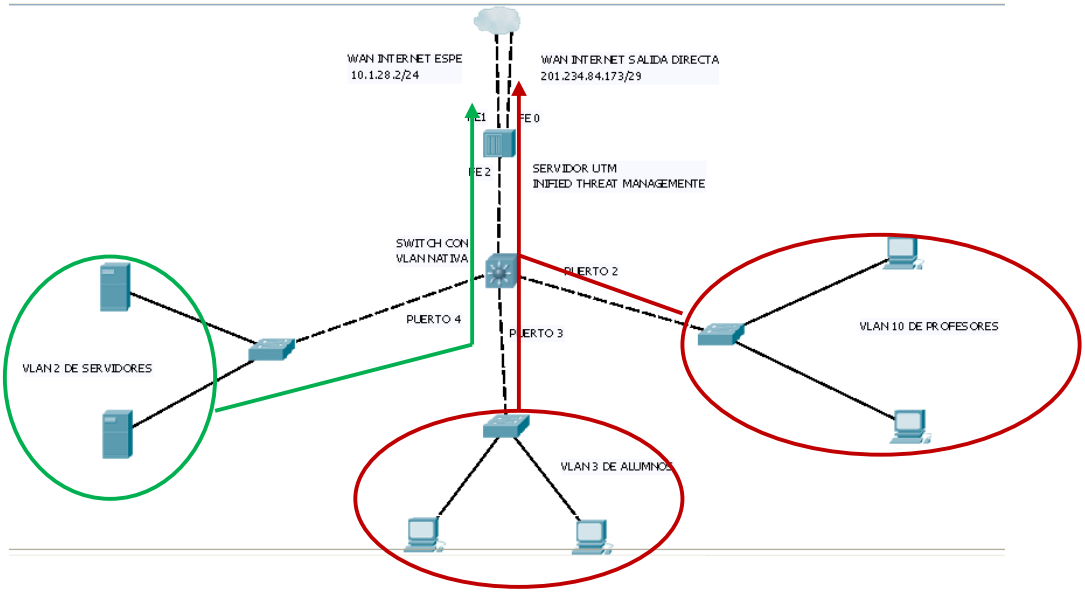

Figura4.38 Política de Balanceo para VLAN2

Como se puede observar en la gráfica anterior mediante las reglas que se muestran en la siguiente figura, en la que se ingresa en interfaz **VLAN2,** source **ANY,** destination **ANY,** y service **ANY,** para las tres VLANs se tiene que sin importar el destino de los paquetes o de que tipo son, ni a dónde se dirigen van a salir: la VLAN2 por el INTERNET ESPE y las VLANs 3 y 10 por el INTERNET DIRECTO, según la gráfica que se muestra a continuación:

Figura4.39 Políticas de balanceo de tráfico

Para la configuración de **FAILOVER,** primero se configura el tiempo con el que se va a comprobar que las dos interfaces estén operando y sin errores, en este caso se establece que 30 segundos es un periodo prudencial para que una interfaz no deje por mucho tiempo en caso de falla sin servicio a los usuarios ni tampoco como para que se le recargue al servidor mucho procesamiento revisando todo el tiempo la operatividad normal de las interfaces. Luego se configuran las reglas de testing. La primera es la que le corresponde al INTERNET DIRECTO, y el tipo de test con el que se comprobará que la interfaz está arriba es mediante 6 pings a la misma, número que se configura en la casilla de **Number of probes** y para ésta se requiere que el ping tenga un éxito del 60%, es decir que no necesita que la interfaz esté totalmente caída como para que se la dé de baja. Para la segunda interfaz, que es la INTERNET ESPE, se configura lo mismo a excepción del éxito de pings efectivos, que en éste caso se lo establece en 40%, pues es la de mayor importancia y la que tiene mayor cantidad de usuarios.

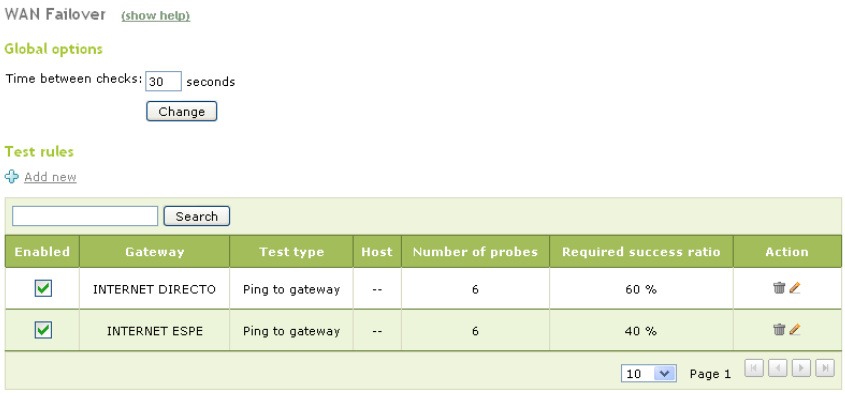

Figura4.40 Interfaz Sobre Fallos

Para que todas las anteriores configuraciones surtan efecto se requiere de la creación en el FIREWALL de la regla que permita que los hosts de la VLAN2 salgan por la salida directa al internet y los de las VLAN10 y 3 por el internet de la ESPE. La primera regla que se muestra en la figura fue creada para el host con la IP 10.10.0.2 con el propósito de que también salga por el INTERNET ESPE 10.1.28.10. Se hace click en Add new, luego se ingresa la IP origen, en este caso la del host que está dentro de la VLAN10 **10.10.0.2/30,** no importa el puerto al que va dirigido el paquete, se elige **any,** así como tampoco interesa el protocolo utilizado ni el origen del mismo, por lo que también se elige **any;** finalmente se ingresa la dirección IP del destino que es la del GATEWAYE INTERNET DIRECTO **10.1.28.10. A**dicionalmente se habilita la regla con el visto en **LOG.**

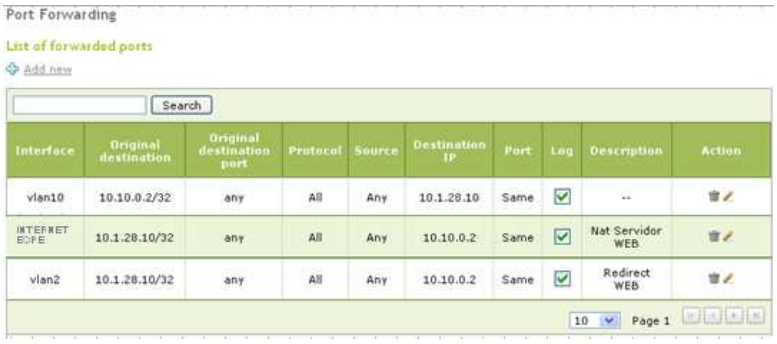

Figura4.41 Regla del Firewall

Como se pudo observar a lo largo de todo el capítulo, los dos servidores tienen muy buenas prestaciones e interfaz con el usuario, pero ZENTYAL UTM, cumplió con todos los requisitos establecidos inicialmente para levantar el servidor.

El principal inconveniente que presentó UNTANGLE UTM fue que para la configuración de red, específicamente refiriéndose a las VLAN se requiere de la actualización de la plataforma LINUX y así poder establecer la topología lógica en una interfaz a bajo nivel, es decir por línea de comandos, aspecto que se sale de los objetivos especificados en el inicio de este proyecto, el de tener la administración total del software sobre una interfaz gráfica amigable con el usuario.

Zentyal UTM permite la implementación de 802.1Q sobre interfaz configurada en la red, es decir, por cada red añadida a la red, sea ésta asignada a una interfaz física directamente o a su vez encapsulada dentro de una interfaz lógica, aspecto que tampoco tenía el otro software, ya que únicamente permitía una sola asignación DHCP a una sola interfaz.

Hablando en cuanto a la administración en general y a los reportes que se generan diariamente para el administrador de red, UNTANGLE y ZENTYAL son muy buenos y detallan todo el tipo de tráfico que pasa por la red, así como todos los posibles ataques que fueron bloqueados. Toda esta información se configura para

que sólo un usuario tenga acceso, ya sea configurando el servidor como para que ésta sea enviada al mail o ingresando al software directamente. En general, según varias características de Zentyal adicionales a las que soporta Untangle es que se definió por éste software para ser implementado en la red del DEEE. Se las detalla en la siguiente tabla:

Tabla4.3 Tabla Comparativa Entre los dos UTM

Tabla Comparativa entre Zentyal y Untangle		
CARACTERÍSTICA	UNTANGLE	ZENTYAL
Filtrado WEB	Sí	Sí
Control de Puertos	Sí	Sí
Interfaz Gráfica Amigable	Sí	Sí
802.1Q	**No**	Sí
MultiWAN	Sí	Sí
DHCP	Sí	Sí
DHCP por interfaz	**No**	Sí
DNS Server	**No**	Sí
Firewall	Sí	Sí
Antivirus	Sí	Sí
Antispam	Sí	Sí
Antiphishing	Sí	Sí
Control de Contenidos	Sí	Sí
Control de Usuarios	Sí	Sí
MultiGateway	Sí	Sí
Control de Intrusos	Sí	Sí
Proxy	Sí	Sí

CAPÍTULO V

PRUEBAS DE OPERACIÓN, CONCLUSIONES Y RECOMENDACIONES

5.1. PRUEBAS DE OPERACIÓN

En este capítulo se realizan dos tipos de pruebas, la primera en la que se observa el desempeño en sí del servidor en funcionamiento, es decir, la capacidad del procesador en uso, cuánta memoria requiere para funcionar en condiciones normales y uso de las tarjetas de red. La segunda parte de las pruebas tiene que ver con las políticas de enrutamiento definidas para las distintas redes LAN virtuales creadas.

5.1.1. Software y Hardware

Una de las características principales de este servidor es la baja capacidad de procesamiento a nivel de servicios y espacio en disco que ocupa, lo que se ve contrastado con la sucesiva ocupación que por motivo de reportes generados se va incrementando (se observa en Anexos), es así que en la figura 5.1 se observa que consume apenas el 1.47% de un total de 144212.47 Mb.

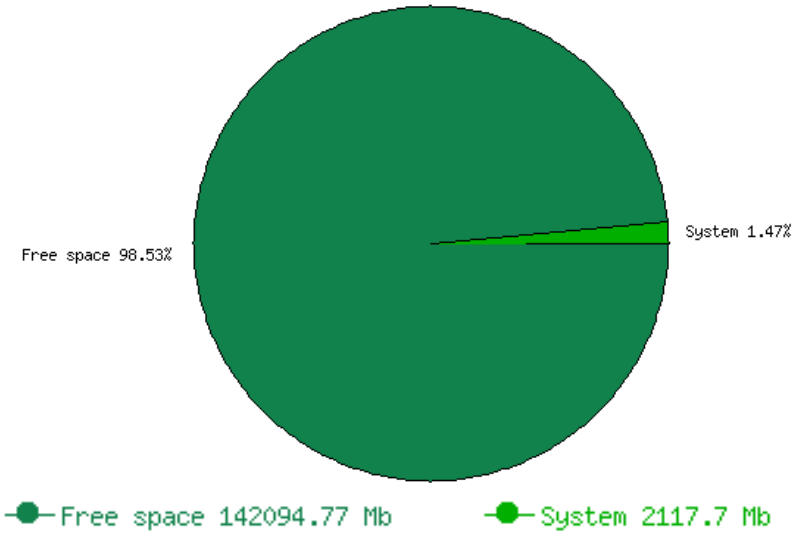

Figura5.1 Capacidad de Memoria Utilizada por Zentyal

En cuanto a memoria RAM consumida, tiene en el siguiente gráfico que consume en una medición tomada cualquiera el 7.04% de los 256 Mb totales.

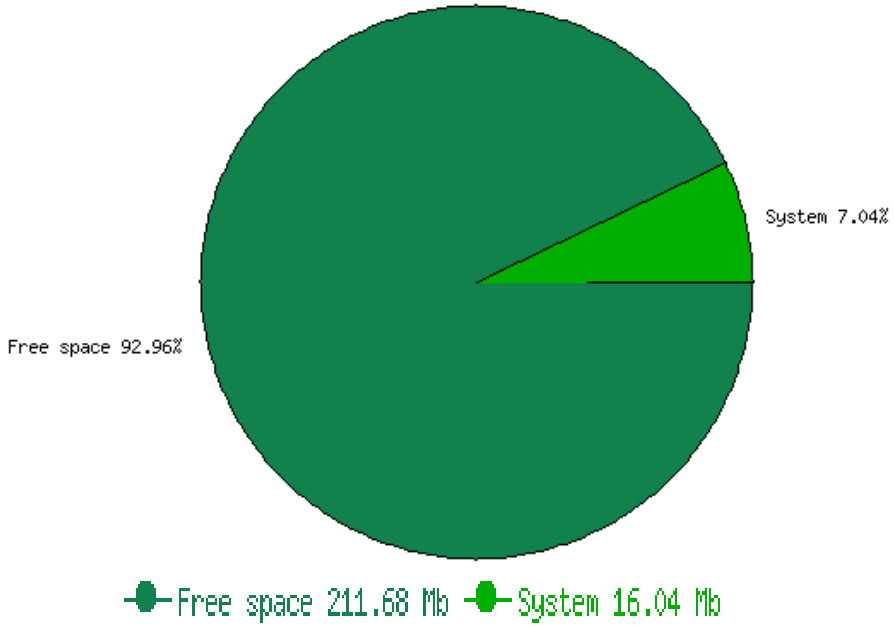

Figura5.2 Memoria RAN consumida del servidor

Para comprobar el funcionamiento de las interfaces de red, se tiene en la pantalla principal del servidor unos cuadros donde se verifica el estado de las interfaces juntamente con las gráficas de consumo en Bytes, mismos que son inexactos y más bien sirven como referencia de funcionamiento ya que no se trata de un software de medición de tráfico especializado como un PRTG o MRTG que se utilizan bastante en el mercado. En los gráficos que se muestran a continuación, en a, b, c están las interfaces configuradas junto con las gráficas respectivas de cada una y su estado; mientras que en la gráfica d están los usuarios que se encuentran conectados a la red en un momento cualquiera dado.

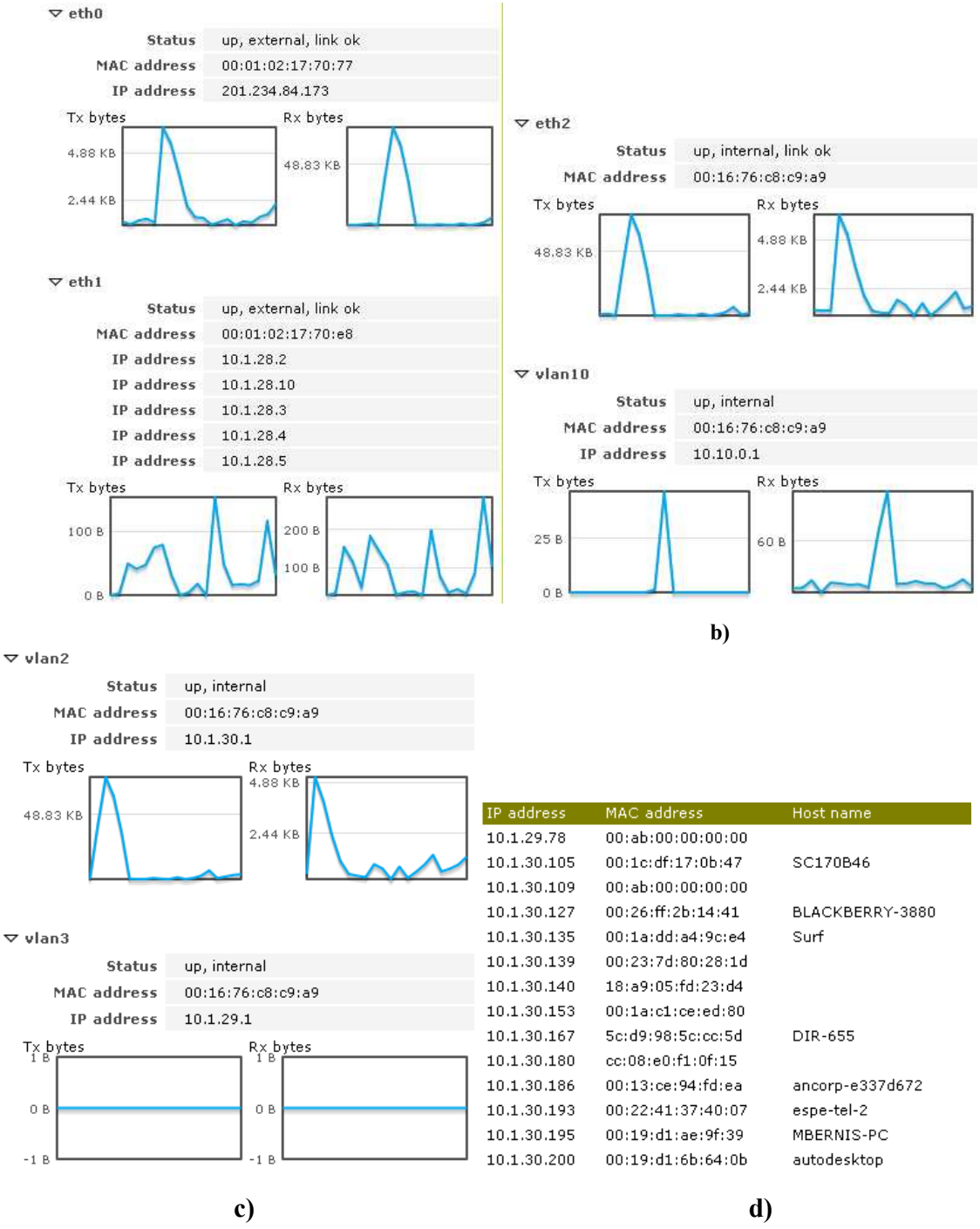

Figura5.3 a) Estado interfaces Eth0 y Eth1 b) Estado interfaces Eth2 y VLAN 10 c) Estado interfaces VLAN2 y VLAN 3 d) Usuarios conectados a la red

5.1.2. Pruebas de Red

Las pruebas a realizarse demuestran el papel del UTM en la parte de enrutamiento, es así que en la imagen 5.4 se describe cómo un host cualquiera perteneciente a la VLAN de ALUMNOS que pertenece a la red 10.1.30.0/24 sale por el GATEWAY 2. Se observa que sale por la 201.234.84.169 en el tercer salto, y a partir del sexto salto ya está en la nube de internet.

Traza a la dirección www.1.google.com [209.85.195.104] sobre un máximo de 30 saltos:

1	<1ms	<1ms	<1ms	DD-WRT [192.168.1.1]
2	1ms	<1ms	<1ms	10.1.30.1
3	7ms	5ms	7ms	201.234.84.169
4	6ms	5ms	5ms	190.216.223.81
5	57ms	59ms	63ms	ge4-1-10G.ar3.SCL1.gblx.net [67.17.106.18]
6	57ms	57ms	58ms	72.14.216.105
7	58ms	60ms	55ms	209.239.240.138
8	76ms	85ms	78ms	216.239.43.87
9	94ms	87ms	90ms	209.85.251.6
10	78ms	80ms	80ms	eze03s01-in-f104.1e100.net [209.85.195.104]

Traza Completa.

Figura5.4 Tracer desde un host de la VLAN de ALUMNOS hacia www.google.com

En la siguiente figura, se observa el servidor DNS en funcionamiento, que corresponde a la IP 10.1.0.101. Se toma como ejemplo la dirección www.yahoo.com, se observa que se resuelve el dominio con 5 direcciones diferentes, esto es porque debe tener 5 servidores en la región.

```
; <<>> DiG 9.7.0-P1 <<>> +time=3 yahoo.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10945
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 7, ADDITIONAL: 2

;; QUESTION SECTION:
;yahoo.com.                     IN      A

;; ANSWER SECTION:
yahoo.com.              369     IN      A       72.30.2.43
yahoo.com.              369     IN      A       98.137.149.56
yahoo.com.              369     IN      A       98.139.180.149
yahoo.com.              369     IN      A       209.191.122.70
yahoo.com.              369     IN      A       67.195.160.76

;; AUTHORITY SECTION:
yahoo.com.              172037  IN      NS      ns6.yahoo.com.
yahoo.com.              172037  IN      NS      ns8.yahoo.com.
yahoo.com.              172037  IN      NS      ns1.yahoo.com.
yahoo.com.              172037  IN      NS      ns2.yahoo.com.
yahoo.com.              172037  IN      NS      ns3.yahoo.com.
yahoo.com.              172037  IN      NS      ns4.yahoo.com.
yahoo.com.              172037  IN      NS      ns5.yahoo.com.

;; ADDITIONAL SECTION:
ns6.yahoo.com.          134678  IN      A       202.43.223.170
ns8.yahoo.com.          134678  IN      A       202.165.104.22

;; Query time: 1 msec
;; SERVER: 10.1.0.101#53(10.1.0.101)
;; WHEN: Fri Oct 21 22:30:29 2011
;; MSG SIZE  rcvd: 265
```

Figura5.5 Servidor DNS

En la figura 5.6 se probará el bloqueo a la página de internet: www.viendosexo.com, agregada en las políticas de filtrado web en el módulo de PROXY. La prueba se la hizo directamente desde el servidor con un trace, el resultado: no se puede acceder.

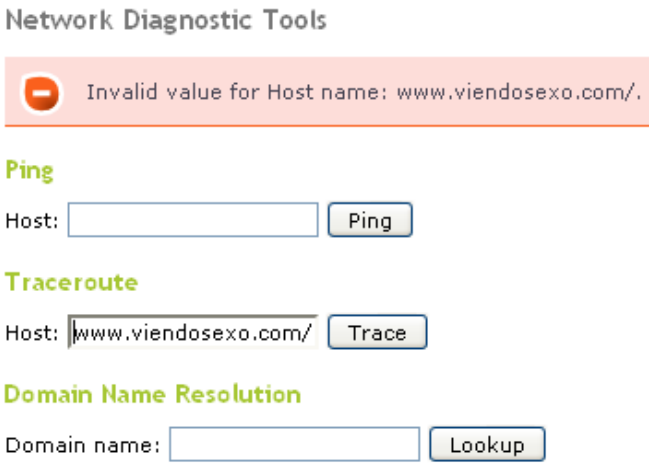

Figura5.6 Filtrado WEB al destino www.viendosexo.com

5.2. CONCLUSIONES

5.2.1. Se logró implementar en el Departamento de Eléctrica y Electrónica un servidor UTM (Unified Threat Management) que dote de seguridad y protección contra amenazas.

5.2.2. De acuerdo a la fundamentación teórica analizada se logró determinar que el mecanismo más óptimo y robusto para proteger a la red del Departamento es el software Zentyal UTM, mismo que cuenta con políticas de administración de usuarios, ancho de banda, balanceo de carga, DHCP y DNS.

5.2.3. Los laboratorios de Electrónica y Redes se encuentra segmentado en redes definidas por 3 VLANs: Profesores, Estudiantes y Masters y se ha precisado el nivel de protección a las tres redes por igual, diferenciándose únicamente por el bloqueo de ciertos tipos de usuarios a páginas que puedan vulnerar la red del DEEE.

5.2.4. Se adaptó el servidor ZENTYAL UTM a la red del DEEE, comprobando que el direccionamiento en cada interfaz sea el correcto, de tal manera que dos interfaces sean GATEWAY para la salida a internet por dos proveedores distintos y que tengan configurado FAILOVER (recuperación ante fallos), y la tercera interfaz que administre las redes LAN del Departamento y en donde se analiza balanceo de carga, accesibilidad, políticas de direccionamiento en el FIREWALL y filtrado WEB.

5.2.5. Los hosts del a VLAN de ESTUDIANTES son enrutados exitosamente por la salida a internet que pasa por el departamento de Tecnologías de Información y Comunicaciones de la ESPE, mientras que los miembros de la VLAN de PROFESORES sale directamente a internet.

5.2.6. Una vez creadas las restricciones de acceso a ciertas páginas de internet para los estudiantes, las pruebas de ping muestran que ya no llegan al destino, es decir, se quedan en el primer salto, que es el servidor UTM.

5.2.7. Debido a que en el servidor se tiene levantado puertos GIGA tanto hacia las salidas a internet como a la parte LAN, no existen colas de paquetes o paquetes descartados en ninguno de los puertos.

5.3. RECOMENDACIONES

5.3.1. Se recomienda la adquisición de la versión pagada de ZENTYAL UTM puesto que es donde se encuentran todos los appliances además de que se cuenta con el soporte del fabricante ante cualquier eventualidad.

5.3.2. Actualmente el servidor UTM levantado tiene una exigencia de procesamiento mínima, y si es que en el futuro la demanda requiere más permisos de acceso, control de protocolos, QoS y políticas en el FIREWALL, se deberá analizar también un incremento de la capacidad del procesador del servidor.

5.3.3. Con el propósito de garantizar disponibilidad, se deberá también analizar el levantamiento de un segundo servidor de back up que reemplace al actual en caso de falla, que puede ser en hardware o software.

REFERENCIA BIBLIOGRÁFICA

1. **Cristian Palacios, Andrea Albán**, "DISEÑO E IMPLEMENTACIÓN DE UNA HONEYNET PARA LA RED DEL DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA (DEEE) UTILIZANDO VIRTUALIZACIÓN", Capítulo II, Escuela Politécnica del Ejército, 2011.

2. **Joel Snyder, Opus One**, "EVALUATING UNIFIED THREAT MANAGEMENT PRODUCTS FOR ENTERPRISE NETWORKS", QuarkXPress™, Agosto 2006.

3. **WatchGuard Technologies; Inc.**, "ZERO DAY PROTECTION", Septiembre 2006.

4. **Villalón Huerta, Antonio**, "SEGURIDAD EN UNIX Y REDES", Versión 2.1, Julio 2002.

5. **eBox TECHNOLOGIES S.L.**, "ZENTYAL 2.2 OFFICIAL DOCUMENTATION", http://doc.zentyal.org/en/, 2004 – 2011.

6. **Marc Catalaa, Jean**, "GUIA DE DIMENSIONAMIENTO FIREWALL/UTM", SONICWALL, Manager, Southern Cone, jmcatalaa@sonicwall.com, Abril 2010.

7. **Endian Headquarters,** "ENDIAN UTM SOFTWARE", Octubre 2009.

8. http://www.smallnetbuilder.com/lanwan/lanwan-reviews/30539-a-powerful-open-source-utm-untangle-gateway-reviewed?showall=&start=1.

9. http://www.clearfoundation.com/docs/user_guide/5.0.