Universidad de Matanzas

Facultad de Ciencias Técnicas

Departamento de Informática

“Propuesta de Implementación del Sistema de Navegación para la Red de Datos de la Universidad de Matanzas.”

Trabajo de Diploma en opción al Título de Ingeniero Informático.

Autor: *Alain Viera González.*

Tutor: *Ángel Luis Zuriarraín Sosa.*

Matanzas, Cuba. Junio 2018.

Declaración de autoría

Yo, Alain Viera González, declaro que soy el único autor de este trabajo, y autorizo a la Universidad de Matanzas, que hagan el uso que estimen pertinente de él. Y para que así conste, firmo la presente a los 14 días del mes de junio del 2018.

Firma del Autor

Firma del Tutor

Opinión del usuario

El Trabajo de Diploma titulado “Propuesta de Implementación del Sistema de Navegación para la Red de Datos de la Universidad de Matanzas.”, fue realizado en el Departamento de Redes de la Universidad de Matanzas. Este centro considera que, en correspondencia con los objetivos trazados, el trabajo realizado le satisface:

_X_ Totalmente

El sistema confeccionado basado en tecnología de Software Libre y código abierto, cumple los requisitos y objetivos trazados durante su planificación con muy buena calidad. Actualmente se encuentra ubicado en el Nodo Central de la Universidad de Matanzas en espera de su aprobación. El estudiante y trabajador Alain Viera González se ha desempeñado de manera independiente y creativa no solo en el campo del análisis y diseño del sistema, sino también investigando las tecnologías de telecomunicaciones y electrónica que favorecen el desempeño de su solución. Ha llegado a un resultado que lo hace aumentar su nivel profesional por ser su primer gran aporte a la práctica social. Y para que así conste, se firma la presente a los 14 días del mes de junio del 2018

Y para que así conste, se firma la presente a los 14 días del mes de junio del año 2018.

Representante de la entidad.	Cargo.
Firma.	Cuño.

Opinión del tutor

DATOS PERSONALES DEL TUTOR

Nombre y apellidos: Ángel Luis Zuriarraín Sosa

Centro de trabajo: Dirección de Informatización, Universidad de Matanzas “Camilo Cienfuegos”

Organismo al que pertenece: Ministerio de Educación Superior, MES.

Especialidad de la que es graduado: Ingeniería en Telecomunicaciones y Electrónica, Facultad Ingeniería Eléctrica, CUJAE, La Habana, 2011.

Categoría docente o investigativa: Profesor Asistente

DATOS DE LA TESIS Y EL DIPLOMANTE

Nombre y apellidos: Alain Viera González

Título de la Tesis: PROPUESTA DE IMPLEMENTACION DEl SISTEMA DE NAVEGACION PARA LA RED DE DATOS DE LA UNIVERSIDAD DE MATANZAS.

OPINIÓN SOBRE EL TRABAJO:

El diseño y la implementación de un sistema de navegación que gestione el tráfico de una universidad constituye un verdadero reto, al cual se le debe dedicar innumerables horas de estudio y preparación. Nuestro centro universitario abarca la totalidad de la Provincia de Matanzas a través de las sedes universitarias y recientemente incluyó una sede muy importante en cuanto a usuarios y servicios: la sede pedagógica Juan Marinello. Es válido destacar que el sistema implementado manipula todo el tráfico interno y externo que utiliza diferentes medios y tecnologías: Fibra Óptica, WIFI, ADSL y Ethernet, cada uno presentando diferentes características en cuanto a velocidad de unidad informativa máxima, retardo y ruido.

La tesis titulada: “Propuesta de implementación de un sistema de navegación para la red de datos de la Universidad de Matanzas” presentada por el estudiante Alain Viera González, en opción al título de Ingeniería Informática, desarrollada en la Dirección de Informatización de la Universidad de Matanzas, intenta resolver una problemática de gran actualidad, pues busca solucionar un problema de primer orden para el país, inmerso en la aplicación de las nuevas Políticas de Informatización de la sociedad cubana

El tutor de este trabajo de diploma considera que, durante su ejecución, el estudiante mostró las cualidades que a continuación se detallan: una absoluta independencia en el desarrollo de su trabajo. Tenacidad y espíritu de investigación, incursionando en una temática de gran complejidad que exige del conocimiento no sólo del área informática, sino de varias especialidades vinculadas a las telecomunicaciones y la electrónica. A pesar de esto, logró captar con rapidez y profesionalidad el conocimiento necesario para enfrentar el problema planteado. Logró ofrecer soluciones importantes que permite apreciar la profesionalidad que ha alcanzado como investigador.

En el trabajo se aprecia profesionalidad, manifestado desde el tratamiento de los conceptos estudiados y referenciados en la bibliografía, hasta las conclusiones a las que arribó, lo que ha contribuido en gran medida a la solución de los problemas enfrentados. Ha dejado planteado importantes elementos a tener en consideración en futuras investigaciones.

Las conclusiones están correctamente estructuradas y en concordancia con los objetivos a lograr. El trabajo cumple con los objetivos propuestos, aborda una temática de gran actualidad y rigor científico.

La solución propuesta es de gran importancia para la Universidad de Matanzas, el Ministerio de Educación Superior y nuestro País, pues contribuye a la aplicación directa de las políticas en cuanto al uso de los recursos informáticos con que se cuenta. El sistema de navegación presentado se encuentra en espera de su aprobación por la máxima dirección de nuestro centro para ser implementado.

Por todo lo anteriormente señalado, considero que el estudiante, Alain Viera González, reúne los requisitos para el título de Ingeniera Informática y espero le sea otorgada la máxima calificación que confiere este Tribunal.

Ángel Luis Zuriarraín Sosa
Ing. Telecomunicaciones y Electrónica
Director de Informatización de la Universidad de Matanzas

Resumen

En los últimos 5 años nuestro país ha sufrido grandes cambios en las tecnologías de Redes y Telecomunicaciones, esto ha traído consigo un impulso en términos de informatización tanto de la sociedad, como de las empresas e instituciones. La Universidad de Matanzas como unos de los principales centros de formación de profesionales necesita ir a la par con los procesos de informáticos del país, abarcando la infraestructura de la Red de Datos y sus servicios brindados. Este proyecto de investigación pretende, partiendo del análisis del funcionamiento del sistema de navegación de la Universidad Matanzas, proponer la implementación de un sistema eficaz acorde a nuestros tiempos. Se pretende obtener un grupo de parámetros que se utilizaran en la instalación y configuración de un *Proxy de Navegación*, capaz de gestionar y monitorear los recursos brindados a los usuarios, así como encauzar correctamente nuestro tráfico de red, apoyándose en un uso de ancho de banda eficiente, un sistema de monitoreo en tiempo real, una *caché* de navegación óptima y en la información de sistemas estadísticos aplicados en el estudio de logs recopilados en los últimos dos años. Siguiendo las orientaciones de nuestro país en términos de política de informatización se propone la realización de un sistema basado en software libre y de código abierto, utilizándose experiencias previas experimentadas en otros centros pertenecientes al Ministerio de Educación Superior.

Summary

In the last 5 years our country has undergone great changes in the technologies of Networks and Telecommunications, this has brought with it an impulse in terms of computerization of society, as well as of companies and institutions. The University of Matanzas, as one of the main centers for the training of professionals, needs to go hand in hand with the computerization processes of the country, starting with the infrastructure of the Data Network and its services provided. This research project intends, starting from the analysis of the operation of the navigation system of the Matanzas University, to propose the implementation of a more efficient system according to our times. It is intended to obtain a group of parameters that will be used in the installation and configuration of a Navigation Proxy, capable of managing and monitoring the resources provided to users, as well as correctly channeling our network traffic, based on a bandwidth use, efficient, a real-time monitoring system, an optimal navigation caché and the information of statistical systems applied in the study of logs compiled in the last two years. Following the guidelines of our country in terms of computerization policy is proposed the realization of a system based on free software and open source, using previous experiences experienced in other centers belonging to the Ministry of Higher Education.

Índice

Introducción

La Internet se ha convertido en una herramienta indispensable dentro del ámbito docente universitario, los usuarios la utilizan para la búsqueda de información las 24 horas del día por lo que lograr la conectividad es un trabajo que implica grandes recursos y preparación tanto de los administradores de red como del resto de los usuarios.

En Cuba tras un esfuerzo de unir todas las universidades del país se creó una red nacional dirigida por el Ministerio de Educación Superior, pero en los últimos años esta red ha crecido de forma exponencial sumándose otras redes de diferentes instituciones del país, por lo que el uso de comunicación y cooperación entre ellas aumenta el flujo de información sobre la red de datos.

La Universidad de Matanzas es uno de los centros educativos que cuenta con un considerable volumen de usuarios, por esta razón se ha vuelto imperiosa la necesidad de proveer a la institución de una óptima administración del *Internet* (ancho de banda asignado) que le permita tener el control de la utilización de las funcionalidades Web de los usuarios; con esto podrán optimizar el ancho de banda contratado y mantener registros de una buena utilización de este servicio.

Esto provoca que las organizaciones deban implementar soluciones que se adapten a sus necesidades, políticas internas y externas, tales como restricciones de acceso, registros de navegación y mantención de caché de los sitios visitados; por lo que un servidor Proxy es uno de los servicios que juega un papel importante en este ámbito.

Justificación: El Departamento de Redes de la Universidad de Matanzas principal encargado de brindar los servicios de telecomunicación, cuenta con un grupo de deficiencias que se abarca desde la infraestructura física de red hasta la preparación e inestabilidad del personal que labora.

Los servicios que se brindan mantienen configuraciones de hace más de 3 años, aun cuando la tecnología ha cambiado. Las políticas de navegación actuales del centro no están en correspondencia con las del Ministerio de Educación Superior o las del Ministerio de Informática y de las Telecomunicaciones de Cuba.

Dando a la tarea de darle solución a los principales problemas con los que se enfrentan cada día, surge la necesidad de un estudio sobre el sistema de navegación implementado hasta la fecha, dando a conocer que existen una serie de fallos que violan las políticas de la entidad y del país.

Por lo anterior planteado la **situación problemática** sería**:** ¿Cómo crear un Sistema de Navegación que optimice de manera eficiente los recursos de ancho de banda asignado a la Universidad de Matanzas, en correspondencia con las políticas de la entidad y el país?

Hipótesis: Si se crea un Sistema de Navegación eficiente en correspondencia con las políticas de la entidad y el país, se optimizará los recursos de ancho de banda asignado a la Universidad de Matanzas.

Objeto de Estudio: Sistema de Navegación por la Red de Datos actual de la Universidad de Matanzas.

Campo de acción: Red de Datos de la Universidad de Matanzas**.**

Objetivo General: Crear un Sistema de Navegación para la red de Datos que optimice de manera eficiente los recursos de ancho de banda asignado a la Universidad de Matanzas

Objetivos Específicos.

- Justificar mediante documentación las bases teóricas que servirán de referencia para la estructuración del presente trabajo.
- Describir el estado actual de la red en función al Sistema de Navegación implementado hasta el momento.
- Analizar los requerimientos físicos y lógicos necesarios para la implementación de la propuesta dada.
- Comparar la validación del sistema propuesto ante la solución actual.

Alcance: El propósito de este proyecto tiene como finalidad encontrar una alternativa que optimice el tráfico de navegación en la Universidad de Matanzas en comparación con un Sistema de Navegación ineficiente implementado hasta el momento

- Se analizará la situación actual de la red. Esto implica realizar una auditoría a las políticas y reglas implementadas sobre el acceso a contenido de Internet, a recursos locales y Red Nacional Cubana, lo que permite establecer pautas estrictas para la implementación de un proxy acorde con las políticas institucionales.
- Se estudiará la topología actual de la red para definir prioridades en dependencias de las subredes pertenecientes a las áreas del centro. Se establecerá los requerimientos físicos y lógicos para la posterior instalación del servidor.
- Implementar el proxy con políticas y reglas acordes con la administración de la red, que permitan dirigir el tráfico hacia un uso racional, enfocado a los procesos docentes e investigativos.

- En el proxy se procurará filtrar contenido web, tomando reportes de la herramienta de gestión y administración de ancho de banda, filtrar el contenido por tiempos y definir horarios convenientes en el que los usuarios puedan acceder a los recursos de internet que estén establecidos.

Estructura de esta Tesis.

- **Capítulo I: Fundamentación teórica y tendencias tecnológicas.**
  - Antecedentes de la investigación
  - Metodología de la investigación
  - Tecnologías asociadas
- **Capítulo II: Diseño de la solución propuesta.**
  - Caracterización de la situación actual de la red de datos de la Universidad de Matanzas
  - Caracterización del sistema de navegación actual
  - Sistema de Navegación propuesto
- **Capítulo III. Construcción de la propuesta y análisis de resultados.**
  - Instalación e integración de los componentes del sistema.
  - Análisis de los resultados y comparación con el sistema de navegación actual

Capítulo I: Fundamentación teórica y tendencias tecnológicas

Introducción.

En este capítulo se analizan las bases teóricas que sustentan y fundamentan la investigación. Se aborda la metodología de investigación utilizada, así como las cinco fases con las que cuenta para su desarrollo. Se encuentran presentes los elementos que ayudan a entender los procesos relacionados con el objeto de estudio, se exponen las principales tecnologías y herramientas relacionadas con la situación problemática.

1.1. Antecedentes de la Investigación.

A la conclusión de una exhaustiva búsqueda bibliográfica que abarcó los sitios de repositorios bibliográficos del MES y otras instituciones de Cuba se determina que, al presente trabajo de investigación, no le antecede proyecto similar realizado en la Universidad de Matanzas, por lo que surge este proyecto en base al análisis realizado al Sistema de Navegación actual en comparación a trabajos publicados en otras Universidades del país y el resto del mundo.

1.1.1. Historia y Evolución de los Sistemas de Navegación.

Un sistema de Navegación por una Red de Datos es un conjunto de servicios de redes enfocados a lograr la conectividad de los usuarios a los diferentes nodos de redes**,** controlando y monitoreando el uso de la tecnología mediante registros llamados *"Trazas"*, los cuales permiten obtener estadísticas como cantidad de tráfico o violaciones de las políticas establecidas.

El exceso de posibilidades que brinda la Internet en nuestros tiempos puede convertirse en un problema para las empresas u organizaciones que no cuentan con un ancho de banda acorde a la demanda de los usuarios. Cada institución u organización presenta un patrón de navegación y servicios diferentes en función de las actividades que se desarrollan. Debido a esto se establecen políticas de navegación para controlar el acceso o dar prioridad según corresponda, garantizando así un uso más eficiente de los recursos de ancho de banda disponible.

1.1.1.1. En el Mundo.

La primera descripción registrada de las interacciones sociales que se podían habilitar a través de la red fue una serie de memorandos escritos por J.C.R. Licklider, del MIT, en agosto de 1962, en los que describe su concepto de "Red galáctica". Imaginó un conjunto de ordenadores interconectados

globalmente, a través de los que todo el mundo podría acceder rápidamente a datos y programas desde cualquier sitio. En espíritu, el concepto era muy similar a la Internet de hoy en día. Licklider era el director del programa de investigación informática de DARPA,4 que comenzó en octubre de 1962. Mientras estaba en DARPA convenció a sus sucesores en dicha agencia (Ivan Sutherland, Bob Taylor y Lawrence G. Roberts, investigador del MIT), de la importancia de su concepto de red. (1)

Leonard Kleinrock, del MIT, publicó el primer documento sobre la teoría de conmutación de paquetes en julio de 1961 y el primer libro sobre el tema en 1964 Kleinrock convenció a Roberts de la factibilidad teórica de comunicarse usando paquetes en vez de circuitos, lo que fue un gran paso en el viaje hacia las redes informáticas. A finales de 1966, Roberts entró en DARPA para desarrollar el concepto de redes informáticas y rápidamente creó su plan para “ARPANET “, que publicó en 1967 (1)

Mientras el equipo de BNN trabajaba en los IMP con Bob Kahn desempeñando un importante papel en el diseño arquitectónico general de ARPANET, Roberts, junto con Howard Frank y su equipo de Network Analysis Corporation, diseñaron la topología y la economía de la red. El sistema de medición de la red lo preparó el equipo de Kleinrock en UCLA (1)

En diciembre de 1970, el Network Working Group (NWG), bajo el liderazgo de S. Crocker, terminó el protocolo de host a host inicial de ARPANET, llamado Network Control Protocol (NCP). Cuando los sitios de ARPANET terminaron de implementar NCP, en el periodo de 1971 a 1972, los usuarios de la red pudieron, por fin, comenzar a desarrollar aplicaciones. (1)

Uno de los retos más interesantes fue la transición del protocolo de host de ARPANET de NCP a TCP/IP el 1 de enero de 1983. Fue una transición “histórica”, que exigió que todos los hosts se convirtiesen simultáneamente para no tener que comunicarse a través de mecanismos especiales. Esta transición se planificó cuidadosamente en la comunidad durante años antes de llevarse a cabo realmente, y fue sorprendentemente bien. Así pues, para 1985 Internet ya estaba bien establecida como tecnología que daba cobertura a una amplia comunidad de investigadores y desarrolladores, y empezaba a ser usada por otras comunidades para comunicaciones informáticas diarias. El correo electrónico se usaba ampliamente entre varias comunidades, a menudo con diferentes sistemas, pero la interconexión entre diferentes sistemas de correo demostraba lo útil que era una amplia comunicación electrónica entre la gente. (1)

Para el año 1990, ARPANET había sido superado y reemplazado por nuevas tecnologías de red, y el proyecto se clausuró. Tras la clausura de ARPANET, en 1994, NSFNet, actualmente ANSNET (Advanced Networks and Services, Redes y Servicios Avanzados) y tras permitir el acceso de organizaciones sin ánimo de lucro, perdió su posición como base fundamental de Internet. Ambos, el

gobierno (EE. UU) y los proveedores comerciales crearon sus propias infraestructuras e interconexiones. Los NAPs regionales se convirtieron en las interconexiones primarias entre la multitud de redes y al final terminaron las restricciones comerciales. (1)

Durante los años 2000 el auge de los dispositivos inteligentes, que incluye sensores, teléfonos, relojes, autos y equipos del hogar, todos conectados en redes, ha provocado un solapamiento entre las tradicionales redes de datos y los emergentes dispositivos que hoy en día la conforman. El aumento de ¨hosts¨ ha provocado un éxodo de Proveedores de Servicios, los cuales se encargan en su mayoría de manipular un tráfico totalmente heterogéneo donde se precian grandes volúmenes de información aportado por contenido de multimedia que consume grandes recursos de ancho de banda. Dicho fenómeno provoca que en la actualidad sea todo un reto ofrecer un servicio de navegación donde la demanda de recursos de banda es en promedio mayor a los recursos que se disponen, lo cual constituye el reto fundamental de los sistemas de navegación. (1)

Estos sistemas se encuentran en la mayoría de las entidades públicas o privadas, desde empresas y universidades hasta negocios pequeños o para uso personal, son implementados analizando la posibilidad de soluciones comerciales o no comerciales que existen, y se eligen en función a sus especificidades, por lo que obtener una solución de otra entidad puede ser costosa o no adaptable a nuestros requerimientos.

1.1.1.2. En Cuba.

Delinear la ruta de Internet en Cuba remite a dos circunstancias fundamentales: el bloqueo económico, comercial y financiero de los Estados Unidos y la profunda crisis económica iniciada en los años noventa. Desde los antecedentes tecnológicos que sentaron las bases para la llegada de Internet al país hasta la actualidad, esta tecnología particular se ha dirimido entre complejas tensiones políticas e infraestructurales. (2)

En la década del 70 ante la necesidad de trabajar en red y compartir recursos para la producción científica, se crean “diseños propios” para la conmutación de paquetes desde el Centro de Investigaciones Digitales (CID) y el Instituto de Matemática, Cibernética y Computación (IMACC). (2)

Llegan los 80, se desarrollan tecnologías para el procesamiento y transmisión de datos, y la creación de redes nacionales. Asociados a estos procesos, es posible mencionar varios acontecimientos significativos:

- El trabajo conjunto con los países miembros del Consejo de Ayuda Mutua (CAME), que permitió el intercambio de información y el acceso a grandes bases de datos, en la medida en que se desarrollaban las redes.
- La introducción y extensión en Cuba de “máquinas grandes” para el procesamiento de datos, y de “minicomputadoras” para aumentar la capacidad y la velocidad de transmisión de datos. Se realizaron las primeras conexiones satelitales entre La Habana y Moscú.
- Se desarrollan las primeras redes de comunicación extendida –WAN (Wide Area Network)– y comienza a usarse el servicio de correo electrónico.
- Surgen los Jóvenes Clubes de Computación y Electrónica, una red de centros tecnológicos comunitarios para la socialización de las tecnologías y la informatización de la sociedad. (2)

A inicios de los noventa, Cuba ocupaba un lugar destacado en la región por la búsqueda de alternativas para el impulso y aplicación de las técnicas de Internet. En el período, es posible mencionar algunos acontecimientos significativos:

- La inclusión de Cuba en un Programa Regional de Desarrollo de las Nuevas Tecnologías para países en Vías de Desarrollo, por parte de la Oficina Regional del Programa de Naciones Unidas para el Desarrollo (PNUD) en La Habana.
- El surgimiento de redes nacionales con servicios innovadores: TinoRed, asociada a los Jóvenes Clubes; Infomed, una red colaborativa para gestionar y compartir recursos de información en el ámbito de la salud; CIGBnet, la red del Centro de Ingeniería Genética y Biotecnología y sus instituciones afiliadas; y RedUniv, red universitaria para información científico-técnica del Ministerio de Educación Superior de Cuba. (2)

Desde 1991 al 2012 estuvieron marcados por la noción de acceso social, y por coyunturas y urgencias contextuales asociadas a la postura defensiva del país ante las tensiones históricas de la relación con Estados Unidos. El período culmina con la conexión de Cuba a Internet mediante fibra óptica (2)

Otro factor muy importante en el desarrollo de la red cubana y el cumplimiento de los objetivos y metas propuestas por el Estado fue la creación de la Empresa de Telecomunicaciones de Cuba (ETECSA) en el año 1994 la cual, dos años después de creada logra detener el deterioro de nuestra infraestructura de telecomunicaciones en el país y emprende la creación de un *backbone* nacional capaz de soportar todos los desarrollos del país en materia de redes e informática. Sin esa determinación, sin duda, no se podrían mostrar los aún modestos adelantos que ya hoy evidencian nuestras redes, instituciones y sociedad en materia de conectividad. Esta acción y la decisión de crear el Ministerio de la Informática y las Comunicaciones en febrero de 2000 marcan la pauta para el desarrollo y aplicación plena de una

sociedad informatizada. La intención de ampliar los usuarios y servicios de Internet en Cuba tienen una expresión palpable en 2012, cuando entró en operación el cable submarino de fibra óptica ALBA-1, que enlaza al país con Venezuela y Jamaica. Con esto, se abre una nueva etapa para el acceso a la red de redes. (2)

La llegada del tercer milenio atrajo un grupo de retos para nuestro país en términos de navegación, llegando a todas los centros e instituciones el servicio de acceso a Internet. La creación de una Red Nacional de la mano en sus principios del Ministerio de Educación Superior y la Empresa de Telecomunicaciones de Cuba ha propiciado que exista un grupo heterogéneo de tráfico a gestionar.

La Universidad Cubana en compañía de la Unión de Informáticos de Cuba, creada recientemente, juega un papel fundamental en la informatización de la sociedad, por lo que se debe asumir el reto de crear conciencia en el uso de los servicios de navegación.

Las problemáticas que existen a nivel mundial se aplican a nuestro país, agregándole la existencia de un Embargo Económico y Comercial impuesto por Los Estados Unidos que prohíbe a Cuba la adquisición de soluciones o aplicaciones presentadas por compañías de dicho país. Por tanto, se orienta la implementación de soluciones basadas en software libre y código abierto.

Los centros pertenecientes al MES se encuentran aplicando este tipo de solución a medida que sus recursos lo permiten, respetando la Misión de la Universidad Cubana y asumiendo las nuevas políticas de informatización. En nuestras universidades el acceso a los servicios de redes es normalizado por resoluciones y normativas, tanto ministeriales como rectorales. Cada persona tiene un nivel de acceso o privilegios según estas normas y solo puede acceder a los servicios que le son aprobados.

El Departamento de Redes de la Universidad de Matanzas ha logrado obtener configuraciones de otros centros universitarios con el objetivo de estudiar la compatibilidad con los requerimientos del nuestro, y así poder comparar con la solución actual incorporando nuevas configuraciones. Internamente en cada centro se dictan resoluciones o políticas dependiendo de sus características: cantidad de usuario, conectividad, conocimiento de los usuarios en términos de la red, ancho de banda e infraestructura de la red, por lo que, aunque es posible utilizar partes de las configuraciones de otros centros para ayudar a comprender la situación, no es aplicable como una solución general, por lo que se tomó como medida la incorporación de una solución propia en la entidad.

1.1.2. Ventajas de un Sistema de Navegación Eficiente.

- Uso eficiente de los recursos: el ancho de banda total puede ser designado en función de las necesidades de la entidad o centro, dando preferencia a los servicios más importantes que se desarrollan.
- Obtención de estadísticas: se realiza una recopilación de toda la información tanto de forma inmediata (monitoreo) como no inmediata *(¨trazas¨).*
- Aplicación de políticas: se puede establecer un grupo de políticas que promuevan el uso de determinados recursos y servicios.
- Control de acceso: se regula el grupo de información no deseada o que pudiera ser nociva para el usuario.
- Aumento de la velocidad: Mediante el uso de técnicas y memorias agregadas (*Caché*) se puede reducir el volumen de datos que se transfiere entre nodos, generando así una sensación de aumento de la velocidad de transferencia de la información.
- Seguridad: un adecuado tratamiento y el conocimiento de la información que se gestiona aumenta la seguridad, detectando al instante errores en el sistema.
- Flexibilidad: un sistema de navegación orientado a servicios brinda la posibilidad de realizar cambios internos en las políticas ya implementadas, permitiendo por separado y sin afectar el sistema.
- Escalabilidad: mediante una estructura modular se permite la implementación de nuevas políticas, así como realizar cambios fácilmente.

1.2. Metodología de Investigación.

Esta investigación es de tipo mixta, debido a que inicialmente se llevó a cabo un estudio teórico (obtenido de libros, artículos virtuales, páginas web, etc.) detallado de la tecnología de Sistemas de Navegación en cuanto a variables como infraestructura y funcionamiento. Además, se realizó una investigación de campo en diferentes escenarios de prueba que permitieron recolectar y analizar datos sobre el uso de la red por los usuarios.

El diseño de la investigación se puede denominar como experimental, debido a que, al identificarse las variables estudiadas, anteriormente mencionadas, se realizó uso y control de estas para llevar a cabo la realización de los escenarios de infraestructura de los servicios de red como se indica detalladamente en la metodología de la tesis.

1.2.1. Método Hipotético-Deductivo.

El método hipotético-deductivo es el procedimiento o camino que sigue el investigador para hacer de su actividad una práctica científica. El método hipotético-deductivo tiene varios pasos esenciales: observación del fenómeno a estudiar, creación de una hipótesis para explicar dicho fenómeno, deducción de consecuencias o proposiciones más elementales que la propia hipótesis, y verificación o comprobación de la verdad de los enunciados deducidos comparándolos con la experiencia. Este método obliga al científico a combinar la reflexión racional o momento racional (la formación de hipótesis y la deducción) con la observación de la realidad o momento empírico (la observación y la verificación) (3)

Este método fue utilizado en el proyecto ya que partimos de una hipótesis, la misma que después será comprobada experimentalmente en base a la realidad. El desarrollo de la metodología consta principalmente de cinco fases, las cuales indican de manera secuencial los procedimientos.

Dichas fases son:

1.2.1.1. Recolección de datos sobre la infraestructura de red estudiada.

Para esto fue necesario la participación de los administradores de redes del centro, así como el Director de Informatización de la Universidad de Matanzas Ángel Luis Zuriarraín, quienes cuentan con experiencia en la expansión de la red de datos de la Universidad. Esta información es necesaria ya que delimita la realidad de comunicación entre las diferentes subredes pertenecientes a los centros entrelazados que conforman la red, así como los segmentos de redes dentro de cada una de ellas.

1.2.1.2. Recolección de datos sobre el funcionamiento del Sistema de Navegación Actual.

Para esto fue necesario obtener la información directamente desde los servidores actuales en cuanto a su funcionamiento interno y tratamiento de información sobre el uso de la red por los usuarios, dicha información fue extraída de los logs de registros diarios guardados por más de un año, así como de experiencia del propio administrador principal, quien cuenta con más de un año al frente de estos servicios.

1.2.1.3. Diseño y estudio para especificación de requerimientos.

Para esta fase se realizó a profundidad una documentación correspondiente a las tecnologías asociadas con el tema del proyecto. Dicha información facilita la comprensión de esta tecnología para proponer la

solución planteada, entender la mejor manera de cómo funcionan las variables manejadas en los escenarios probados y facilitar la selección de las herramientas utilizadas.

1.2.1.3.1. Clasificar y estructurar requerimientos.

El clasificar requerimientos es una forma de organizarlos, ya que existen algunos que por sus características no pueden ser tratados igual que a otros. Por ejemplo, los requerimientos de entrenamiento de personal no son tratados de la misma manera que los requerimientos de una conexión a Internet.

La siguiente es una recomendación de cómo pueden ser clasificados los requerimientos, aunque cada proyecto pueda usar sus propias clasificaciones.

Requerimientos del "entorno".

- El entorno es todo lo que rodea al sistema, existen ciertos tipos de requerimientos que se clasifican en esta categoría y el sistema necesita como fuente de servicios necesarios para su funcionamiento. Como ejemplos podemos mencionar, sistemas operativos, sistema de autentificación e infraestructura de red.

Requerimientos de desempeño.

- Estos requerimientos nos informan las características de desempeño que debe tener el Sistema. ¿Qué tan eficaz? ¿Qué tan seguro?

Disponibilidad (en un determinado período de tiempo).

- Este tipo de requerimientos se refiere a la durabilidad, degradación, portabilidad y flexibilidad. Son muy importante en servicios de tiempo real puesto que estos servicios manejan aplicaciones críticas que no deben estar fuera del servicio por periodos prolongados de tiempo.

Entrenamiento

- Este tipo de requerimientos se enfoca a las personas que van a administrar la solución. ¿Qué tipo de usuarios son? ¿Qué tipo de operadores? ¿Qué manuales se entregarán y en qué idioma?

Este tipo de requerimientos, aunque muchas veces no termina con especificaciones de la configuración del servicio, son muy importantes en el proceso de diseño ya que facilitan la introducción y aceptación del servicio en donde será implementado.

Restricciones de diseño.

- Muchas veces las soluciones de un servicio son normadas por leyes o estándares, este tipo de normas caen como "restricciones de diseño".

1.2.1.4. Montaje de los escenarios de prueba del Servicio de Navegación para estudio de las herramientas y variables implicadas.

Para el desarrollo de esta fase, inicialmente se determinan qué herramientas serían utilizadas para el montaje de los escenarios probados. Se realizan varios escenarios con el objetivo de determinar la viabilidad de la implementación propuesta en relación con la actual, esto se conforma desde una configuración básica hasta una configuración más compleja teniendo en cuenta los objetivos de este proyecto.

- Comenzar con medir las capacidades de *hardware* y *software* con las que cuenta el sistema actual para realizar pruebas sin mayor complejidad y entender en la práctica el funcionamiento de la estructura implementada.
- Instalación de un servidor demo en el cual se obtiene datos sobre las peticiones de los usuarios a Internet y Red Nacional Cubana, la utilización de las peticiones del centro en general solo fue posible en determinados espacios de tiempo ya que esto llevaba consigo la interrupción de los servicios prestados a la comunidad atrasando la gestión de los procesos de los trabajadores y estudiantes.
- Pruebas de configuración más avanzadas y profundas sobre las tecnologías asociadas a la implementación propuesta.
- Obtención de información de las pruebas realizadas.

1.2.1.5. Metodología para implementación de la solución propuesta.

Después de realizar las cuatro anteriores fases para comprender y obtener la fiabilidad de las herramientas y configuraciones, se presenta una guía metodológica que permita implementar el sistema propuesto

1. Selección de hardware y software encargado de la implementación de este sistema.
2. Configuraciones básicas y avanzadas de las herramientas seleccionadas que permitan una optimización a la hora de obtener datos sobre el uso de los servicios.
3. Pruebas de flujo de información y respuesta desde los servidores.

4. Comprobación de la factibilidad de la propuesta dada.

1.3. Tecnologías Asociadas.

1.3.1. Software libre

En 1984, Richard Stallman comenzó a trabajar en el proyecto GNU, y un año más tarde fundó la Free Software Foundation (FSF). El proyecto GNU fue iniciado con el objetivo de crear un sistema operativo completamente libre, para asegurar que el software GNU permaneciera libre para que todos los usuarios pudieran "ejecutarlo, copiarlo, modificarlo y distribuirlo", el proyecto debía ser liberado bajo una licencia diseñada para garantizar esos derechos al tiempo que evitase restricciones posteriores de los mismos. La idea se conoce en inglés como copyleft -'copia permitida'- (en clara oposición a copyright -'derecho de copia'-), y está contenida en la Licencia General Pública de GNU(GPL). (4)

Stallman introdujo la definición de free software (software libre) que desarrolló para otorgar libertad a los usuarios y para restringir las posibilidades de apropiación del software. El software libre suele estar disponible gratuitamente, o al precio de coste de la distribución a través de otros medios; sin embargo, no es obligatorio que sea así, por lo tanto, no hay que asociar software libre a "software gratuito" (denominado usualmente freeware), ya que, conservando su carácter de libre, puede ser distribuido comercialmente ("software comercial"). Análogamente, el "software gratis" o "gratuito" incluye en ocasiones el código fuente; no obstante, este tipo de software no es libre en el mismo sentido que el software libre, a menos que se garanticen los derechos de modificación y redistribución dedicas versiones modificadas del programa. (4)

1.3.1.1. Linux.

GNU/Linux, es el término empleado para referirse a la combinación del sistema operativo GNU, desarrollado por la FSF, y el núcleo(kernel) Linux, desarrollado por Linus Torvalds y la Linux Foundation.

Una de las principales razones para utilizar Linux es que es que no son necesarias licencias. Linux mantiene la marca registrada Linux, el kernel de Linux se distribuye bajo la licencia GPL, esto significa que se puede obtener y modificar el código fuente. (4)

Linux es distribuido mediante una serie de distribuciones como RedHat, Slackware, Debian, Ubuntu, etc., las cuales se diferencian por su método de instalación y por los paquetes (software) que viene incluido. Hay muy buenas razones para optar por Linux ya que, el sistema ofrece estabilidad, seguridad y velocidad. Otro aspecto importante es su capacidad de conectividad en redes que ha sido decisiva

para la conquista del mercado de servidores. Debido a esta disponibilidad nadie está a merced de ningún productor de software, sino que es posible hacer adaptaciones y extensiones según las necesidades.

Tampoco hay que olvidar que el uso de Linux no exige la adquisición de licencias; da igual si se usa de forma particular o con propósitos comerciales. Aunque Linus Torvalds, el creador de Linux, mantiene la marca registrada Linux, el Kernel de Linux y la mayoría del software que le acompaña se distribuye bajo licencia *GPL*.

Este sistema se ha instalado tanto en negocios y universidades, como para uso personal. Lo que hace a Linux tan diferente, es que es una implementación de *UNIX* sin costo. Fue y todavía es desarrollada por un grupo de voluntarios, principalmente de Internet, quienes intercambian código, reportan trucos y resuelven problemas en un ambiente completamente abierto

1.3.1.1.1. Debian.

El proyecto *Debian* es una comunidad conformada por desarrolladores y usuarios que mantiene un sistema operativo operado por *GNU* basado en software libre. El sistema operativo (SO) se llama Debian GNU/Linux o simplemente Debian. Debian en sus inicios parecía destinada a desintegrarse y colapsar, pero la realidad resultó muy diferente no sólo sobrevivió sino que prosperó y, en menos de una década, se convirtió en la mayor distribución de Linux y, posiblemente, el mayor proyecto de software colaborativo jamás creado. (4)

Actualmente, el proyecto incluye más de mil desarrolladores, cada uno de ellos posee algún lugar en el proyecto ya sea relacionado con los paquetes: mantenimiento, documentación, control de calidad o relacionado con la infraestructura del proyecto: coordinación de lanzamientos, traducciones de web, etc. Esta integración y estabilización progresiva de paquetes y componentes, junto a los sólidos y probados mecanismos de control de calidad, le han dado a Debian la reputación de ser una de las distribuciones más probadas y libres de errores de la actualidad. (4)

Debian es famoso por filosofía de estabilidad, por eso mismo, no tiene un cronograma de lanzamiento de nuevas versiones, estas se liberan cuando están listas. Esto hace que sea una de las opciones más estables de GNU/Linux. (4)

Ventajas: No es recomendado para principiantes por lo que para expertos en redes es la una de las mejores opciones. Una de las distribuciones más estables. Ligero, no necesita grandes recursos físicos para funcionar. Solo utiliza software libre, aunque es posible instalar software propietario sobre él. Distribución preferida para muchos y la base de numerosas distribuciones. Por lo general es más seguro, altamente customizable y posee mayor rendimiento.

Desventajas: los lanzamientos estables de Debian no resultan particularmente actualizados, y envejecen rápidamente, especialmente si se considera que los lanzamientos estables se publican cada 1 - 3 años. Los usuarios que prefieren contar con los paquetes y tecnologías más recientes se ven forzados a usar los ramales "*testing*" o "*unstable*", los cuales pueden contener errores

Otras características:

- Manejo de paquetes de software: *Advanced Package Tool (APT)* usando paquetes *DEB*
- Ediciones disponibles: CD/DVD de instalación e imágenes de *live CD* para 11 arquitecturas de procesador, incluyendo procesadores *AMD* e *Intel* de 32-bit y 64-bit, entre otras
- Distribuciones alternativas basadas en Debian: *Ubuntu, Damn Small Linux, KNOPPIX, sidux, Dreamlinux, Elive, Xandros, 64 Studio*

1.3.1.1.2 Ubuntu.

Ubuntu es una distribución GNU/Linux que ofrece un sistema operativo orientado principalmente a computadoras personales, aunque también proporciona soporte para servidores. Es una de las más importantes distribuciones de GNU/Linux a nivel mundial. Se basa en Debian GNU/Linux y concentra su objetivo en la facilidad y libertad de uso, la fluida instalación y los lanzamientos regulares (cada 6 meses: las versiones .04 en abril y las .10 en octubre). El principal patrocinador es Canonical Ltd., una empresa privada fundada y financiada por el empresario sudafricano Mark Shuttleworth (4)

Ediciones disponibles: *Ubuntu, Kubuntu, Xubuntu, Ubuntu Studio y Mythbuntu para 32-bit (i386) y 64-bit (x86_64) y Ubuntu Server Edition*

- **Ventaja:** Ciclo fijo de lanzamiento y período de soporte; amigable con el novato en Linux, riqueza en la documentación tanto oficiales como en contribuciones de los usuarios
- **Desventaja:** Varios softwares de Ubuntu (por ejemplo, *Launchpad, Rosetta*) son software propietario, además carece de compatibilidad total con Debian

1.3.2. Sistema de Virtualización.

En sentido general, cuando se habla de virtualización, a lo que se refiere es a la virtualización de servidores, lo que significa particionar un servidor físico en varios servidores virtuales. Cada máquina virtual puede interactuar de forma independiente con otros dispositivos, aplicaciones, datos y usuarios, como si se tratara de un recurso físico independiente. Diferentes máquinas virtuales pueden ejecutar diferentes sistemas operativos y múltiples aplicaciones al mismo tiempo utilizando un solo equipo físico.

Debido a que cada máquina virtual está aislada de otras máquinas virtualizadas, en caso de ocurrir un bloqueo esto que no afecta a las demás máquinas virtuales.

La virtualización se desvaneció como centro de atención durante un tiempo, ahora es una de las últimas tendencias en la industria una vez más, ya que las organizaciones tienen por objeto aumentar la utilización, la flexibilidad y la rentabilidad de sus recursos informáticos. *VMWare, Citrix, Microsoft, IBM, Red Hat* y muchos otros proveedores ofrecen soluciones de virtualización.

¿Cuáles son las ventajas de la virtualización?

- Disminuye el número de servidores físicos. Esto trae como consecuencia una reducción directa de los costos de mantenimiento de hardware.
- Mediante la implementación de una estrategia de consolidación de servidores, puede aumentar la eficiencia de la utilización del espacio en su centro de datos.
- Al tener cada aplicación dentro de su propio "servidor virtual" puede evitar que una aplicación impacte otras aplicaciones al momento de realizar mejoras o cambios.
- Usted puede desarrollar una norma de construcción de servidor virtual que se puede duplicar fácilmente lo que acelerará la implementación del servidor.
- Usted puede desplegar múltiples tecnologías de sistemas operativos en una sola plataforma de hardware.

1.3.2.1. VMWare ESXi

Es un hypervisor nativo especialmente diseñado, líder del mercado. ESXi se instala directamente en el servidor físico, lo que permite dividirlo en varios servidores lógicos denominados máquinas virtuales. Los clientes pueden utilizar ESXi con la versión gratuita vSphere Hypervisor o como parte de una edición de pago de vSphere. (5)

Características de vSphere ESXi.

- Fiabilidad y seguridad mejoradas: La funcionalidad de gestión del hypervisor nativo ESXi se integra en Kernel, lo que reduce el tamaño a 150 MB. Esto ofrece una superficie de ataque muy pequeña para los programas maliciosos y las amenazas de red, lo que mejora la fiabilidad y la seguridad.
- Implementación y configuración optimizadas: Dado que tiene menos opciones de configuración y que la implementación y la configuración son sencillas, la arquitectura ESXi facilita el mantenimiento de una infraestructura virtual homogénea.

- Seguridad mejorada: No es necesario compartir el acceso ni una cuenta de superusuario común para realizar tareas administrativas.
- Registros y auditorías exhaustivos: registra toda la actividad de los usuarios, desde el Shell y la interfaz de usuario de consola directa, en la cuenta del usuario. De esta forma, se garantiza la responsabilidad por parte de los usuarios y resulta sencillo auditar su actividad.
- La migración dinámica: permite trasladar una máquina virtual completa de un servidor físico a otro, sin tiempo de inactividad, además de migrar máquinas virtuales entre clústeres.
- Código Propietario: Soporta SO como Windows, Linux, Unix, etc.
- Server de Administración Dedicado: necesario para las vista o administración centralizada.
- Es necesario una cuenta de suscripción para una licencia válida por 3 meses.
- Soporta alta disponibilidad (HA) y Balanceo de Carga. (5)

1.3.2.2. Proxmox Virtual Environment.

Proxmox Virtual Environment (Proxmox VE) es una plataforma de virtualización de código libre desarrollado y mantenido por Proxmox Server Solutions GmbH y financiado por la Internet Foundation Austria. Proxmox VE permite correr aplicaciones virtuales y máquinas virtuales de una manera muy sencilla. (6)

Proxmox VE es un completo software de gestión de virtualización de servidor de código abierto. Se basa en la virtualización KVM (Máquina Virtual basada en el núcleo) y la virtualización basada en contenedores y administra máquinas virtuales KVM, contenedores de Linux (LXC), almacenamiento, redes virtuales y clúster de alta disponibilidad. Proxmox VE permite crear una estructura de servidores completa a partir de un hardware sin ninguna instalación previa en menos de una hora incluyendo proxys de email y web, wikis, intranets (6)

Desde su página web podemos descargar una imagen *ISO* que será la que tendremos que instalar en el equipo (desde un *CD* o *USB*) para poder habilitar la interfaz y las funciones del software de virtualización.

Proxmox utiliza un entorno basado en Debian con un kernel modificado ya que una de las ventajas es que las operaciones que se pueden realizar son por medio de líneas de comando o por interfaz gráfica mediante el navegador web.

Características de Proxmox.

- Alta Disponibilidad y escalabilidad sin límites. Puede colocarse en servidores con carga de trabajo extremo sin presentar problemas. Puede utilizar las últimas versiones de Procesadores Intel/AMD.
- Virtualización: Permite virtualizar sistemas operativos en sus versiones 32/64 bits: Linux en todas sus versiones, Windows XP/ Vista / Seven/ v8/ v10, Solaris, AiX, entre otros.
- KVM (Máquina Virtual basada en el Núcleo).
- LXC (Linux Container).
- Backup & Restore de "Máquinas Virtuales": Se acciona a través de su interfaz Web y de forma sencilla. Se pueden efectuar de forma inmediata o dejarse programado. La restauración es simple, solo debe seleccionar el bakup darle un número identificativo y listo.
- Snapshot Live. Permite hacer copias instantáneas de "Máquinas Virtuales" incluyendo el contenido de la RAM, su configuración y estado de los discos duros. Se puede retroceder en el tiempo la MV restaurando el último "Live Snapshot".
- Migración en caliente. La administración de los nodos es centralizada a través de una interfaz web permitiendo movilizar "Máquinas Virtuales" entre cada "Servidor Físico (NODO)" sin tener que apagar la Máquinas Virtuales.
- Clúster Alta disponibilidad: Permite definir reglas de "Alta disponibilidad", si un nodo esté sobrecargado se transfiere automáticamente a otro "Servidor Físico (NODO)" con menos carga la Máquinas Virtuales.
- Administración centralizada. En un "Clúster Proxmox" se debe definir uno de los Nodos como "Orquestador" con el objetivo de centralizar el trabajo, sin embargo, cada nodo cuenta con su propio administrador web.
- SPOF (Single Point of Failure). Cada "Servidor Físico (NODO)" Cuenta con su propio interfaz Web Permitiendo el acceso a la administración de las MV. Si el nodo "Orquestador" llega a fallar, cada nodo tiene replicado la información del "Orquestador" y desde cualquier nodo puede tomar el control del clúster.
- Puentes de red: Proxmox administra las tarjetas físicas a través de Bridges que comparte a las Máquinas Virtuales, es muy fácil asociar 1 o varias tarjetas a un "Bridges" haciendo un balanceo automático del tráfico de red.
- NAS & SAN: Es muy sencillo utilizar "Dispositivos de almacenamientos" a través de NAS con NFS o en caso de SAN con "iSCSI".

- Autentificación. Puede configurar la autenticación de acceso al área de “Administración a los Nodos” a través de cuentas propias con Proxmox o utilizando LDAP/Active Directory. (7)

1.3.2.2.1. LXC (Linux Container).

Los contenedores son una alternativa ligera a las máquinas virtuales completamente virtualizadas. En lugar de emular un sistema operativo (SO) completo, los contenedores simplemente utilizan el sistema operativo del host en el que se ejecutan. Esto implica que todos los contenedores usan el mismo núcleo y que pueden acceder a los recursos directamente desde el host. Esto es genial porque los contenedores no desperdician la potencia de la CPU ni la memoria debido a la emulación del kernel. Los costos de tiempo de ejecución del contenedor son casi nulos y generalmente insignificantes. (8)

Cada proceso ejecutado en cada contenedor es como un proceso ejecutado en el *Host* y por tanto más ligero que el mismo proceso ejecutado en una Máquinas Virtuales. Esto significa que cuando un contenedor termina de ejecutar su tarea, el contenedor se para y deja de consumir recursos del *Host*.

1.3.2.2.2. Kernel-based Virtual Machine (KVM)

Es una solución para implementar virtualización completa con Linux. Está formada por un módulo del núcleo (con el nombre kvm) y herramientas en el espacio de usuario, siendo en su totalidad software libre. KVM permite ejecutar máquinas virtuales utilizando imágenes de disco que contienen sistemas operativos sin modificar. Cada máquina virtual tiene su propio hardware virtualizados: una tarjeta de red, discos duros, tarjeta gráfica, etc. (9)

Tendremos que instalar o mantener en cada Máquinas Virtuales todas las librerías y aplicaciones que necesite el SO y las aplicaciones y servicios que queramos correr.

1.3.3. Active Directory.

Servicios de directorio es una base de datos distribuida que permite almacenar información relativa a los recursos de una red con el fin de facilitar su localización y administración. Las cuestiones básicas relacionadas con un centro de servicios de directorio giran alrededor de la información que se puede almacenar en la base de datos, cómo se almacena, cómo se puede consultar información específica y qué se puede hacer con los resultados. Active Directory se compone del propio servicio de directorio junto con un servicio secundario que permite el acceso a la base de datos y admite las convenciones de denominación X.500 (10)

Puede consultar el directorio con un nombre de usuario para obtener información como el número de teléfono o la dirección de correo electrónico de ese usuario. Los servicios de directorio también son lo suficientemente flexibles como para permitir la realización de consultas generalizadas. (10)

Los servicios de directorio también ofrecen la ventaja de suponer un único punto de entrada para los usuarios a la red de toda la empresa. Los usuarios pueden buscar y usar recursos en la red sin conocer el nombre o la ubicación exactos del recurso. Igualmente, puede administrar toda la red con una vista lógica y unificada de la organización de la red y de sus recursos (10)

1.3.3.1. LDAP.

LDAP (Protocolo ligero de acceso a directorios) es un protocolo de software que permite a cualquier persona ubicar organizaciones, individuos y otros recursos como archivos y dispositivos en una red, ya sea en la Internet pública o en una intranet corporativa. LDAP es una versión "ligera" (menor cantidad de código) de Directory Access Protocol (DAP), que es parte de X.500, un estándar para servicios de directorio en una red. LDAP es más ligero porque en su versión inicial no incluía características de seguridad. LDAP se originó en la Universidad de Michigan y ha sido respaldado por al menos 40 compañías. Netscape lo incluye en su último conjunto de productos de Communicator. Microsoft lo incluye como parte de lo que llama Active Directory en una serie de productos, incluido Outlook Express. Los servicios de directorio NetWare de Novell interactúan con LDAP. Cisco también lo admite en sus productos de red (11)

Un directorio es un conjunto de objetos con atributos organizados en una manera lógica y jerárquica. Habitualmente, almacena la información de autenticación (**usuario y contraseña**) y es utilizado para autenticarse, aunque es posible almacenar otra información (**datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados**, etc.). A manera de síntesis, LDAP es un protocolo de acceso unificado a un **conjunto de información sobre una red.** (11)

1.3.4. Firewall.

Un firewall es una entidad confiable que se asienta para separar áreas sensibles dentro de una red de computadoras. El cortafuego *(firewall)* se configura con un conjunto de reglas que dependen de las políticas de seguridad de la organización, que determinan a qué tráfico de red se le permitirá pasar y cual será bloqueado o rechazado

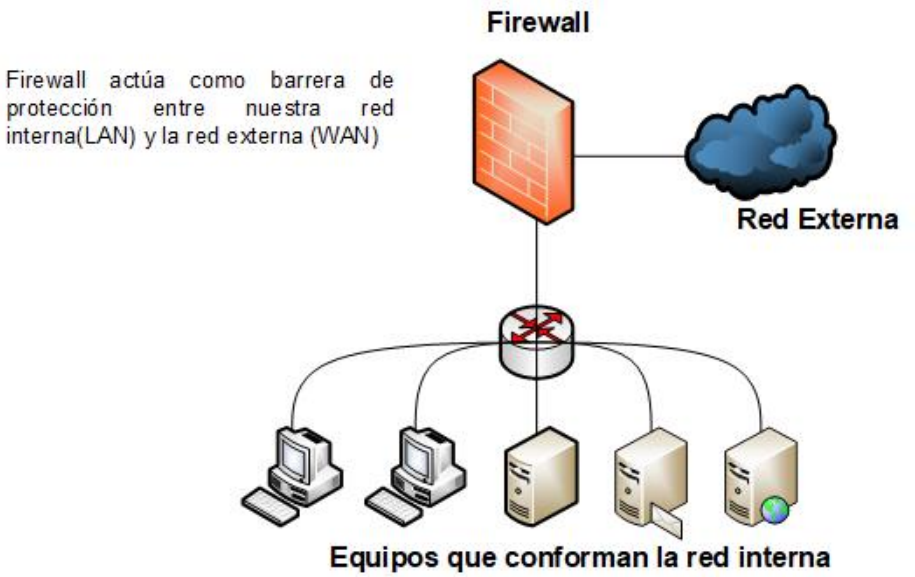


Figura 1. Esquema de un Firewall. Fuente. Creado por el autor

1.3.4.1. Firewalls de software.

Un *firewall* de *software* es una aplicación que puede estar integrada en el mismo sistema operativo (*Iptables*) o puede instalarse independientemente, son fácilmente escalables ya que se pueden integrar a proxies.

1.3.4.1.1. Iptables.

Netfilter es un framework disponible en el núcleo Linux que permite interceptar y manipular paquetes de red. Dicho framework permite realizar el manejo de paquetes en diferentes estados del procesamiento. Netfilter es también el nombre que recibe el proyecto que se encarga de ofrecer herramientas libres para cortafuegos basados en Linux. (12)

El componente más popular construido sobre Netfilter es Iptables, una herramienta de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4 o mantener registros de log. El proyecto Netfilter no sólo ofrece componentes disponibles como módulos del núcleo, sino que también ofrece herramientas de espacio de usuario y librerías (12).

Iptables es el nombre de la herramienta de espacio de usuario mediante la cual el administrador puede definir políticas de filtrado del tráfico que circula por la red. El nombre Iptables se utiliza frecuentemente de forma errónea para referirse a toda la infraestructura ofrecida por el proyecto Netfilter. Sin embargo, el proyecto ofrece otros subsistemas independientes de Iptables tales como el *connection tracking system* o sistema de seguimiento de conexiones, que permite encolar paquetes para que sean tratados

desde espacio de usuario. Iptables es un software disponible en prácticamente todas las distribuciones de Linux actuales (12)

Hay varios tipos de reglas dentro de ellas las tres de filtrado son las más utilizadas

- *INPUT*: reglas de filtrado para el tráfico entrante
- *OUTPUT*: reglas de filtrado para el tráfico saliente, pero que se implementan tras las transformaciones que se aplicadas
- *FORWARD*: reglas de tráfico para el tráfico saliente

1.3.4.2. Firewall Físicos.

Un firewall físico es un hardware específico con un sistema operativo que filtra el tráfico *TCP/UDP/ICMP/…/IP* y decide si un paquete pasa, se modifica o se descarta. A diferencia de los firewalls de Software estos suelen estar ya pre-configurados para su implementación

1.3.4.2.1. PfSense (Firewall).

Es una distribución libre de firewall de red, basado en el sistema operativo FreeBSD con un kernel personalizado e incluyendo paquetes de software libre de terceros para la funcionalidad adicional. PfSense software es capaz de proporcionar la misma funcionalidad o más de los servidores de seguridad comercial común, sin ninguna de las limitaciones artificiales (13)

PfSense es una aplicación que se instala como un sistema operativo ya que tiene varias funcionalidades entre estos servicios de redes LAN y WAN, con detalle estos servicios son los siguientes:

- Firewall: PfSense se puede configurar como un cortafuego permitiendo y denegando determinado tráfico de redes tanto entrante como saliente a partir de una dirección ya sea de red o de host de origen y de destino, también haciendo filtrado avanzado de paquetes por protocolo y puerto.
- Servidor VPN: PfSense puede configurar como un servidor VPN usando protocolos de tunneling tales como IPSec, PPTP, entre otras.
- Servidor de Balanceo de Carga: PfSense puede ser configurado como servidor de balanceo de carga tanto entrante como saliente, esta característica es usada comúnmente en servidores web, de correo, de DNS. También para proveer estabilidad y redundancia en él envió de tráfico a través del enlace WAN evitando los cuellos de botella.
- Portal Cautivo: Este servicio consiste en forzar la autenticación de usuarios en una página web especial de autenticación, para aceptar los términos de uso o para poder tener acceso a la red.

El portal cautivo es usado comúnmente para control de accesos a la red en los puntos de accesos inalámbricos de los hoteles, restaurantes, parques y kioscos.

- Tabla de estado: PfSense es un stateful firewall, el cual como característica principal guarda el estado de las conexiones abiertas en una tabla. La mayoría del firewall no tienen la capacidad de controlar con precisión la Tabla de estado. PfSense tiene un enorme número de características que permiten una granularidad muy fina para el manejo de la tabla de estado.
- Servidor DNS y reenviador de caché DNS: PfSense se puede configurar como un servidor DNS primario y reenviador de consultas de DNS.
- Servidor DHCP: También funciona como servidor de DHCP, se puede también implementar VLAN desde PfSense.
- Servidor PPPoE: Este servicio es usado por los ISP para la autenticación de usuarios que puedan ingresar a internet, por una base local o vía radius.
- Enrutamiento estático: PfSense funciona como un enrutador ya que entrega direccionamiento IP y hace el nateo hacia afuera.
- Redundancia: PfSense permite configurar dos o más cortafuegos a través del protocolo CARP (Common Address Redundancy Protocol) por si uno de los cortafuegos se cae el otro se declara como cortafuegos primarios.
- Reportes Y Monitoreo: A través de los gráficos PfSense muestra el estado de los siguientes componentes: Utilización de CPU y rendimiento total, estado del Firewall, rendimiento individual por cada interface, paquetes enviados y recibidos por cada interface, manejo de tráfico y ancho de banda. (13)

1.3.5. Modelo de acceso a Internet.

Compartir el acceso a Internet para una organización, más que una opción es una necesidad, bien sea por la falta de direcciones IP públicas para acceder a la red, o por razones de seguridad. Las dos soluciones más aceptadas para ofrecer este servicio son el uso de un servicio de traducción de direcciones de red (NAT), o la implementación de un servidor proxy.

1.3.5.1.NAT

La traducción de direcciones de red (NAT, Network Address Translation) también es conocida como enmascaramiento de IPs. Es una técnica mediante la cual las direcciones fuente o destino de los paquetes IP son reescritas, sustituidas por otras (de ahí el "enmascaramiento"). (4)

Esto es lo que ocurre cuando varios usuarios comparten una única conexión a Internet. Se dispone de una única dirección IP pública, que tiene que ser compartida. Dentro de la red de área local (LAN) los equipos emplean direcciones IP reservadas para uso privado y será el proxy el encargado de traducir las direcciones privadas a esa única dirección pública para realizar las peticiones, así como de distribuir las páginas recibidas a aquel usuario interno que la solicitó. (4)

Esta situación es muy común en empresas y domicilios con varios ordenadores en red y un acceso externo a Internet. El acceso a Internet mediante NAT proporciona una cierta seguridad, puesto que en realidad no hay conexión directa entre el exterior y la red privada, y así los equipos no están expuestos a ataques directos desde el exterior. (4)

Mediante NAT también se puede permitir un acceso limitado desde el exterior, y hacer que las peticiones que llegan al proxy sean dirigidas a una máquina concreta que haya sido determinada para tal fin en el propio proxy. (4)

1.3.5.2. Proxy

Es una solución software implementada en la capa de aplicación la cual intercepta los mensajes de solicitud HTTP (y otros protocolos), para hacer la solicitud en representación de los usuarios de la red corporativa. Generalmente un servidor proxy se ubica en la frontera entre la red corporativa y la red del proveedor de acceso a Internet (4)

El cliente realiza una petición de un recurso de internet, cuando este desea acceder a dicha información, es el proxy quien realiza la comunicación y traslada el resultado al equipo originario. Los Proxys pueden filtrar el contenido de las páginas Web servidas y bloquear contenido ofensivo. (4)

En la mayoría de los casos se añade la funcionalidad adicional de mantener los resultados obtenidos en una memoria caché que permite acelerar consultas coincidentes. Cuando el proxy caché recibe la petición, busca la URL resultante en su caché local. Si la encuentra, contrasta la fecha y hora de la versión de la página demanda con el servidor remoto. Si la página no ha cambiado desde que se cargó en caché la devuelve inmediatamente, ahorrándose de esta manera mucho tráfico pues sólo intercambia un paquete para comprobar la versión. Si la versión es antigua o simplemente no se encuentra en la caché, lo captura del servidor remoto, lo devuelve al que lo pidió y guarda o actualiza una copia en su caché para futuras peticiones (4)

Ventajas.

- Control: para limitar y restringir los derechos de los usuarios, y dar permisos sólo al proxy.
- Ahorro: Solo el proxy realizará el control de la red.
- Velocidad: Si varios clientes van a pedir el mismo recurso, el proxy, por medio del caché proporcionará una respuesta inmediata, porque guarda en memoria las peticiones que fueron solicitadas en un principio.
- Filtrado: El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.
- Anonimato: Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos

Desventajas

- Abuso: Al estar dispuesto a recibir peticiones de muchos usuarios y responderlas, es posible que haga algún trabajo que no corresponda. Por tanto, ha de controlar quién tiene acceso y quién no a sus servicios.
- Carga: Un proxy ha de hacer el trabajo de muchos usuarios.
- Intromisión: Es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el proxy.
- Incoherencia: Si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino.

Tipos de Proxy

- ***Web Proxy Cache***: Se dice que un servidor está actuado como Web Proxy caché cuando almacena en su disco duro las páginas Web descargadas de forma que, en próximas consultas, pueda acceder a ellas de forma muy rápida. De esta forma se optimiza el canal de acceso a Internet de la organización del usuario en momentos de ocupación importante de la línea (4)
- ***Proxy Inverso***: Un Proxy inverso (o reverse Proxy) es aquel que se sitúa cerca de uno o más servidores Web, de forma que es el Proxy quien recibe las peticiones de los clientes, las reenvía a los servidores Web Remotos y actualiza una copia en su caché para futuras peticiones (4)
- ***Proxy Transparente****:* Es posible usar un Proxy para aplicar políticas de control de acceso a Internet. Normalmente esta configuración no es transparente: es necesario modificar el cliente para que use el Proxy al acceder a Internet, de forma que es posible que un usuario modifique esta configuración (4)

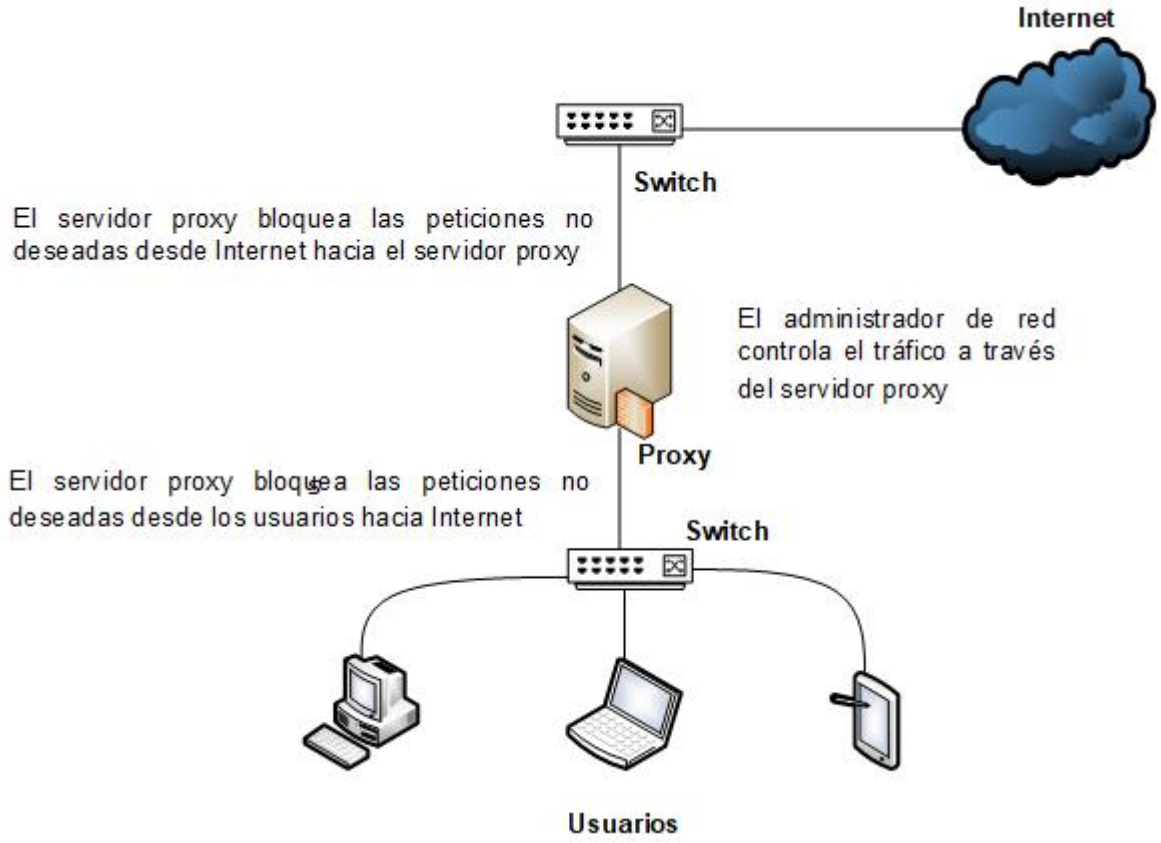


Figura 2. Funcionamiento de un servidor proxy. Fuente: Creado por el autor

1.3.6. Squid.

Squid es el software para servidor proxy más popular y extendido entre los sistemas operativos basados sobre UNIX®. Es muy confiable, robusto y versátil. Al ser software libre, además de estar disponible el código fuente, está libre del pago de costosas licencias por uso o con restricción a un uso con determinado número de usuarios. (4)

Entre otras cosas, Squid puede hacer proxy y caché con los protocolos *HTTP, FTP, GOPHER y WAIS, Proxy de SSL*, caché transparente, caché de consultas DNS y otras muchas más como filtración de contenido y control de acceso por IP y por usuario. (4)

- **Proxy/caché**: Proporciona servicio proxy a peticiones del tipo http, https y ftp a equipos que se encuentran en nuestra red local para que puedan acceder hacia internet y a su vez provee la funcionalidad de caché en el cual se almacenan localmente las páginas consultadas por los usuarios de forma que incrementa la rapidez de acceso a la información web y ftp.

- ***Proxy SSL:*** Es un servicio de Squid compatible con SSL, con el cual se aceleran las peticiones y las peticiones hacia internet estarían cifradas.
- ***Jerarquías de Caché:*** Nuestro Squid puede pertenecer a una jerarquía de caché que trabajan conjuntamente sirviendo peticiones. En este caso tendremos varios servidores Squid resolviendo peticiones de una página web, si no la tiene registrada le pregunta a otro hasta que es encontrada la información Squid sigue los protocolos ICP, HTCP, CARP y caché digests que tienen como objetivo permitir a un proxy "preguntarle" a otros proxys caché si poseen almacenado un recurso determinado.
- ***Control de Accesos:*** En este parte establecemos reglas de control de acceso, esto permite establecer políticas de denegación o aceptación.
- ***SNMP:*** Permite activar el protocolo SNMP, esto permite la administración de red, que permite supervisar, analizar y comunicar información de estado entre una gran variedad de máquinas, pudiendo detectar problemas y proporcionar mensajes de estados.
- ***Caché de resolución DNS***: Squid está compuesto también por el programa dnsserver, que se encarga de la búsqueda de nombres de dominio. Cuando Squid se ejecuta, produce un número configurable de procesos dnsserver, y cada uno de ellos realiza su propia búsqueda en DNS. De este modo, se reduce la cantidad de tiempo que la caché debe esperar a estas búsquedas DNS. (4)

1.3.6.1. SquidGuard.

SquidGuard es un programa auxiliar que se incorpora a Squid en su función de crear listas de acceso (ACLs) para el bloqueo de sitios clasificados como prohibidos por su contenido. Las listas que utiliza este software son llamadas squidguard-blacklists las cuales tienen diferentes clasificaciones como sitios de juegos, malware, virus, etc. Hay dos grandes ventajas para SquidGuard: es rápido, gratis y se publica bajo la licencia pública de GNU

1.3.6.2. Sistema de Cuotas. Squish.

Squish es una aplicación realizada en *Perl* la cual permite establecer cuotas a los usuarios por diferentes categorías como son cuota por día, mes o año, así como en medida de datos *(B, MB, GB*,..).Esta herramienta lee las definiciones de las cuotas asignadas a cada usuario en un fichero de configuración y crea una base de datos *user.stor* en la cual en dependencia del tráfico generado por cada usuario y que registra los logs de squid va guardando la cuota gastada y a su vez crea un archivo con los que se sobre pasan la cuota asignada, este fichero es leído por squid el cual deniega la navegación.

1.3.7. Sistemas de análisis de logs de Squid.

1.3.7.1 Analizador Squid Analysis Report Generator (SARG).

Squid Analysis Report Generator (Sarg): Es una herramienta que permite conocer, toda la actividad de los usuarios y/o equipos incluidos en la red, registrada en los logs del proxy. Fue desarrollada con el lenguaje de programación C y es distribuida bajo la licencia GPL v2. Provee mucha información sobre las actividades de los usuarios de Squid: tiempo, bytes, sitios y otros. Este analizador brinda una variedad de información como: listados de sitios más visitados, reportes diarios, semanales y mensuales, gráficos semanales y mensuales del consumo por usuario/host, detalles de todos los sitios a los que entró un usuario/host y descargas (14).

1.3.7.2. WebSpy Analyzer Giga.

Es una herramienta de análisis para monitorear el uso de Internet. Esta herramienta permite una organización lógica de los datos usando alias y perfiles configurables. Importa las bitácoras generadas por los servidores de Proxy o firewalls de las empresas. Incluye tareas pre-programadas para «establecer y olvidar» análisis de datos. Utiliza los recursos de red existentes tal como Windows NT® User Groups. Además, analiza de manera eficientemente gran cúmulo de datos. También genera una variedad de informes personalizables en formatos comunes. (14)

1.3.7.3. SquidAnalyzer.

Analiza el archivo de logs de Squid y genera un reporte de estadísticas acerca de los sitios (URLs) visitados por cada usuario, desplegando un calendario donde el usuario puede seleccionar las estadísticas acerca de un día en específico. Además, se obtienen datos como los sitios más visitados durante un día, los usuarios que más navegan durante el día.

1.3.7.4. Lightsquid.

Lightsquid se trata de un conjunto de *cgi* y *scripts* en *Perl* que se despliegan en el servidor web, y aunque a priori no ofrezca una interfaz muy moderna y elegante, se trata de un buen aliado por rapidez y sencillez. Este lee los logs de squid y genera las trazas de cada usuaria e ip de donde realizó la petición. Permite establecer filtro como gráfica de consumo, horario de la petición (sólo en la hora no minutos).

1.3.7.5. AAInternet.

Aplicación realizada por Segurmática, la cual permite extraer información de los ficheros log de los servidores proxy, generar reportes gráficos de análisis de la navegación de los usuarios, donde pueden

observarse la fecha y hora de visita al sitio, los dominios o sitios Web visitados y la transferencia por usuarios, entre otros datos. Funciona sobre el sistema operativo Windows. Utiliza una base de datos creada a partir del procesamiento de archivos log del servidor proxy, para ello es necesario copiar manualmente hacia la estación donde está instalada esta herramienta los archivos log que se deseen parsear o a una estación dentro de la red donde sean accesibles estos archivos desde la estación donde se encuentra instalado AAInternet. (14)

1.3.7.6. SRNI.

El Sistema de Reportes de la Navegación por Internet (SRNI) es una aplicación web realizada en UCI, desarrollada bajo la tecnología Java y que utiliza como gestor de base de datos PostgreSQL. Debido a que es una aplicación web puede consultarse desde cualquier lugar de la UCI. El software brinda a los usuarios reportes dinámicos de su navegación, los cuales son creados a partir de las trazas del servidor proxy. La información de acceso que se puede consultar es por URL, dirección IP, días y horas. (14)

1.3.8. Ejecución de las tareas diarias. Crontab.

Crontab permite programar lo que se conoce como crones, esto es, tareas que se ejecutarán en un momento determinado de tiempo de manera automática. El sistema Linux (y cualquier Unix en general) comprueba regularmente, guiándose por el evento del reloj del sistema, si existe alguna tarea programada para ejecutarse y, en caso afirmativo, la ejecuta sin necesidad de que nadie (ningún usuario) lo haga explícitamente.

1.4. Conclusiones del capítulo I.

En este capítulo se ha presentado el soporte teórico-metodológico y las tecnologías que permitieron desarrollar dicha investigación. En el estudio de los antecedentes se comprobó que en Cuba no existe un proyecto de trabajo de culminación de estudios que proponga un sistema de navegación orientado a cumplir las políticas de informatización de un centro universitario. Se analizan los sistemas de navegación de amplia difusión en el mundo actual que utilizan soluciones de software libre y se comparan con las soluciones parciales ofrecidas en las diferentes instituciones pertenecientes al MES.

El estudio de las diferentes tecnologías utilizadas en los sistemas de navegación nos proveyó de criterios a aplicar en la selección de las herramientas a emplear en el desarrollo del Sistema de Navegación de la universidad de Matanzas. Basándonos en sistemas de virtualización, sistemas operativos y herramientas de código abierto y software libre se propone el sistema continuando las políticas de informatización cubana.

Capítulo II. Diseño de la solución propuesta.

Introducción.

En este capítulo se determina la situación actual en la que se encuentra la red de datos de la Universidad de Matanzas a través de la metodología antes descrita. Se realiza un informe sobre el estado del arte del Sistema de Navegación actual y la obtención de estadísticas sobre el uso del Internet y Red Nacional por parte de los usuarios de la red. Se determina la solución propuesta a través de los resultados antes descritos y las herramientas seleccionadas para ello.

2.2. Determinación de la situación actual.

Para determinar la situación actual primero se recopiló toda la documentación existente sobre la red y el Sistema de Navegación actual, para poder tener un criterio concreto del estado de situación y su funcionamiento.

2.2.1. Caracterización de la Red de Datos de la Universidad de Matanzas.

2.2.1.1. Topología de enlaces.

Actualmente la red de la Universidad De Matanzas está conformada por dos grandes sedes y un conjunto de subsedes universitarias ubicadas en los municipios de la provincia, las cuales son catalogadas en CUM y FUM. Las características geográficas de nuestro centro infieren un alto grado de heterogeneidad en cuanto a tipo de enlace, tecnología y ancho de banda utilizado.

Las dos Sedes Universitarias principales (Sede Juan Marinello y Sede Camilo Cienfuegos) se encuentran enlazadas mediante fibra óptica y es gestionado dicho enlace, por la Empresa de Telecomunicaciones de Cuba ETECSA. La velocidad de transferencia máxima contratada es de 10 Mbps/s y se utiliza una VPN creada para dicho enlace.

Las CUM/FUM se enlazan con la sede Principal (Sede Camilo Cienfuegos) utilizando enlaces ADSL que oscilan en función de la cantidad de PC e importancia de la sede, entre 128,256,512 y 1024 Kbps/s de velocidad máxima de transferencia. Dichos enlaces utilizan la VPN provincial dedicada a la Universidad de Matanzas, la cual es gestionada por ETECSA.

El Proveedor de Servicios (ISP) actualmente es el Ministerio de Educación Superior(MES) con el cual existe un enlace de 20 Mbps/s que utiliza el sistema de fibra óptica nacional. La conexión con nuestro ISP es dividida en dos servicios fundamentales: acceso a internet y acceso a la Red Nacional Cubana,

para lo cual se designa (de forma ministerial) valores entre 8 y 10 Mbps/s para Internet y de 10 a 12 Mbps/s para Red Nacional. (Las asignaciones del MES varían en función de las características del servicio y de las actividades que se desarrolla en los centros universitarios del país.)

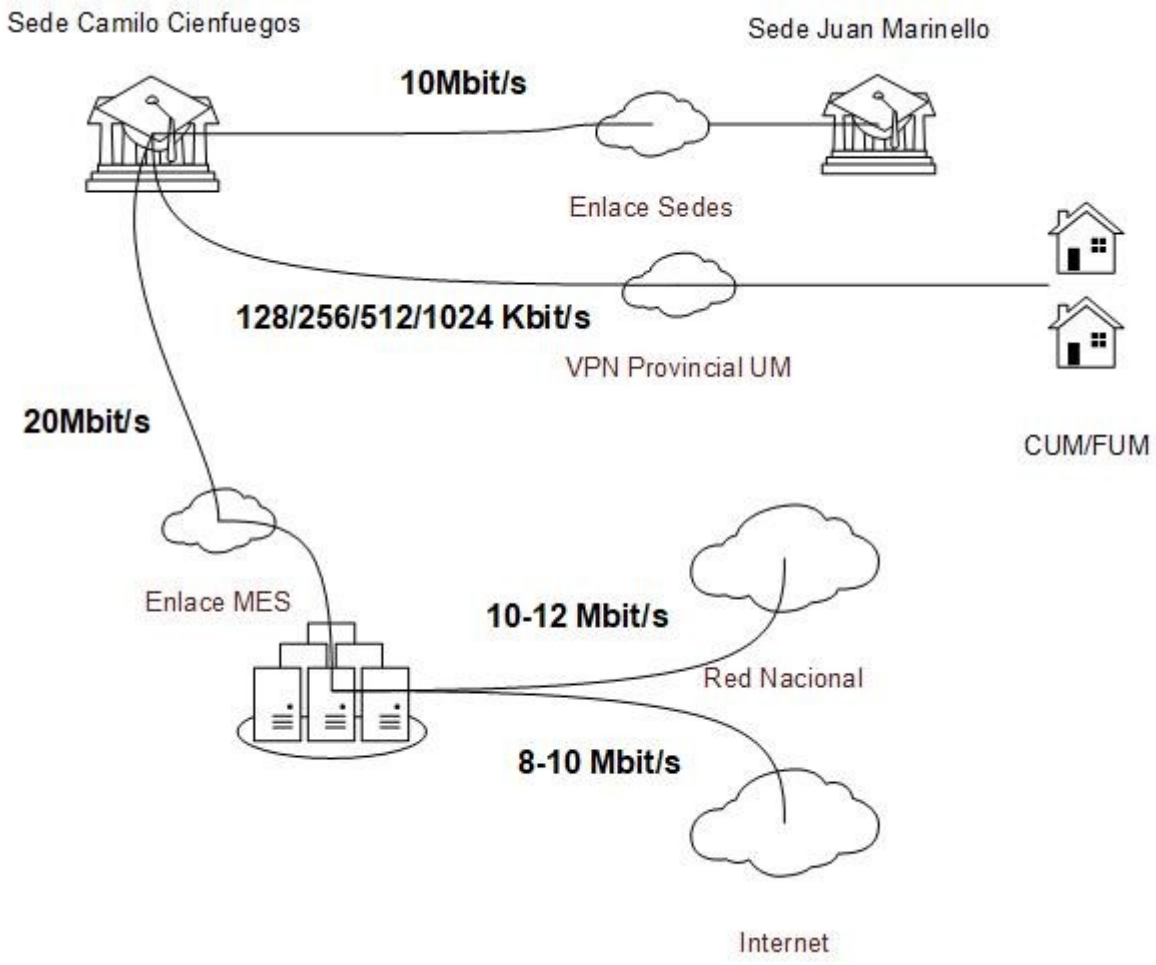


Figura 3. Enlaces de Datos Universidad de Matanzas. Anchos de Banda. Fuente: Creado por el autor.

2.2.1.2. Topología de Red.

El diseño original de la red de datos de la UM contemplaba una estructura de topología de árbol que se conformaba por una jerarquía de *modulador/demodulador, router, Switch Capa 3* (distribución) y finalmente los *Switch* de acceso, lo cual definía explícitamente las 3 partes que conforman una red de datos: Core (núcleo), distribución y acceso.

Con el deterioro de los equipos de telecomunicaciones originales y la migración hacia nuevas tecnologías como la fibra óptica, wifi, etc., se han implementado soluciones que alteraron la topología original. Actualmente se puede verificar que la topología de red corresponde más a una de estrella, pues

el sistema de rutas internas e interconexiones se realizan a través de un *Switch* central capa 3. Aunque existen router, tanto físicos como lógicos la mayor parte del proceso de routin lo realiza el Switch que originalmente realizaba el proceso de distribución

2.2.1.3. Direccionamiento IP.

El bloque de direcciones de ip privadas clase A asignados por el MES a nuestro centro es 10.34.0.0/15 lo cual representa un total de 131072 direcciones disponibles. El bloque de direcciones de ip públicas con que se dispone es 200.14.52.64/27 que permite el uso de 30 direcciones.

Internamente el proceso de direccionamiento incluye la división del bloque de direcciones privadas 10.34.0.0/15 en subredes de 1024 IP, las cuales delimitan las diferentes áreas de nuestro centro. Es por esto que la máscara de subred utilizada es 255.255.252.0.

2.2.1.4. Red inalámbrica.

La introducción de una nueva tecnología de acceso a provocado que se realicen cambios en el direccionamiento, la seguridad y los servicios. Con la inclusión de puntos de acceso wifi en nuestra red se han implementado soluciones que han transitado desde subredes independientes con acceso limitado hasta la actualidad que se cuenta con sistema de acceso inalámbrico donde se realiza un proceso de autentificación con el directorio de la Universidad de Matanzas.

2.2.1.5. Infraestructura Tecnológica.

Los equipos de comunicación en su mayoría cuentan con más de 15 años de explotación, pues el proceso actualización se ha realizado paulatinamente y de forma escasa. La característica de un enlace en su mayoría por fibra óptica provoca que para nuestro centro, ministerio y país sea muy difícil realizar cambios de tecnología que demanda nuestra red.

Los *switch* de acceso son en su mayoría *H*irschmann, *TP-Link* y *Allied Telesis*.El Switch de distribución es Hirschmann mientras que los router físicos utilizados fueron fabricados por Cisco por tanto utiliza un sistema operativo privativo (IOS). El equipamiento inalámbrico con el que se cuenta es en su totalidad TP-Link.

El equipamiento utilizado como servidor está formado en su mayoría por PCs de escritorio con las siguientes prestaciones:

- Servidores profesionales marca *Inspur* que han sido adquiridos recientemente
- Dos servidores marca *DELL* donados desde Italia

- Un servidor profesional marca DELL enviado desde el MES.

2.2.1.6. Información del Servidor Físico.

Se cuenta un servidor profesional con grandes características de rendimiento y almacenamiento idóneo en el cual se encuentra instalado un Servidor Proxmox v4.3 en el cual corren tres sistemas virtualizados Debian 8 quienes responden a:

- Servidor DNS de resoluciones internas a internet.
- Servidor Proxy-Internet.
- Servidor Proxy-Nacional

Por falta de recursos en el departamento en la prestación de servicios, este servidor está expuesto a la incorporación de más servidores virtualizados en correspondencia de los recursos que fueran necesarios ocupar para ello

Debido a la escasa preparación de los administradores de red encargados de estos servidores el Servidor Proxmox v4.3 se instaló en todo el disco físico de la máquina. Al ocurrir esto Proxmox realizó sus 2 particiones predeterminadas llamadas local y local-lvm donde:

Local: es donde Proxmox utiliza para sus ficheros de instalación, bakup, descarga de plantillas LXC, ISOS de sistemas operativos, entre otros.

Local-LVM: para crear los discos duros de los sistemas virtualizados y donde prácticamente no se pude realizar cambios

Al ocurrir lo anterior de un disco de 3TB Proxmox utilizó 100 GB para la partición local dejando prácticamente sin espacios para guardar datos principalmente de los backups. Al no contar con un servidor de respaldo NAS por pocos recursos y rotura del anterior, las salvas tenían que hacerse manual con un máximo de 2 por poco espacio, propiciando a que por olvido o problemas externos se perdieran los datos guardados, por lo que se tomó como medida guardar copias en las estaciones de los administradores encargados siendo en proceso tedioso y poco ético.

2.2.2. Recolección de datos sobre el Sistema de Navegación Actual.

2.2.2.1. Funcionamiento lógico.

Debido al gran uso de esa tecnología para la búsqueda de información, entretenimiento, servicios, comunicación, redes sociales, etc., la Universidad de Matanzas implementa un sistema para compartir la conexión de red dada por el Ministerio de Educación Superior hacia el resto de los nodos del país.

El método actual utilizado para lograr este fin es un Sistema de Navegación conformado por un conjunto de servicios de redes, entre ellos, la implementación de dos servidores proxy, uno para Internet y otro para Intranet Nacional. El servidor PfSense-Firewall que se encuentra entre los servidores remotos y los servidores *proxies* se encarga de hacer las traducciones NAT y permitir la salida de los puertos de navegación estándar o algún otro incluido necesario para la comunicación con recursos en la red externa y es el encargado de gestionar el ancho de banda para cada servidor en la red.

Las peticiones de los usuarios en sus diferentes subredes viajan a través de los dispositivos de interconexión de redes (*switch*), hacia el router principal, quien recibe todos paquetes enviados a la red de servidores desde otras subredes. Como el *proxy* de navegación está configurado de forma manual en los navegadores de los usuarios y no de forma transparente, las peticiones van directo al Proxy-Internet quien responde a la URL de configuración ***http://proxy.umcc.cu/proxy.pac.*** Como se aprecia al final de dicha URL se encuentra apuntando a un archivo **proxy.pac** quien tiene dentro de él una serie de configuraciones que permiten diferenciar si la petición va hacia los IPs o dominios del Canal ICT,.CU, Internet o si es UMCC.CU, este último al ser dominio interno no responde y deja pasar sin problemas.

También existe la forma de conexión a través de la dirección **ip: puerto** *(socket)* del proxy a utilizar. Pero esto provoca la equivocación por parte de los usuarios los cuales utilizando el Proxy-Internet tienden a navegar a sitios de la Intranet Cubana por lo que sus peticiones eran rechazadas o les consumía grandes cantidades de datos de su cuota de Navegación.

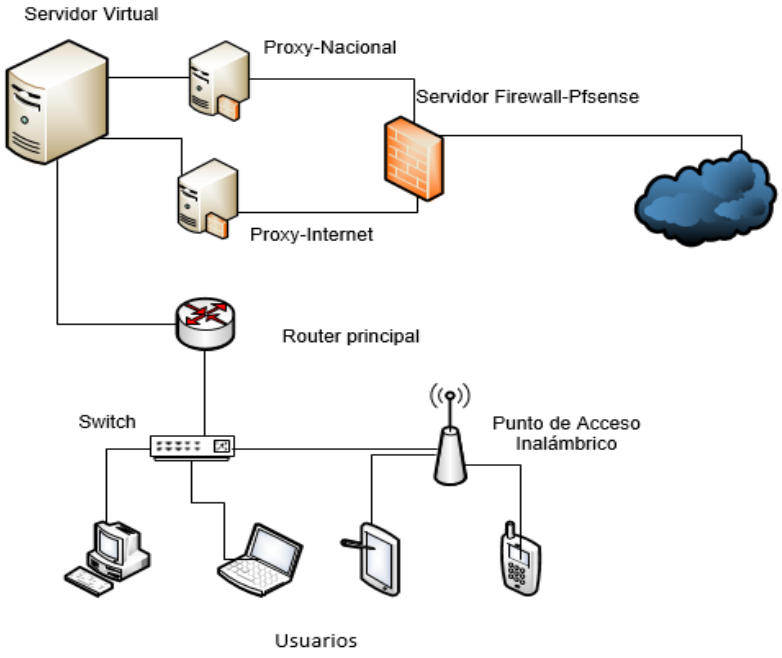


Figura 4. Funcionamiento del Sistema de Navegación actual. Fuente. Creado por el autor.

2.2.2.2. Herramientas implementadas.

Los dos *proxies* cuentan con versiones de squid 3.4 el cual autentifica con un servidor de dominio Active Directory mediante LDAP y a su vez importa los permisos que se le otorgan al dominio UMCC.CU.

Squid utiliza estas credenciales para otorgarles permisos de navegación por grupos de usuarios dependiendo de sus permisos, estos permisos pueden ser:

- Internet: permisos a internet en general.
- Redes Sociales: usuarios que tiene permiso a Redes Sociales a cualquier hora del día.
- Correo Externo: Usuarios que tienen permisos a correos como Gmail o Yahoo!
- Profesor: Usuarios que son profesores docentes.
- Informática: Usuarios de la carrera de Ing. Informática.

Existen problemas con estos permisos, principalmente en el otorgamiento de Redes Sociales a cualquier usuario por cualquier motivo y permisos de Profesor a usuarios que son trabajadores, pero no docentes.

2.2.2.2.1. Herramientas de revisión de trazas

Los dos *proxies* tienen implementado *Sqstat* como herramienta de monitoreo en tiempo real en la cual se pude observar datos como.

- Cantidad de usuarios conectados, ancho de banda consumido de forma en general por Squid. cantidad
- Qué usuarios está conectado.
- Cantidad de tráfico consumido por hilos y en general por cada usuario.
- Las URLs en las que se encuentra cada usuario.

El Proxy-Internet también tiene implementado la herramienta Lightsquid la cual genera reportes cada 10 min cada día de la semana y la cual se revisa diariamente para la verificación del cumplimiento de las políticas de navegación implementadas hasta el momento

El Proxy-Nacional no cuenta con ninguna herramienta que genere traza de navegación ya que se toma con poca importancia este canal en cuestiones de seguridad y solamente se guardan los logs por si ocurre algún incidente. Esto trae consigo que no se verifique si el proxy esté funcionando correctamente en cuestiones de acceso solo a Red Nacional y no a Internet, por lo que no se pudo detectar por cierto tiempo que estuvo propiciando conectividad a esta red.

2.2.2.3. Tratamiento de información sobre el uso del canal de Internet

En el reporte de SquidAnalyzer muestra las estadísticas de uso de Internet. Entre otras informaciones, se puede observar el uso de ancho de banda del canal mediante: dirección IP, cantidad de peticiones desde dicha IP, sitio web solicitado, cantidad de MB, cantidad de usuarios que se han conectado desde esa IP.

En las gráficas tomadas en los primeros 15 días del mes de mayo se observa el mal uso que los usuarios le dan al internet, navegando en páginas de descargas de contenido y que consumen grandes cantidades de tráfico como mega.co.nz, mediafare.com y descargas de YouTube (googlevideo.com), además se puede observar que existe navegación por IP el cual tiene un aproximado de 19 Gb consumo el cual viola una de las políticas actuales la cual prohíbe este tipo de navegación.

Estadísticas de red en 2018-05

Número de redes: 1177

Redes	Peticiones (%)	Mega bytes (%)	Duracion (%)	Throughput (MB/s)	Usuarios	El más largo	Url
10.34.104.12	46011 (2.16)	19,002.63 (9.15)	465:48:14 (0.99)	0.01	10	16,865.20	172.98.77.126:443
10.34.24.45	13509 (0.63)	15,557.75 (7.49)	448:06:21 (0.95)	0.01	2	293.58	oqfnwp.oloadcdn.net:443
10.34.42.4	10924 (0.51)	3,894.15 (1.87)	570:24:56 (1.21)	0.00	1	160.53	gfs270n155.userstorage.mega.co.nz:443
10.34.36.22	6501 (0.31)	3,508.62 (1.69)	115:19:13 (0.25)	0.01	3	161.59	gfs270n083.userstorage.mega.co.nz:443
10.34.50.7	3392 (0.16)	3,487.93 (1.68)	35:55:10 (0.08)	0.03	13	1,382.94	213.108.110.82:443
10.34.16.217	53299 (2.50)	3,448.46 (1.66)	1006:33:04 (2.14)	0.00	81	41.37	dw18.uptodown.com:443
10.34.32.22	51113 (2.40)	2,988.92 (1.44)	343:11:58 (0.73)	0.00	1	1,043.16	www.mediafire.com:443
10.34.41.8	9551 (0.45)	2,580.19 (1.24)	215:14:13 (0.46)	0.00	11	100.06	dw47.uptodown.com:443
10.34.41.11	13380 (0.63)	2,157.16 (1.04)	431:00:14 (0.92)	0.00	12	237.40	gsf-cf.softonic.com:443
10.34.32.47	31444 (1.48)	2,144.32 (1.03)	293:49:41 (0.63)	0.00	4	17.44	r3---sn-xuxjn5-i58e.googlevideo.com:443

Figura 5. Estadísticas del uso de Internet. Fuente: Generado por SquidAnalyzer

En el reporte generado de *URLs* solicitadas por los usuarios del centro, se observa que predominan dominios de Facebook (fbcdn.net,facebook.com) principalmente en imágenes (scontent-mia3-2.xx) y videos (video-mia3-2.xx) con un aproximado de 50 Gb solo en 15 días en un top de los 10 sitios más visitados.

En otros tipos de reportes se pudo observar que dominios de Mozilla, Opera y Windows (Update) se encontraban con más de 30 Gb de consumo por lo que se determinó que este tráfico era propiciado de actualizaciones SO Windows y de navegadores web.

scontent-mia3-2.xx.fbcdn.net:443	90688 (0.02)	21,323.06 (0.06)	3380:17:59 (0.03)	0.00	May 15 12:10:05
static.xx.fbcdn.net:443	89110 (0.02)	9,837.71 (0.03)	3098:22:05 (0.02)	0.00	May 15 12:10:06
www.msftconnecttest.com	73013 (0.02)	69.34 (0.00)	00:27:09 (0.00)	0.04	May 15 12:08:02
dl-ca2.driverscape.com	62222 (0.02)	104.98 (0.00)	07:30:27 (0.00)	0.00	May 11 13:39:08
ocsp.digicert.com	48984 (0.01)	42.71 (0.00)	08:26:49 (0.00)	0.00	May 15 12:10:43
wwwdl3.filescdn.net:443	35271 (0.01)	357.81 (0.00)	17:15:00 (0.00)	0.01	May 11 10:56:04
m.facebook.com:443	33638 (0.01)	3,147.98 (0.01)	1849:15:38 (0.01)	0.00	May 15 12:10:15
www.facebook.com:443	33170 (0.01)	7,426.22 (0.02)	1900:25:58 (0.02)	0.00	May 15 12:10:41
www.google.com:443	26442 (0.01)	3,315.90 (0.01)	1293:56:25 (0.01)	0.00	May 15 12:10:18
ocsp.pki.goog	23437 (0.01)	21.75 (0.00)	03:17:58 (0.00)	0.00	May 15 12:10:42
googleads.g.doubleclick.net:443	18084 (0.00)	314.24 (0.00)	876:55:31 (0.01)	0.00	May 15 12:10:32
facebook.com:443	15829 (0.00)	40.16 (0.00)	716:26:13 (0.01)	0.00	May 15 12:10:18
r3---sn-xuxjn5-i58e.googlevideo.com:443	15046 (0.00)	1,872.33 (0.00)	126:50:46 (0.00)	0.00	May 15 12:09:48
video-mia3-2.xx.fbcdn.net:443	14531 (0.00)	15,490.90 (0.04)	499:16:12 (0.00)	0.01	May 15 11:54:51

Figura 6. Estadísticas URLs más solicitadas en los primeros 15 días del mes de mayo. Fuente. Generado por SquidAnalyzer.

Es esencial obtener los dominios generales son los más solicitados en la entidad para poder comprobar que el Proxy-Internet es utilizado para dar uso del Internet y no de sitios cubanos. De esta forma se puede determinar que el ancho de banda para conexiones a Internet no es utilizado para la Intranet Cubana.

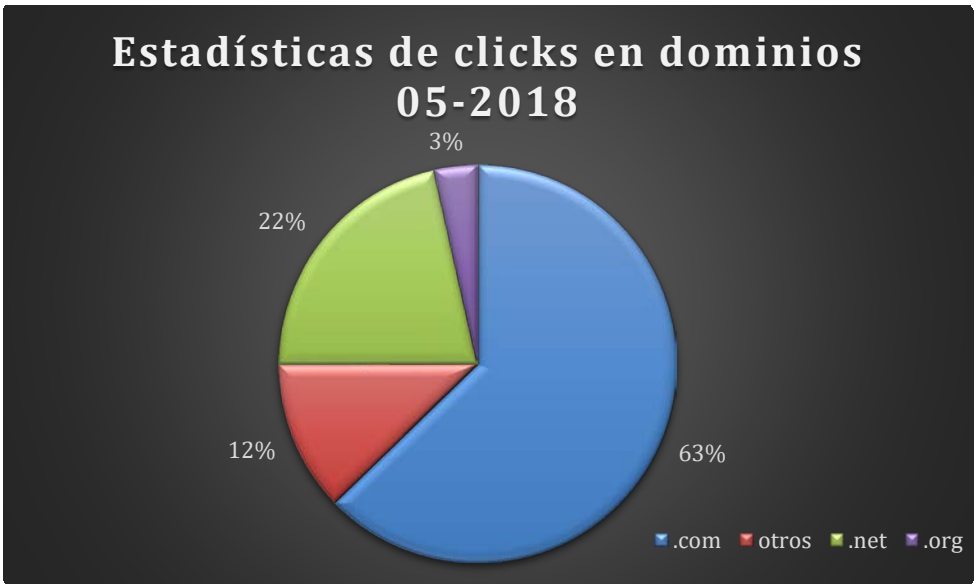


Figura 7. Estadísticas sobre los Dominios Generales más solicitados por los usuarios. Fuente. Generado por SquidAnalyzer.

En Figura 8 se puede apreciar en porciento los dominios más solicitados en la entidad en el mes de mayo, dando a conocer que la Red Social Facebook sobresale por encima de los demás con un 17% lo que demuestra una vez más el uso de la red para actividades de ocio. También existe un 4% en peticiones a dominios de Microsoft por lo que se debe revisar este tipo de tráfico y ver qué es lo que lo genera.

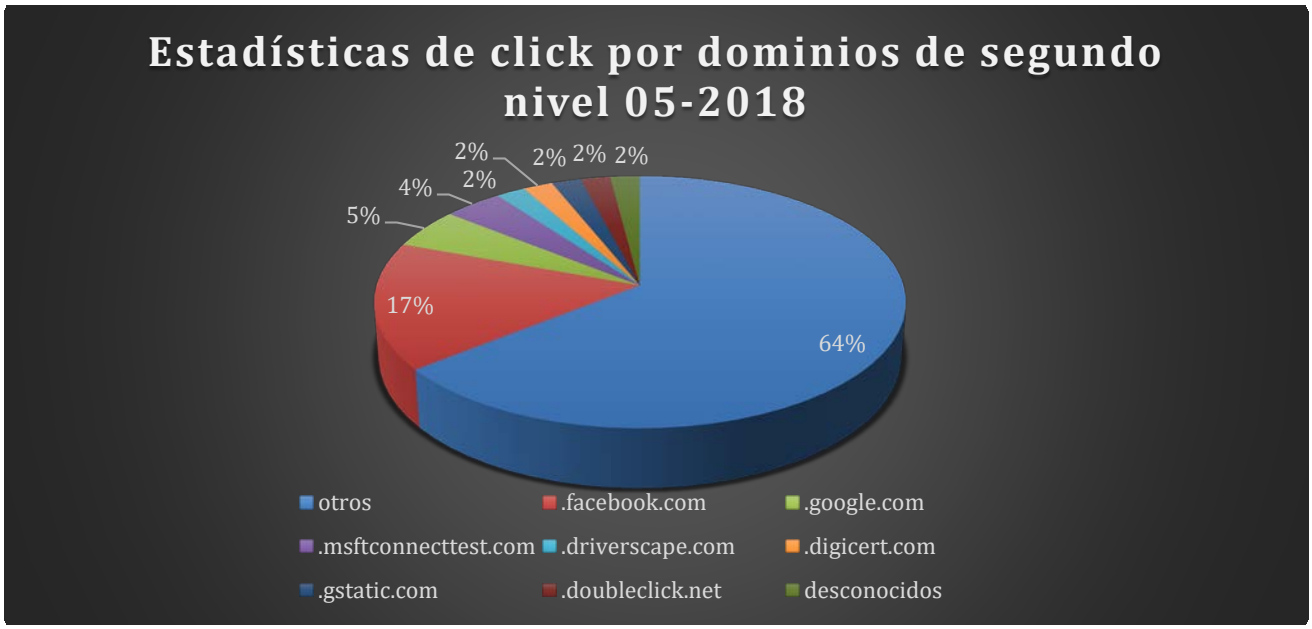


Figura 8. Estadísticas de dominios de segundo nivel más visitados en el mes de mayo. Fuente. Creado por el autor, recopilado de herramientas como Lightsquid y SquidAnalyzer.

Las próximas estadísticas demuestran que sitios de ocio y redes sociales son los que más datos de tráfico consumen en el centro. El consumo a Facebook es extremadamente grande para un centro de estudios y de investigación, el cual su ancho de banda y conectividad no es para este tipo de fin por lo que hay que determinar nuevas políticas de horario y gestión de tráfico, así como de permisos de acceso para este tipo de dominios.

Sitios de descargas como *Mega* el cual simula varios hilos de descarga, lo que conlleva a consumir más ancho de banda que cualquier otro sitio en tiempo real y que se encuentra entre los primeros dominios solicitados en la Universidad, debe ser gestionado con más cuidado principalmente ya que su funcionamiento de Nube en Internet e utilización de protocolos seguros como HTTPS delimita saber el contenido de la descarga.

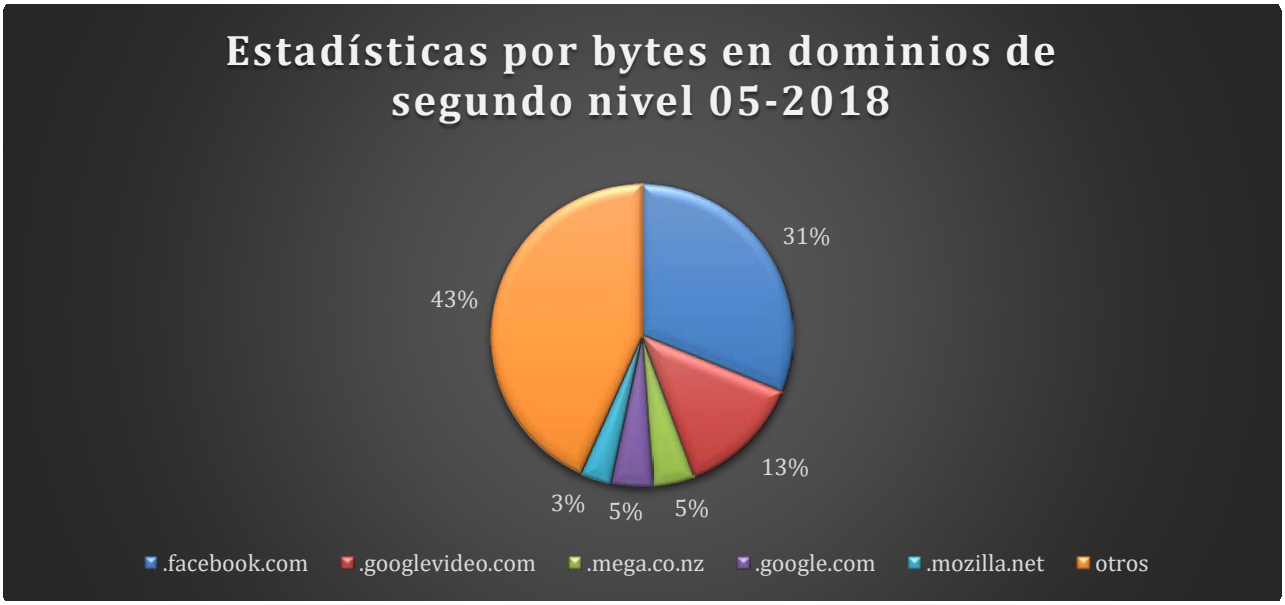


Figura 9. Estadísticas de bytes de consumo en dominios de segundo nivel en el mes de mayo. Fuente: Generado por SquidAnalyzer.

Saber el comportamiento de la red en cuanto a peticiones a internet es esencial para la administración de servicios por lo que conocer el ancho de banda que generan estas peticiones y en el horario que ocurren ayudar a comprender más a los usuarios de la red y de esta forma crear horarios que faciliten los procesos de la entidad

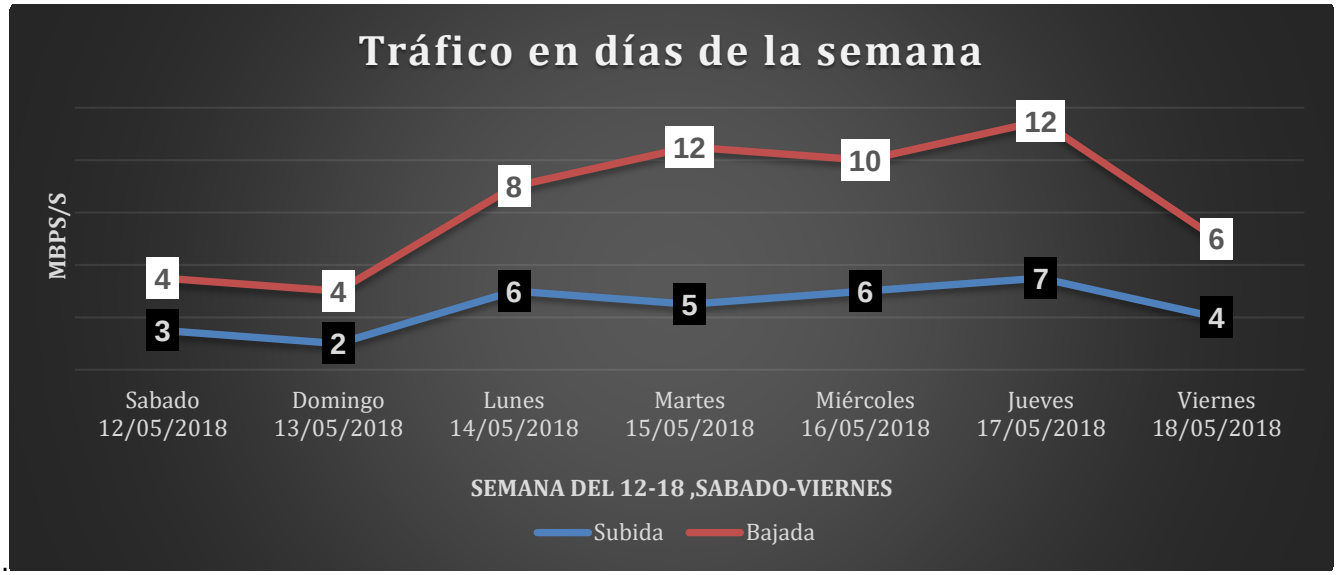


Figura 10. Comportamiento de ancho de banda a internet por día de la semana. Fuente: Creado por el autor de datos recopilados de gráficos generados por Proxmox

Es necesario conocer con más detalles el comportamiento del tráfico del servidor Proxy-Internet para de esta forma delimitar horarios del día en lo que se pueda gestionar de una mejor manera el ancho de banda asignado a dicho servicio. Al realizar varias comprobaciones con el servidor Proxmox se puede determinar con seguridad que el comportamiento de este proxy está en función de las actividades diarias del centro, además de seguir patrones de cambio debido a estas tareas también lo realiza debido a las configuraciones internas del propio servidor principalmente de las que determina Squid.

Se puede dividir el uso de la red en varios horarios como:

- **00:00-08:00**. Horario que es de madrugada y solo se encuentran activos aquellos usuarios en una PC de nuestro centro realizando peticiones automáticas al tener configurado el proxy.
- **08:00-12:00**. Horario de la mañana el cual comienza con un reinicio de las políticas de Squid y la conexión de la mayor cantidad de usuarios a la red, por lo que el tráfico aumenta de forma vertiginosa.
- **12:00-14:00.** Horario del mediodía y en el cual los usuarios se van desconectando para ir a almorzar por lo que el tráfico da un pequeño descenso.
- **14:00-17:00**. Horario de la tarde y el cual el tráfico vuelve a aumentar, aunque no tanto como en la mañana ya que gran cantidad de usuarios se retiran del centro.
- **17:00-00:00** solo se encuentra un pequeño grupo de estudiantes realizando tiempo de máquina en los laboratorios, aquellos conectados desde la Sede Juan Marinello o desde la **WIFI_UMCC.**

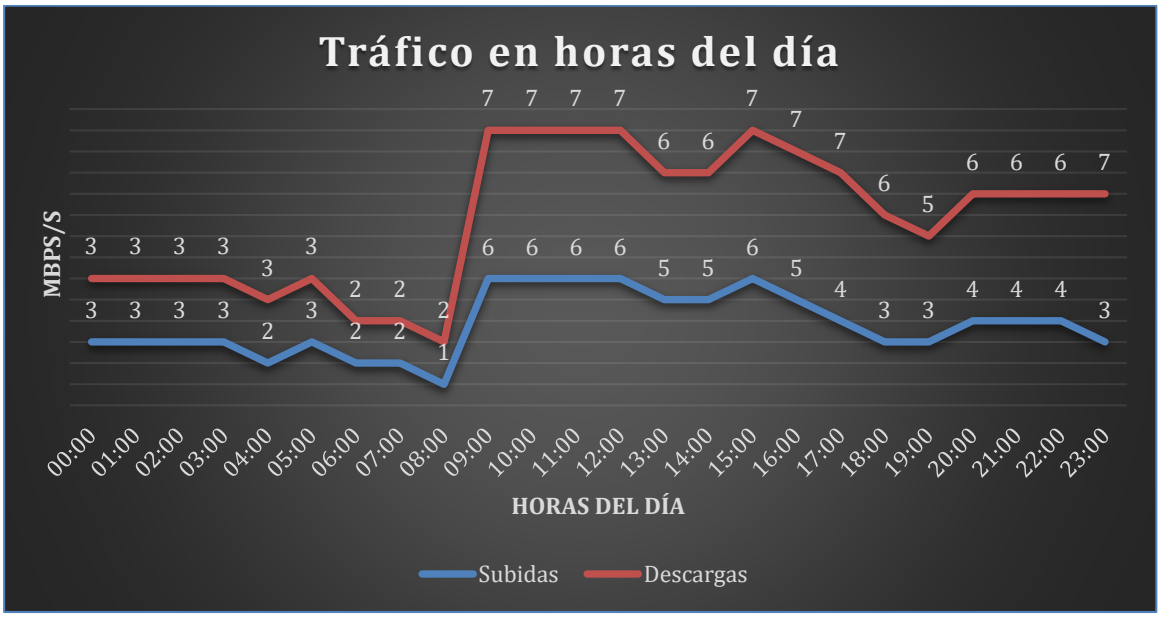


Figura 11. Tráfico aproximado en horas del día. Fuente. Creado por el autor, a partir de gráficos generados por Proxmox.

En la *Figura 12* se puede observar que en los días 14,15,16,17 y 18 de mayo pertenecientes a días laborables de lunes a sábado los usuarios aumentan en cierta cantidad, esto se debe también en parte a que la aplicación determina que un usuario que se conecte en el día en más de un IP contará como usuarios distintos. De esta imagen se pude determinar que los días con más usuarios y tráfico en la red son martes, miércoles y jueves.

Squid user access report
Work Period: May 2018

Calendar											
2016				2017				2018			
01	02	03	04	05	06	07	08	09	10	11	12

Date	Group	Users	Oversize	Bytes	Average	Hit %
18 May 2018	grp	775	407	29.8 G	39.3 M	1.52%
17 May 2018	grp	1240	592	41.4 G	34.2 M	1.60%
16 May 2018	grp	1372	642	46.2 G	34.5 M	2.07%
15 May 2018	grp	1281	460	32.2 G	25.7 M	2.77%
14 May 2018	grp	1114	557	34.3 G	31.5 M	2.16%
13 May 2018	grp	78	44	28.7 G	376.4 M	0.04%
12 May 2018	grp	212	131	24.1 G	116.4 M	1.28%
11 May 2018	grp	525	255	20.5 G	39.9 M	0.65%
10 May 2018	grp	1101	451	28.6 G	26.6 M	0.92%
09 May 2018	grp	1262	565	38.5 G	31.2 M	1.01%
08 May 2018	grp	612	265	19.0 G	31.8 M	0.58%
Total/Average:		870	397	343.1 G	71.6 M	1.33%

Figura 12. Comportamiento de cantidad de usuarios por día. Fuente: Generados por Lightsquid.

2.2.2.4. Tratamiento de información sobre el uso del canal de Red Nacional.

En el reporte de SquidAnalyzer muestra las estadísticas de uso de Red Nacional Cubana en el mes de mayo del 2018 ya que se necesitaban pruebas recientes por los constantes cambios que existen en esta red. Entre otras informaciones, se puede observar el uso de ancho de banda del canal mediante: dirección IP, cantidad de peticiones desde dicha IP, sitio web solicitado, cantidad de MB, cantidad de usuarios que se han conectado desde esa IP.

Se puede observar cual es el IP que más tráfico ha consumido en el mes y cuál URL fue la solicitada, dando a conocer que sitios de descargas de contenido son los más solicitados, dentro de ellos Softlib un sitio de software y 200.14.52.101 sitio perteneciente al MES el cual contiene series, películas, videos,

música, etc. Este último sitio es conocido como Medianet y es solicitado por los usuarios las 24h del día generando un ancho de banda que consume todo el canal nacional.

Número de redes: 1002

Redes	Peticiones (%)	Mega bytes (%) ▾	Duracion (%)	Throughput (MB/s)	Usuarios	El más largo	Url
10.34.16.65	7423 (1.06)	5,438.22 (6.84)	44:19:28 (1.08)	0.03	2	368.00	http://softlib.uclv.edu.cu/softlib/software
10.34.16.102	8609 (1.23)	5,251.81 (6.60)	50:35:53 (1.24)	0.03	4	339.49	http://200.14.48.101/medianet/peliculas/
10.34.0.129	1255 (0.18)	4,266.21 (5.36)	18:47:36 (0.46)	0.06	1	1,579.00	http://repos.uclv.edu.cu/isos/linux/mint/l
10.34.16.63	3275 (0.47)	4,241.19 (5.33)	53:04:47 (1.30)	0.02	1	298.63	http://softlib.uclv.edu.cu/softlib/software
10.34.16.200	2661 (0.38)	3,937.90 (4.95)	40:15:15 (0.98)	0.03	2	601.54	http://200.14.48.101/medianet/peliculas/
10.34.16.154	19825 (2.84)	3,929.64 (4.94)	16:25:06 (0.40)	0.07	4	105.22	http://ftp.mes.edu.cu/1-biblioteca%20digi
10.34.32.33	3649 (0.52)	3,161.92 (3.97)	04:10:55 (0.10)	0.21	1	347.23	http://debian.uci.cu/debian/pool/main/t/
10.34.16.15	3997 (0.57)	2,838.62 (3.57)	27:47:38 (0.68)	0.03	2	27.12	http://200.14.48.101/medianet/peliculas/
10.34.52.15	1720 (0.25)	2,812.86 (3.54)	14:39:36 (0.36)	0.05	5	614.07	http://ftp.mes.edu.cu/1-biblioteca%20digi
10.34.8.147	619 (0.09)	2,666.12 (3.35)	22:35:50 (0.55)	0.03	1	41.36	http://200.14.48.101/medianet/series/blu
10.34.36.61	10186 (1.46)	2,365.37 (2.97)	54:32:20 (1.33)	0.01	2	181.51	http://softlib.uclv.edu.cu/softlib/drivers/i
10.34.16.170	4926 (0.71)	2,227.58 (2.80)	70:18:20 (1.72)	0.01	3	263.23	http://200.14.48.101/medianet/peliculas/

Figura 13. Top de redes con más tráfico en Mb en el mes de mayo 2018. Fuente: Generado por SquidAnalyzer.

Dentro de las URLs más solicitadas volvemos a encontrarnos con Medianet con un total de 15 Gb en 21 días, sitios de FTP tanto del MES, la UCLV y UPR, así como sitios de repos de software libre tanto de la UCI o Joven Clubs.

Url	Peticiones (%)	Mega bytes (%) ▾	Duracion (%)	Throughput (MB/s)	Última visita
200.14.48.101	2265 (0.00)	15,007.02 (0.32)	109:59:57 (0.01)	0.04	Nov 21 07:41:44
ftp.mes.edu.cu	26059 (0.04)	8,364.25 (0.18)	20:35:32 (0.00)	0.11	Nov 21 08:35:26
mochila.cubava.cu	14580 (0.02)	8,302.58 (0.18)	189:49:30 (0.01)	0.01	Nov 20 22:28:59
softlib.uclv.edu.cu	4369 (0.01)	7,493.16 (0.16)	52:26:04 (0.00)	0.04	Nov 21 08:10:00
www.google.com.cu:443	46715 (0.08)	6,903.69 (0.15)	1962:31:16 (0.12)	0.00	Nov 21 09:52:24
debian.uci.cu	2553 (0.00)	3,410.75 (0.07)	01:44:41 (0.00)	0.54	Nov 21 09:25:37
download.jovenclub.cu	4618 (0.01)	2,799.38 (0.06)	04:06:01 (0.00)	0.19	Nov 21 09:25:39
ubuntu.uci.cu	3020 (0.01)	1,528.09 (0.03)	00:32:08 (0.00)	0.79	Nov 21 06:10:29
ftp.upr.edu.cu	3452 (0.01)	1,137.38 (0.02)	11:42:43 (0.00)	0.03	Nov 20 15:49:23
jorgen.cubava.cu	7532 (0.01)	919.06 (0.02)	10:49:00 (0.00)	0.02	Nov 21 09:35:45

Figura 14. Top de URLs con más peticiones por consumo en Mb en el mes de mayo 2018. Fuente: Generado por SquidAnalyzer.

Saber la distribución por redes cubanas es de máxima importancia para así poder tomar medidas en cuanto a prioridad de conexión o saber si los enlaces a las diferentes universidades funcionan correctamente

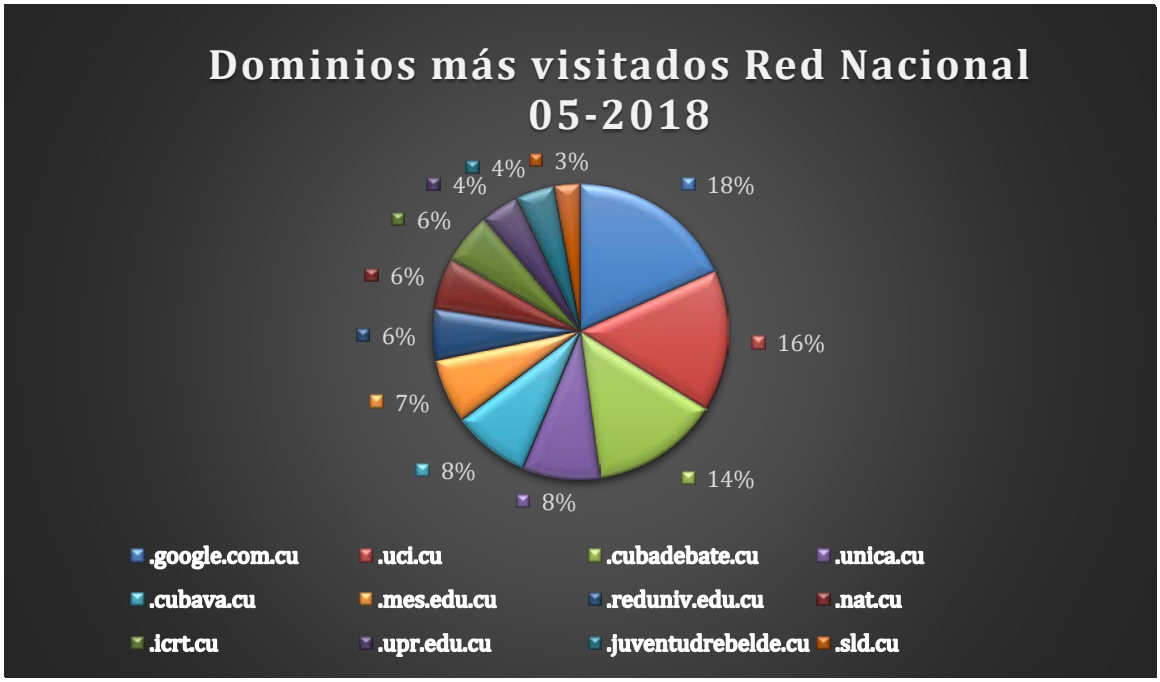


Figura 15. Dominios más visitados Red Nacional mayo 2018. Fuente. Creado por el autor de datos recopilados de SquidAnalyzer.

El tráfico máximo que puede gestionar el Proxy-Nacional está comprendido entre 10 y 12 Mbps/s ya que al tener un canal de 20 este hay que compartirlo entre los dos proxys, ya que si se establecen los 20 Mbps/s para Red Nacional consumirá todo el tráfico y no se podrá utilizar Internet.

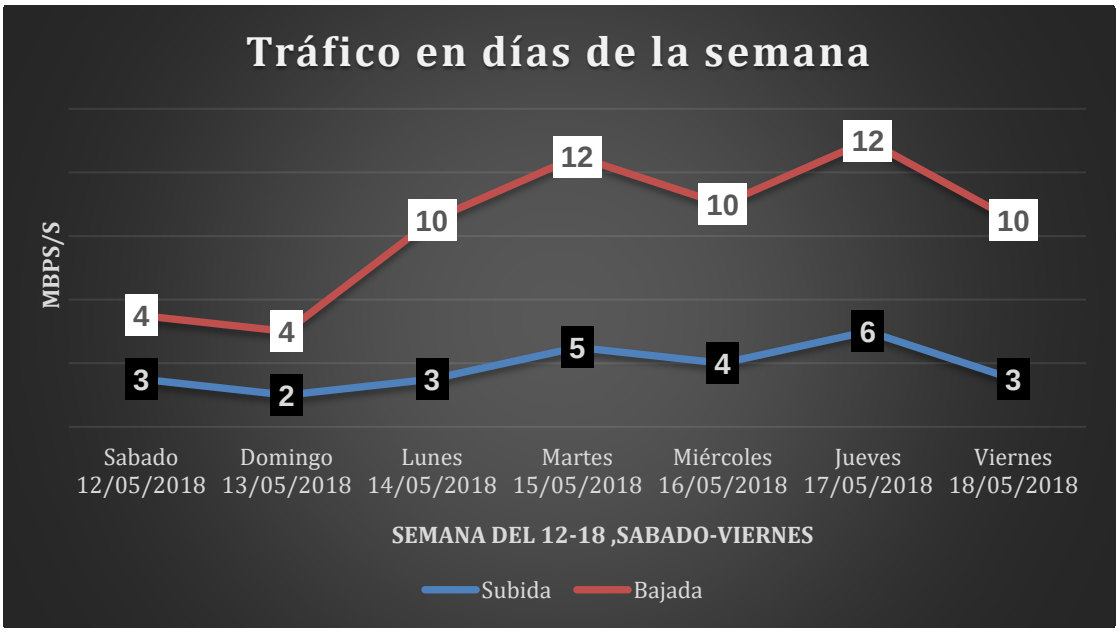


Figura 16. Comportamiento de ancho de banda a Red Nacional por día de la semana en horario laboral. Fuente: Creado por el autor de datos recopilados de gráficos generados por Proxmox

Lo anterior descrito se me mejor gestionado más adelante (Ver *Figura 17*) con el comportamiento en las horas del día, ya que es muy poco probable que exista tráfico que consuma los 20 Mbps de enlace, por ser compartido con Internet

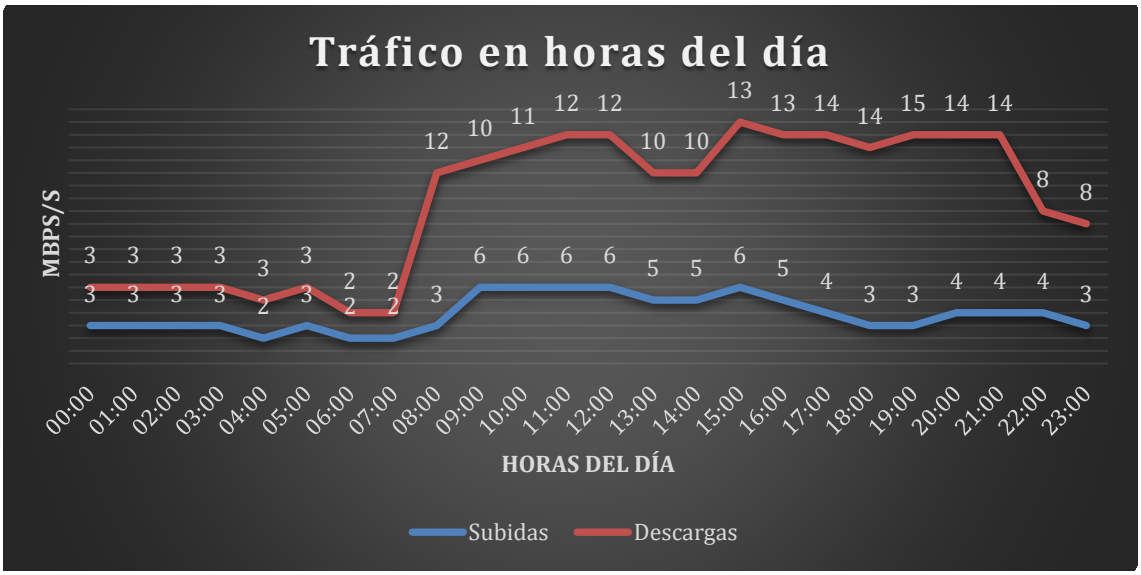


Figura 17. Tráfico aproximado en horas del día Red Nacional. Fuente. Creado por el autor, a partir de gráficos generados por Proxmox

2.2.3. Políticas del uso de los recursos de red en la Universidad de Matanzas.

Las políticas que se detallan a continuación cumplen con el escenario vigente de la red de datos institucional y la información ha sido recolectada del Departamento de Redes de la Universidad de Matanzas, y corresponden a la gestión que desarrolla el administrador de Redes de la institución.

2.2.3.1. Políticas sobre el uso de los servicios de la red

- Todos los servicios que presta la universidad a su personal administrativo y estudiantil, se encuentran alojados en servidores dentro del Nodo Central junto al Departamento de Redes excepto aquellos que pertenecen a la Sección de Seguridad Informática.
- Cada servidor debe ser administrado por el personal capacitado.
- El acceso a la administración de los servidores es restringido y exclusivo de quien lo administra.
- Se debe respaldar la información dos veces a la semana.

2.2.3.2. Políticas de acceso a internet.

- Autenticación contra el Active Directory y obtención de los permisos otorgados por la administración del centro.

- Sitios nacionales e sitios de investigación del canal ICT redireccionados a través del archivo **proxy.pac** hacia el Proxy-Nacional.
- Archivo proxy.pac muestra los IPs de los proxies lo que proporciona un fallo de seguridad.
- Denegación a través de SquidGuard de los dominios que se encuentre entre sus clasificaciones antes descritas.
- Denegación a las cuentas de usuario que se conecten por más de un IP al mismo tiempo.
- Autentificación obligatoria con una petición automática desde el servidor si el usuario no usa el sistema en 30 minutos.
- Creación de dos horarios utilizados para la restricción de ancho de banda y control de acceso.
    - Horario Laboral de 8:00-15:30
    - Horario No Laboral 15:30-8:00
- Denegación a los usuarios que consuman su cota de Internet excepto sitios de investigación como.ebscohost.com o .ebrary.com, entre otros.
- Cuota básica de Internet de 500 Mb
- Denegación a través de ACLs a las URLs de Correo Externo (Gmail, Yahoo!) a los usuarios que no tengan esos permisos.
- Denegación a través de ACLs a las URLs de Redes Sociales a los usuarios que no tengan esos permisos en Horario Laboral
- Denegación a través de ACLs a la navegación por IP.
- Denegación a través de ACLs al dominio interno .CU, es direccionado al Proxy-Nacional.
- Denegación a través de ACLs a descargar archivos mp4, mpg, avi, iso, exe, etc., en Horario Laboral.
- Denegación a través de ACLs a las URLs que pueden contener virus, pornografía, violencia, spam, subversión, proxies anónimos, etc.
- Denegación a través de ACLs a los laboratorios de la carrera de Ingeniería Informática a aquellos usuarios que no tenga el permiso de Informática en el Active Directory.
- Control de ancho de banda.
    - Redes Sociales 512 Kbps/s para toda la entidad
    - Formatos 256 Kbps/s para toda la entidad.
    - El resto no es controlado.
- Tamaño de caché de solo 16 GB.
- Tiempos de refrescos de caché de 1 a 3 días.
- Pocos formatos de archivos para ser cacheados.

2.2.3.3. Políticas de acceso a Red Nacional.

- Autentificación contra el Active Directory.
- Denegación a las cuentas de usuario que se conecten por más de un IP al mismo tiempo.
- Autenticación obligatoria con una petición automática desde el servidor si el usuario no usa el sistema en 30 minutos.
- Permite acceso solo a dominios .CU. IPs pertenecientes al Bloque de direcciones del canal Nacional.
- Redirección al proxy ICT perteneciente al MES de los sitios de Investigación de dicho proyecto.
- Tamaño de caché de solo 16 GB.
- Tiempos de refrescos de caché de 1 a 3 días.
- Pocos formatos de archivos para ser cacheados.

2.2.3.4. Responsabilidad del administrador de la red

- El administrador de la red tiene la responsabilidad de mantener la conectividad hacia Internet y Red Nacional.
- Debe definir y documentar claramente los niveles de autorización y privilegios de acceso de los usuarios hacia los recursos de la organización.
- Monitorear cualquier actividad relacionada con los activos de la organización.
- Monitorear cualquier actividad relacionada con la seguridad del servidor y las políticas de navegación.
- Tener contacto apropiado con las autoridades relevantes, por ejemplo, la organización puede necesitar de terceras personas como grupos de interés y profesionales en el área de seguridad.
- La información podría ser expuesta por grupos externos por lo que se podría tomar en consideración del administrador utilizar acuerdos de no-divulgación.

2.2.3.5. Responsabilidades de los usuarios de la red

- El usuario es responsable de mantener sus contraseñas en secreto.
- El usuario es responsable del uso y acceso a los servicios de la red Universitaria.
- No proporcionar datos personales por medio de correo o teléfono.
- Se prohíbe la excesiva o abusiva navegación por Internet con fines extra laborales.
- Se prohíbe la transmisión de información confidencial a personal que no labore en la Universidad.

- ❖ Los usuarios deben tener conciencia sobre las responsabilidades y problemas que comprenden la seguridad de la información.
- ❖ Los usuarios tienen la responsabilidad de reportar eventos que pongan en riesgo los activos de la organización.

2.2.3.6. Políticas y reglas Iptables

- ❖ Se aceptan todo tráfico que se origina en la interfaz de l*oopback*, esto permite procesar tareas que se originan en el sistema.
- ❖ Se permite tráfico con destino al puerto SSH solo desde la red administrativa.
- ❖ Se permite tráfico con destino al puerto 80 HTTP solo desde la red administrativa e IP del administrador principal en la Sede “Juan Marinello”
- ❖ No se permite el tráfico ICMP (ping) desde ningún IP.
- ❖ Se acepta tráfico con destino al puerto 3128 desde la red universitaria.

2.3. Solución propuesta.

Debido a que existen dos tipos de enlaces hacia diferentes nodos de red como Internet y Red Nacional se determinó que el Sistema de Navegación propuesto contará con dos Proxy como en el sistema actual ya que es una buena práctica diferenciar los canales y así tener un mejor control del uso de la red. Por tanto, los dos proxies tendrán prácticamente las mismas características diferenciándolos en algunas que serán especificadas más adelante

2.3.1. Virtualización.

Muchas universidades o empresas se trasladan a soluciones de software libre para los costos de su implementación y la obtención del pleno acceso a sus funcionalidades. En el caso de los sistemas virtualizados es necesario para tener un entorno virtual flexible, fácil de trabajar y entender.

En definitiva, las opciones de VMWare y Proxmox son prácticamente igualmente positivas, pero resulta esencial contar con una infraestructura única que relacione a todos los involucrados, soluciones rápidas eficientes que puedan comunicarse entre ellas.

Como resultado del proceso de investigación y prueba, tomando como base varias herramientas muy utilizadas en la actualidad, se decidió implementar Proxmox VE, que ha cumplido con los puntos más importantes y críticos a la hora de la selección.

¿Por qué Proxmox?

La mayoría de los productos de virtualización tienen un alto costo o su modelo de licenciamiento lo basan en la cantidad de equipos instalados, cantidad de sockets, etc. Esto no ocurre con Proxmox puede ser instalado en cualquier cantidad de máquinas libre de licencias o suscripciones obligatorias. Toda su documentación es accesible, así como su repositorio oficial. Esto no ocurre con VMWare quien tiene recursos prohibidos para nuestro país y tener que crearse una cuenta para obtener una licencia por 3 meses para su uso.

Se utilizará la última versión publicada hasta la fecha Proxmox v.5.1, con fecha de salida 24.10.2017. Basado en Debian Stretch 9.2, con Kernel 4.13.3 y LXC actualizado a 2.1.

Se utilizará LXC como forma de virtualización, por su fácil instalación y su gran funcionamiento, ahorrando recursos para compartir entre otros servidores virtualizados que estarán corriendo en el mismo nodo.

2.3.2. Sistema Operativo.

Se utilizará el sistema operativo Debian por ser un sistema estable y práctico, siendo el número uno en servidores y cuenta con el apoyo de los administradores de redes del centro por experiencia en trabajos anteriores. Tomaremos la plantilla basada en Debian 9.3.1 última versión de SO ya que resuelve varios problemas comparada con la versión actual implementada Debian 8.5.

2.3.3. Sistema de Autenticación y Permisos de Dominio. LDAP/Active Directory.

Se utiliza LDAP/Active Directory propiciado en Windows Server 2016 como único método de autentificación, este servicio es el que brinda la información sobre los permisos que debe tener cada usuario por lo que las políticas de navegación deben estar en correspondencia con los permisos que solicita el usuario al crearse la cuenta, y la cual está respaldada por una planilla firmada por el solicitante y quién autoriza sus permisos.

2.3.4. Políticas de seguridad del Servidor.

Se utilizará *Iptables* de forma personalizada (Ver Anexo 5) dentro del servidor virtualizado Debian para aplicar las políticas internas en aceptación de peticiones desde el resto de la red local universitaria.

La salida del servidor hacia la red externa será controlada por el servidor PfSense, el cual mediante sus reglas aplicadas a la Red LAN dará acceso mediante el protocolo TCP y UDP destino ANY por los principales puertos utilizados por los protocolos que utiliza un proxy Squid.

La Política Restrictiva será la utilizada para todas las políticas de seguridad de la solución dada, ya que es más difícil permitir tráfico peligroso por error, que mientras con la *Política Permisiva* es posible que no se haya contemplado algún caso de tráfico peligrosos y sea permitido por defecto.

2.3.5. Gestión de Ancho de Banda.

La herramienta *Traffic Shaping* es la que controla el ancho de banda asignado al centro el cual tiene diferentes reglas para los distintos servidores en red**.** La división de ancho de banda asignado para cada servidor debe ser fijo, pero esto no siempre es así ya que en momentos del día pude ser utilizado con otros fines, como una actualización de emergencia o instalación de algún servicio en la red. La responsabilidad de los cambios en el ancho de banda cae sobre el Jefe de Redes quién decide que cambios debe de realizar en función de mejorar los servicios, en caso de que el cambio sea por varias horas debe ser informado a la Sección de Seguridad Informática y a la comunidad universitaria.

2.3.6. Rotación y retención de logs en línea.

Se hará uso script Shell personalizado el cual guardará los logs de Squid todos los días a las 00:10 am los guardará por fecha y en formato comprimido. Le será guardado una copia en los servidores de Seguridad Informática y en un Servidor de Respaldo del Dpto. de Redes incorporando una partición NFS en los servidores.

2.3.7. Respaldo y recuperación.

Se generará un procedimiento de respaldo de los archivos de configuración y de los datos contra un servidor Linux en particular, para luego generar un procedimiento de recuperación parcial o total del sistema

2.3.8. Registros y estadísticas de navegación

Una vez que se otorgue el permiso de tráfico cada usuario estará sujeto a las políticas de acceso definidas a través de las ACLs de Squid y SquidGuard, generando los reportes de utilización por medio del software Lightsquid y SquidAnalyzer, el cual se realizará en cada uno de los dos proxys. Se utilizará Sqstat en cada uno de los servidores para la navegación en vivo y Squish para ver el tráfico en cantidad de datos por usuarios. Los reportes son visibles con Apache2.4 vía Web, mediante la creación de host virtuales para cada herramienta antes mencionada.

2.4. Squid como servidor proxy. Definiciones Avanzadas.

2.4.1. Estructura y funcionamiento.

La estructura de Squid está compuesta por un programa servidor principal, llamado Squid, un programa de resolución de Nombres de Dominio (DNS), dnsserver, algunos programas opcionales para reescribir peticiones y funciones de autenticación, y algunas herramientas de administración de clientes. Cuando Squid se inicia, éste genera un número configurable de procesos dnsserver, cada uno de ellos puede resolver un único y bloqueante petición DNS. Esto reduce la cantidad de tiempo que la petición DNS espera en la caché.

La configuración de Squid es realizada mediante la asignación de valores a un número cercano a 200 directivas en un archivo de configuración similar al de otros servicios en sistemas tipo Unix. La mayoría de estas directivas tiene un valor asignado por defecto; sin embargo, es necesario ajustar algunos de estos valores para tener un servidor Squid operando con una configuración básica.

Directivas de Squid se pueden agrupar en siete categorías, de acuerdo con sus características.

- Un primer grupo de directivas de identificación.
- Un segundo grupo establece el control de acceso básico.
- El tercer grupo establece el control de acceso avanzado.
- En cuarto lugar, las directivas de configuración básica de caché.
- En quinto lugar, la configuración avanzada de caché.
- Un sexto grupo dedicado al caché distribuido.
- Un grupo de directivas dedicado al control de ancho de banda.

2.4.1.1. Directivas de configuración básica de Squid.

- Parámetro **http_port:** Por defecto, SQUID utilizará el puerto 3128, aunque puede configurarse para que use cualquier otro, incluso varios puertos simultáneamente.
  # Default: http_port 3128

Squid no utiliza todos los recursos del equipo donde está instalado, sino que es necesario definir qué cantidad de memoria RAM y espacio en disco puede utilizar como máximo para la caché. Los parámetros por defecto son muy conservadores para evitar crear problemas iniciales en máquinas con pocos recursos, por lo que es lógico aumentarlos de acuerdo a los recursos disponibles.

- Parámetro **cache_mem**: Establece la cantidad de memoria RAM dedicada para almacenar los datos más solicitados.
  # Default: cache_mem 256 MB

- Parámetros **caches_swap:** Dentro del cache_swap, existen dos parámetros: **cache_swap_low cache_swap_hight** Con estos le indicamos a Squid que mantenga los niveles del espacio del área de intercambio o también conocido como swap. Estos parámetros vienen siempre desactivados por cual los buscaremos para activarlos**.** Con lo siguiente decimos al Squid que mantenga los niveles del espacio del área de intercambio entre 90% y 95%.
  #Default: cache_swap_low 90
  #Default: cache_swap_hight 95

- Parámetro**s maximum_object_size:** Utilizamos esta directiva para indicar el tamaño máximo para los objetos a almacenar en la caché.
  #Default: maximum_object_size 4 MB

- Parámetro**s maximum_object_size_in_memory:** tamaño máximo de los objetos cachéados en RAM.
  #Default: maximum_object_size_in_memory 512 KB

- Parámetro **visible_hostname:** Es el nombre del equipo
  #visible_hostname Nombre

- El espacio en disco reservado para almacenar los distintos objetos que se piden a través del proxy se define con la directiva cache_dir. La ubicación, formato y tamaño de este espacio en disco está definido por:
  #Default: cache_dir ufs /var/spool/squid3 100 16 256

El formato genérico de esta directiva es:
cache_dir tipo directorio Mbytes L1 L2

- Tipo. Tipo de sistema de almacenamiento a utilizar (ufs es el único que está definido por defecto en la instalación).
- Directorio. Ruta del directorio que se va a utilizar para guardar los datos del caché.

- Mbytes. Cantidad de espacio en disco en Megabytes que se va a utilizar para el caché. Si queremos que utilice el disco entero es recomendable poner aquí un 20 % menos del tamaño.
- L1. Número de subdirectorios de primer nivel que serán creados bajo directorio.
- L2. Número de subdirectorios de segundo nivel que serán creados bajo cada subdirectorio de primer nivel.

Puesto que el contenido de este directorio va a cambiar con frecuencia, es recomendable ubicarlo colocarlo en una partición separada por varias razones:

- La caché podría sobrepasar al resto del sistema de archivos o de la partición que comparte con otros procesos.
- Cuanto más cambie un sistema de archivos, mayores son también las posibilidades de que se encuentre dañado. Mantener la caché en una partición limita la parte de su sistema completo de archivos que resulta dañado.

Con esto establecemos el tamaño que deseamos que tenga la caché en el disco, se puede incrementar hasta el tamaño que desee el administrador por ejemplo 100 MB de caché con 16 directorios subordinados y 256 niveles cada uno.

- Parámetro **refresh_pattern** (factor para páginas sin caducidad): Permite especificar qué fecha en minutos deben de tener los documentos que su servidor no estableció una cabecera Expires indicando su caducidad.

Sus valores pueden ser: expresión regular mín porcentaje máx, tal como se muestra a continuación.

```
#refresh_pattern -i \.gif$ 14400 70% 43200
#refresh_pattern ^ftp: 1440 20% 10080
#refresh_pattern . 0 20% 4320
```

El valor correspondiente a la expresión regular debe de contener la especificación del objeto basándose en la dirección (URL) de la petición o un "." para indicar el resto. En los ejemplos se muestra como especificar cualquier objeto "gif" y cualquier petición "FTP".

El valor **mín.** corresponde a los minutos mínimos que un objeto que no dispone de una cabecera Expires (indicando su caducidad), pueda ser considerado como no caducado (fresco). El valor "0" se recomienda para que no se obligue la retención de objetos no deseados como pueden ser los dinámicos.

El valor **porcentaje** sirve para especificar en aquellos objetos sin fecha de caducidad, cuál será su fecha, aplicando un porcentaje sobre su tiempo desde la última modificación (la última modificación de un objeto se obtiene de la cabecera Last-Modified.

El valor **máx.** corresponde a los minutos máximos que un objeto podrá ser considerado como no caducado.

- Parámetros de **logs**

access_log: Especifica en que directorio se realizara el registro de accesos al Squid.

#access_log /var/log/squid/access.log squid

cache_log: Aquí es donde va la información general sobre el comportamiento del squid sobre la caché.

#caché_log /var/log/squid/caché.log

cache_store_log: Registra las actividades del administrador de almacenamiento. Muestra qué los objetos son expulsados de la memoria caché, y qué objetos son guardado y por cuánto tiempo.

#cache_store_log /var/log/squid/store.log

2.4.1.2. Control de acceso.

Una de las funciones principales de Squid es controlar el acceso de los equipos de la red local a otras redes y es posible realizar esto a través de listas de control de acceso o ACL. También es posible utilizar programas auxiliares como Dansguardian o SquidGuard para estas funciones.

El procedimiento que se sigue es definir las distintas ACL y posteriormente se permite o deniega el acceso a una determinada función de la caché. La opción de configuración encargada es normalmente http_access, que permite o deniega al cliente el acceso a Squid.

Reglas ACLs: Una ACL es una definición de control de acceso para squid, existen varios tipos de reglas ACL como: **src, time, dst, url_regex, srcdomain, urlpath_regex, dstdomain, url_regex, proxy_auth,** entre otras.

Las ACLs se definen como:

#acl [nombre] [tipo] [lista o dirección del archivo lista]

Control de Acceso: El control de acceso define si se permite o deniega el acceso a las reglas para que empecemos a crear el filtrado. Nomenclatura:

http_access allow/deny [Regla]

Dentro de la configuración http_access, existe una expresión "!" que significa no, esto permite que una regla se permitida o denegada. Es lo contrario a la primera definición del control de acceso.

Nota: Hay que tener en cuenta que la lectura se realiza de arriba a abajo y que Squid deja de leer líneas de **http_access** en cuanto encuentra una que aplicar.

2.4.1.3. Algoritmos Utilizados Por Squid para Política de reemplazo de Caché.

A través de un parámetro (cache_replacement_policy) Squid incluye soporte para los siguientes algoritmos para el caché:

- **LRU (Least Recently Used)** que traduce como Menos Recientemente Utilizado. En este algoritmo los objetos que no han sido accedidos en mucho tiempo son eliminados primero manteniendo siempre en el caché a los objetos más recientemente solicitados. Ésta política es la utilizada por Squid de modo predefinido.
- **LFUDA (Least Frequently Used with Dynamic Aging)** que se traduce como Menos Frecuentemente Utilizado con Envejecimiento Dinámico. En este algoritmo los objetos más solicitados permanecen en el caché sin importar su tamaño optimizando la eficiencia (hit rate) por octetos (Bytes) a expensas de la eficiencia misma, de modo que un objeto grande que se solicite con mayor frecuencia impedirá que se pueda hacer caché de objetos pequeños que se soliciten con menor frecuencia.
- **GDSF (GreedyDual Size Frequency)** que se traduce como Frecuencia de tamaño GreedyDual (codicioso dual), que es el algoritmo sobre el cual se basa GDSF. Optimiza la eficiencia (hit rate) por objeto manteniendo en el caché los objetos pequeños más frecuentemente solicitados de modo que hay mejores posibilidades de lograr respuesta a una solicitud (hit). Tiene una eficiencia por octetos (Bytes) menor que el algoritmo LFUDA debido a que descarta del caché objetos grandes que se han solicitado con frecuencia.

2.4.1.5. Desempeño de Squid con respecto al sistema de archivos y al esquema de almacenamiento.

Squid ofrece una variedad de opciones en el proceso de instalación y configuración, especialmente relacionadas con el almacenamiento de los archivos en disco. Squid puede funcionar con cinco esquemas de almacenamiento: *ufs*, *aufs*, *diskd*, *coss* y *null*. Estos esquemas tienen diferentes propiedades y técnicas para organizar y acceder a los datos almacenados en el caché mediante llamadas a operaciones del sistema de archivos

2.4.2. Requisitos para Squid.

2.4.2.1.CPU para Squid.

La *figura 18* nos muestra las características de CPU que cuenta nuestro equipo. Squid no hace uso amplio de CPU, en las únicas ocasiones en las que hace uso intensivo de CPU es cuando el proceso es inicializado. Es posible instalar Squid en sistemas con un solo CPU de velocidades modestas. Se realizó la prueba de cantidad de procesamiento que utiliza Squid **(color rojo)** al instante que se inicia el proceso y se comprobó que no realiza uso intensivo de la capacidad de CPU, llegó a ocupar un 0.5% de la capacidad total. Esto ocurre por la velocidad alta de procesamiento del servidor físico. Pero pude llegar hasta un 3.5% en servidores más lentos.

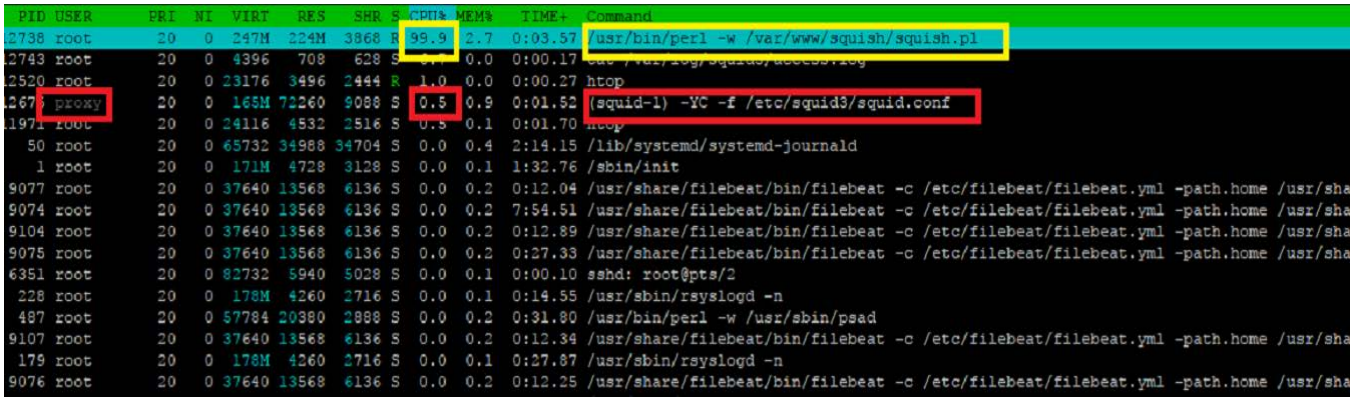


Figura 18. Consumo de CPU de Squid. Fuente. Creado por el autor.

Se puede apreciar (color amarillo) que el máximo consumo lo genera un script de Perl que es el encargado de actualizar las cuotas de navegación de los usuarios. Este script se ejecuta cada 5 min por solo unos segundos por lo que no representa peso de carga al servidor.

2.4.2.2. Disco Duro para Proxy Squid.

El caché en disco se almacena en un directorio del sistema de archivos, se recomienda que esté en una partición independiente de la del sistema operativo, de preferencia en un disco duro independiente. El espacio en disco que asigne al caché debe ser lo suficientemente grande para poder almacenar los objetos estáticos de los sitios visitados por lo menos por un día para que el uso del proxy sea eficiente, si las peticiones son a sitios con objetos estáticos que no cambian tan seguido entonces se recomienda que calcular el espacio en base al número de días que quiere conservar los objetos en el caché y la velocidad de descargas asignada al servidor proxy. También tienen que ver factores como el tamaño promedio de los objetos en el caché y los hábitos de descargas de los usuarios.

En un enlace de 8 Mb/s dedicado de forma fija para Internet debería haber una descarga de:

8Mb/s=1MB/s=3.6GB/h lo que sería aproximadamente **86GB/día.**

Date	Group	Users	Oversize	Bytes	Average	Hit %
18 May 2018	grp	775	407	29.8 G	39.3 M	1.52%
17 May 2018	grp	1240	592	41.4 G	34.2 M	1.60%
16 May 2018	grp	1372	642	46.2 G	34.5 M	2.07%
15 May 2018	grp	1281	460	32.2 G	25.7 M	2.77%
14 May 2018	grp	1114	557	34.3 G	31.5 M	2.16%
13 May 2018	grp	78	44	28.7 G	376.4 M	0.04%
12 May 2018	grp	212	131	24.1 G	116.4 M	1.28%
11 May 2018	grp	525	255	20.5 G	39.9 M	0.65%
10 May 2018	grp	1101	451	28.6 G	26.6 M	0.92%
09 May 2018	grp	1262	565	38.5 G	31.2 M	1.01%
08 May 2018	grp	612	265	19.0 G	31.8 M	0.58%
Total/Average:		870	397	343.1 G	71.6 M	1.33%

Figura 19. Bytes de descarga de Internet en 10 días. Fuente. Generado por Lightsquid.

Se tomaron 5 días laborales desde el 14 al 18 donde se pudo comprobar que por promedio se consume 36 GB por día, lo que representa solo un aproximado del 42 % de lo posible. Esto se debe al bajo uso que se le da en horario no laboral o las limitaciones de ancho de banda impuestas en el Firewall PfSense.

Por tanto se pudiera necesitar 86 GB de espacio en el disco duro para el caché pero según (15) el aumento de protocolo https ha aumentado en un 20 % en los 2 últimos años, tomando que todo el contenido http es *cacheable* le restamos el 20% del https,esto sería un 70GB de peticiones http.

En sistemas con volúmenes de peticiones grandes se recomienda dedicar una partición de 20 GB para la partición */var/log*. Si va a almacenar reportes web de los accesos al proxy se recomienda que dedique por lo menos 10 GB adicionales para el sistema de archivos /var/www para almacenar los reportes por 6 meses.

2.4.2.3. Memoria RAM para Proxy Squid.

Al dimensionar las capacidades de memoria RAM que usará el sistema que hará de proxy con Squid, no solo considera la memoria que usa el proceso principal de Squid, también se considera el uso de memoria de otros programas que se ejecuten aparte del sistema operativo, como pueden ser servicios

DNS, Web, bases de datos, etc. A continuación, mencionaremos las partes en las que Squid hace uso de memoria RAM.

Squid utiliza la memoria RAM para almacenar una tabla o índice con los objetos más usados, estos objetos son conocidos como objetos *calientes* o *en tránsito*, esto permite acelerar el tiempo de respuesta a las peticiones de los clientes ya que siempre es más rápido acceder a la memoria RAM que a disco duro como en el caso de caché a disco (más para objetos recurrentes), el uso predeterminado de caché en memoria RAM es de 256MB, para entornos con grandes volúmenes de peticiones se recomienda incrementar el valor y agregar más memoria RAM para acelerar el servicio.

Además, por cada 1 GB de espacio en disco que se asigne para la memoria caché en disco, Squid usará aproximadamente 6 MB de memoria RAM para mantener una tabla o índice con la referencia a los objetos almacenados en el caché de disco. Esto significa que, entre más grande sea el caché de disco, más memoria RAM usará Squid. Por tanto, de 70 Gb para el caché de Squid multiplicado por 6 MB se utilizaría 420MB de RAM.

Ya que se cuenta con un servidor de grandes recursos es importante tener en cuenta:

- Cambia la opción *"cache_mem*" de 256MB, el predeterminado, a 512 MB o si se dispone un servidor con recursos disponibles, aumentar esta opción de memoria caché puede mejorar mucho el rendimiento. Algunos expertos recomiendan poner 1024 MB o más.
- Añade la opción "*half_closed_clients*" para ponerla en "off" en el archivo de configuración. Además, cambia la opción "*maximum_object_size*" por "1024 KB" para mejoras menores. Indica tus servidores de nombres DNS usando la opción "*dns_nameserves*". Esto es importante puesto que Squid se queda atascado cuando hace búsquedas de DNS.
- Añade las opciones "*cache_swap_low*" y "*caché_swap_high"* que ayudan a determinar cuándo Squid empezará a vaciar la caché. Esto es importante para mantener la caché dentro de unos límites razonables y accesibles rápidamente.
- Ajusta la opción "*memory_pools*" en "off" para que Squid libere la RAM que no está usando el servidor y la coloque en la fuente de memoria.

El tamaño de los archivos de un sitio web sin archivos de grandes datos como audio o video puede llegar como promedio a 420 KB.

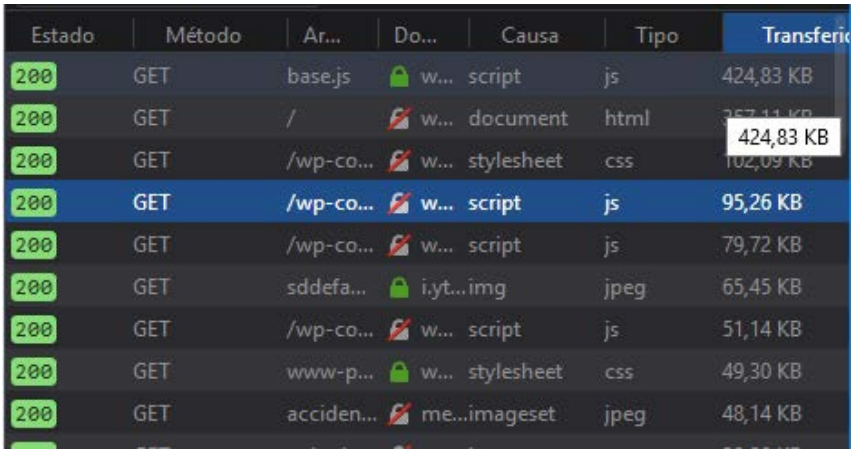


Figura 20. Tamaño medio de archivos de Internet. Fuente. Creado por autor.

Por tanto, se pude resumir que un servidor Squid consume un nivel medio de recursos de hardware y que es posible implementarlo en PC de escritorio de uso diario.

Partición	**Punto de Montaje**	**Tamaño Gb**
Sistema base	/ - raíz del disco	20 Gb
Caché de Squid	/mnt/caché/squid	70 Gb
Logs	/var/log/	20 Gb
Reportes	/var/www/html/	10Gb
Total		**120 Gb**

Tabla 1. Requisitos de disco duro para Servidor Proxy.

2.4.2.4. Requerimientos de conectividad.

- Conectividad con uno o más servidores DNS. Si el o los servidores DNS están en la red LAN asegúrese de que tenga permitidos los siguientes puertos: UDP/53 y TCP/53
- Conectividad hacía Internet para los protocolos FTP, HTTP y HTTPS, también es posible que se tengan que abrir otros puertos para sitios o servicios web que se ejecutan en puertos HTTP o HTTPS no estándar, este último caso es muy común para páginas de gobierno.
- Si el servidor Proxy va a realizar algún tipo de autenticación con un servidor externo, por ejemplo, LDAP o Active Directory debe estar permitido el puerto TCP/369 en el servidor LDAP.

2.5. Planificación del proyecto.

Las tareas a realizar serán las siguientes:

- Instalación de un Servidor Físico Proxmox v5.1
  - Instalación de servidores virtuales LXC. Instalar, actualizar y configurar dos servidores con el sistema operativo seleccionado Debian 9.
- Configuración básica de los principales servicios en Debian.
  - Configuración básica de SSH en los dos servidores para permitir autentificación con usuario root.
  - Configuración avanzada de Squid en dos servidores.
  - Instalación de la herramienta SquidGuard en el servidor proxy Internet.
  - Instalación de la Herramienta de generación de reportes por usuarios Lightsquid y SquidAnalyzer en los 2 servidores.
  - Instalación de Apache en los dos servers. Configuración de los hosts virtuales en Apache para la visualización de Lightsquid y SquidAnalyzer en los 2 servidores.
  - Configuración del host virtual en apache para la visualización de Squish-Cuotas en los dos servidores, pero en el servidor proxy Nacional las cuotas serán ilimitadas o solo se utilizará para reportes de uso de las descargas por usuario.
  - Establecer todas las tareas automáticas con Cron. Implementar scripts para tareas como el reinicio todos los meses las cuotas de los usuarios en ambos servidores y la salva de los logs diariamente.
- Monitoreo.
  - Instalación de la herramienta *Sqstat* en los dos servidores. Creación del host virtual con Apache para ver los reportes se *Sqstat*
- Respaldo y recuperación.
  - Bakup automático para el servidor Proxmox de todo el container LXC para el volumen LVM.
  - Bakup manual cada 3 días para el servidor NAS.
  - Coger uno de los bakup automáticos y restablecer el container LXC. Ver que se levante sin problemas.
  - Coger uno de los bakup del NAS y restablecer el container LXC. Ver que se levante sin problemas.

Seguridad

- Implementar un script de Shell que funcione con las reglas de Iptables Netfilter.

La facilidad de los *backups* de la solución propuesta es la infraestructura de servidores Proxmox implementadas por los administradores permitiendo en caso de fallo y/o corrosión del servidor físico levantar uno de los *backups* en otro servidor sin problemas.

2.7. Conclusiones del Capítulo II.

Al concluir este capítulo se obtiene la planificación que dará solución al problema científico, así como los requisitos fundamentales que caracterizan el entorno al cual tributa el sistema de navegación. Se especifican las características tecnológicas de la propuesta en cada etapa de realización del proyecto. Se realiza una caracterización del sistema de navegación actual de la Universidad de Matanzas, donde se demuestra la ineficacia del mismo.

Capítulo III. Construcción de la propuesta y análisis de los resultados obtenidos.

Introducción.

En este capítulo se aborda el proceso de instalación del sistema de navegación propuesto, así como la integración a través de las configuraciones diseñadas entre los diferentes módulos que lo conforman. Se realizan las pruebas referentes al funcionamiento, estabilidad y la mejoría en cuanto a la eficiencia del uso del ancho de banda que dispone la Universidad de Matanzas.

3.1. Instalación de los componentes del Sistema.

3.1.1. Instalación de Proxmox.

Para la instalación de Proxmox se utilizó uno de los servers profesional de marca **Inspur** en el cual se encontraba el Sistema implementado hasta el momento, esto fue posible debido a que el Departamento de Redes no contaba con servidores suficiente como para tomar uno para las pruebas necesarias.

La principal medida tomada fue realizar salvas de las máquinas Container que se encontraban funcionando hasta el momento en caso de fallos posibles al levantarlas en la versión de Proxmox propuesta, así como utilizar un horario que no interrumpiera de manera prolongada los servicios a la comunidad universitaria. Dicha tarea se realizó entre sábados y domingos ya que es cuando menos usuarios se conectan a la red.

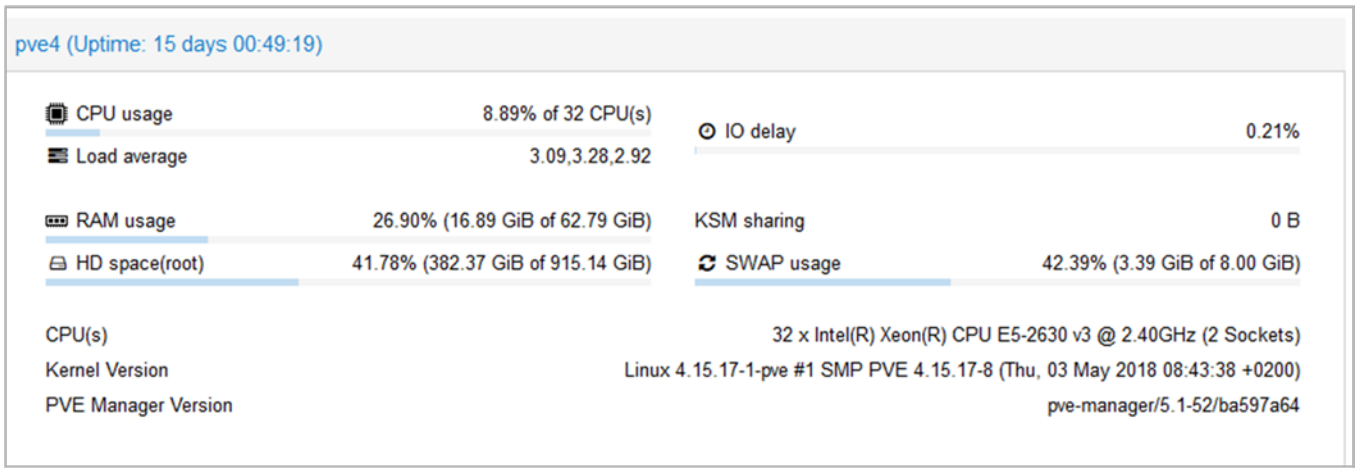


Figura 21. Características del servidor físico después de instalar Proxmox. Fuente. Creado por el autor. Tomado de la interfaz web de Proxmox.

3.1.1.1. Crear las máquinas virtuales en Proxmox.

El proceso de instalación de Proxmox (Ver Anexo 1) es rápido y con un entorno amigable para aquellos con menos experiencias en este sistema de virtualización. Tras la instalación básica de Proxmox se realiza la creación de los dos Container que se utilizarán como servidores de prueba e implementación de las herramientas seleccionadas. Se utilizó la herramienta de administración WinSCP (Ver Anexo 4) para de esta forma administrar los servidores con una interfaz más amigable. WinSCP permite configurar host mediante el protocolo SFTP y junto a su integración con la herramienta Putty (Ver Anexo 5) mediante SSH permite la ejecución de comandos de SHELL directamente en los servidores.

Proxmox permite la incorporación de servidores NAS (Ver Anexo 3) a través incorporación de disco duros externos en formato NFS. Tener un servidor NAS permite tanto que los disco dura de las máquinas virtuales como las salvas de ellas pueden hacerse de forma automática y tener algún respaldo en caso de rotura del servidor físico principal.

Cuando se crean los contenedores que actúan como proxies es necesario poder configurar el protocolo SSH para permitir la administración remota mediante *Putty*. Esta tarea se realiza mediante la interfaz web de Proxmox al seleccionar el Container a trabajar en el botón de consola establecer una nueva sección. El comando nano es un editor de texto y será utilizado para las modificaciones de archivos.

```
root@internet:~# nano /etc/ssh/sshd_config
```

Buscar la línea **#PermitRootLogin without-password** y cambiarla por **PermitRootLogin yes.** Será necesario reiniciar el servicio ssh.

```
root@internet:~# service ssh restart
```

3.1.2. Instalación de las herramientas propuestas en los dos servidores

Es necesario tener siempre actualizados nuestros sistemas operativos para de esta forma poder utilizar las últimas versiones de nuestras herramientas y programas

```
root@internet:~# apt update -y && apt  upgrade -y
```

-y se utiliza para aceptar todas las preguntas de confirmación .

3.1.2.1. Instalación de Squid

Para instalar Squid hay que utilizar simplemente:

```
root@internet: ~# apt install squid
```

Los ficheros y directorios más importantes son:

- */etc/squid/* - donde se guardan los ficheros de configuración, fundamentalmente el fichero squid.conf.
- */usr/share/doc/squid/* - La documentación se encuentra en esta ubicación.
- */var/spool/squid/* - donde se almacenan las páginas *cachéadas*, es decir, las que se han traído de Internet y que se guardan mientras no caduquen para la próxima vez que las solicite alguien. Se puede cambiar este directorio en nuestro caso utilizamos */mnt/caché/squid/*
- */var/log/squid/* - donde se ubican los ficheros de registro de Squid que son independientes del *syslog* del sistema.

Configuración elemental

El archivo de configuración que utiliza Squid es /etc/squid/squid.conf. Este fichero es un tanto peculiar, ya que incluye muchos parámetros comentados que no se utilizan inicialmente y además incluye bastantes comentarios sobre la utilización y sintaxis de estos parámetros. En concreto, en la versión que estamos utilizando, el fichero de configuración de Squid consta de **7654** líneas. Para tener una primera idea de algunos parámetros que se están utilizando de forma explícita, lo sacamos por la salida estándar, quitando las líneas que empiecen por un espacio en blanco (suponemos que son líneas en blanco) y por # (comentarios):

```
root@internet: ~# cat /etc/squid/squid.conf | grep -v ^$ | grep –v ^#
```

```
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
http_access allow localhost
http_access deny all
http_port 3128
coredump_dir /var/spool/squid3
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern -i (/cgi-bin/|\?) 0     0%      0
refresh_pattern .               0       20%     4320
```

Figura 22. Configuraciones básicas de squid. Fuente. Creado por el autor.

Las *ACLs* declaradas en *squid* para la determinación de dominios, formatos, o direcciones de red que contenga varios ejemplos de ello serán creados en archivos externos al fichero principal de squid de esta forma solo se modifican dichos archivos y no el archivo principal.

Los archivos declarados serán:

- Dominios prohibidos.
- Mails prohibidos.
- Formatos lentos
- Formatos rápidos.
- Sitios de actualizaciones (Windows Update, Firefox, Opera, etc.)
- Sitios de descarga lenta. (Mega, Facebook, YouTube)
- Sitios de Prioridad Alta (Aquellos sitios de investigación y búsqueda de información como Google, ScienceDirect, Wikipedia, etc.)

3.1.2.2. Instalación de SquidGuard.

```
root@internet:~# apt install squidguard
```

Los ficheros y directorios más importantes son:

- /etc/squidguard/ donde se encuentra el archivo de configuración principal squidguard.conf
- /var/lib/squidguard/db donde se crean las bases de datos que contendrán las reglas a denegar.

Dentro de squidguard.conf podemos declarar el directorio de las bases de datos con: **dbhome /var/lib/squidguard/db**, directorio de los logs **logdir /var/log/squidguard**, así como los archivos con las listas a denegar **dest dialers {domainlist dialers/domains}**

Las categorías de SquidGuard (Ver Anexo 6) son las siguientes:

- Games: sitios sobre juegos que permitan las descargas o la práctica online.
- Porn: sitios de contenido para adultos.
- Proxy: sitios web que brindan la posibilidad de utilizar proxys anónimos y de esta forma saltarse las restricciones impuestas por la entidad.
- Socialnetworking: sitios considerados como redes sociales o de contenido asociado que son consideradas de ocio y con contenido racista, obsceno, etc.
- Virusinfected: sitios que proporcionan virus mediante los navegadores o peticiones de descarga de software.
- Webmail: sitios de correos en internet no tradicionales como Gmail, Yahoo!, etc. que son conocidos por envió de spam.

3.1.2.3. Instalación de Squish.

Para utilizar Squish es necesario descargarse el contenido comprimido, como Squish se integra con apache para crear un host virtual y mostrar el consumo de las cuotas es necesario copiar el archivo antes descargado en el directorio **/var/www/html/**

En nuestro directorio de squid creamos el archivo principal squish.conf y declaramos las cuotas.

```
root@internet:~# mkdir /etc/squid/squish.conf
```

Lo modificamos con nano o con WinSCP y dentro podemos poner:

```
1  ##--Ejemplos---##
2  #usuario              25h/day      B-Mb-Gb/day-week-month-year
3  nombre.apellidos      25h/day 1Gb/day
4  nombre2.apellido2     25h/day 20 Mb/week
5
6  #Resto de los usuarios (cuota básica)
7  .*       25h/day 500Mb/month
```

Figura 23. Ejemplos de creación de cuotas con Squish. Fuente. Creado por el autor.

Dentro del fichero squish.pl en la línea 30 modificamos nuestro directorio al fichero squid.conf así como el archivo de generación de usuarios bloqueados squished de donde Squid lee para denegar el acceso.

Ejecutamos nuestro script para actualizar las cuotas y general la base de datos user.stor donde se guarda el consumo diario de los usuarios y cuando sobre pasa lo antes descrito en squish.conf entonces se genera el fichero squished.

```
root@internet:~# /var/www/html/squish/squish.cron.sh
```

3.1.2.4. Instalación de Apache y Lightsquid.

Descargamos apache y sus librerías para arrancar con la instalación:

```
root@internet:~# apt install apache2 libgd-gd2-perl -y
```

Ingresamos en la carpeta donde descargamos Lightsquid

```
root@internet:~# cd /var/www/html/
```

Descargamos la fuente de Lightsquid 1.8

```
root@internet: /var/www/html#  wget http://mikrotik.com.pe/lightsquid-1.8.tgz
```

Descomprimimos y renombrados la carpeta

```
root@internet: /var/www/html# tar -xzf lightsquid-1.8.tgz
root@internet: /var/www/html# mv lightsquid-1.8 Lightsquid
root@internet: /var/www/html# cd Lightsquid
```

Le damos permisos de ejecución a extensiones cgi y pl

```
root@internet: /var/www/html/ Lightsquid# chmod +x *.cgi
root@internet: /var/www/html/ Lightsquid# chmod +x *.pl
root@internet: /var/www/html/ Lightsquid# chown -R www-data.www-data *
```

Modificamos el archivo de configuración de Lighsquid para decirle donde se encuentran los ficheros a leer.

```
14  #path to additional `cfg` files
15  $cfgpath                ="/etc/lightsquid";
16  #path to `tpl` folder
17  $tplpath                ="/usr/share/lightsquid/tpl";
18  #path to `lang` folder
19  $langpath               ="/usr/share/lightsquid/lang";
20  #path to `report` folder
21  $reportpath             ="/var/www/html/lightsquid/report";
22  #path to access.log
23  $logpath                ="/var/log/squid";
24  #path to `ip2name` folder
25  $ip2namepath            ="/usr/share/lightsquid/ip2name";
```

Figura 24. Archivo de configuración de Lighsquid. Fuente: Creado por el autor.

Ejecutamos nuestro script de Perl para general nuestros reportes

```
root@internet:~# /var/www/html/Lighsquid/lightparser.pl
```

Crear el host virtual de apache:

```
root@internet:~# nano /etc/apache2/ sites-available/ lightsquid-trace.conf
```

```
<VirtualHost *:80>
    ServerName proxytrace.umcc.cu
    ServerAdmin admin.redes@umcc.cu
    DocumentRoot /var/www/html/lightsquid
    <Directory /var/www/html/lightsquid>
        Options +ExecCGI
        AddHandler cgi-script .cgi
        AllowOverride All
        Order allow,deny
        Allow from all
    </Directory>
ErrorLog ${APACHE_LOG_DIR}/lightsquid-error.log
CustomLog ${APACHE_LOG_DIR}/lightsquid-access.log combined
</VirtualHost>
```

Figura 25. Crear el host de Lighsquid en apache. Fuente. Creado por el autor.

Creamos el enlace simbólico y para aplicar los cambios reiniciamos el servicio.

root@internet:~# ln –s /etc/apache2/sites-available/lightsquid-trace.conf /etc/apache2/sites-enable/lightsquid-trace.conf
root@internet:~# service apache2 restart

3.1.2.5. Instalación de SquidAnalyzer.

Nos movemos al directorio opt se utiliza mucho para procesos de instalaciones temporales

root@internet:~# cd /opt/

Para esta instalación comenzamos por descargarnos la aplicación, descomprimir e instalar.

root@internet:~/opt# wget http://sourceforge.net/projects/squid-report/
root@internet:~/opt # tar -xzvf squidanalyzer-6.2-1.tar.gz
root@internet:~/opt # install build-essential

Nos movemos dentro de la carpeta creada con los archivos de instalación y compilamos.

root@internet:~# cd /opt/squidanalyzer-6.2/
root@internet:~ cd /opt/squidanalyzer-6.2# perl Makefile.PL
root@internet:~ cd /opt/squidanalyzer-6.2# make && make install

Agregar entrada en el apache, crear nuestro enlace a los sites-enabled y reiniciar el servicio.

root@internet: ~# nano /etc/apache2/sites-available/squidanalyzer.conf
root@internet: ~# ln –s /etc/apache2/sites-available/squidanalyzer.conf /etc/apache2/sites-enabled/squidanalyzer.conf
root@internet: ~# service apache2 restart

```
<VirtualHost *:80>
ServerName squidanalyzer.umcc.cu
ServerAlias squidreport
   DocumentRoot /var/www/squidanalyzer
   Alias        /squidreport /var/www/squidanalyzer
    <Directory /var/www/squidanalyzer>
        Options -Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order deny,allow
        Allow from 127.0.0.1
    </Directory>
ErrorLog /var/log/apache2/squidanalyzer-error.log
CustomLog /var/log/apache2/squidanalyzer-access.log combined
</VirtualHost>
```

Figura 26. Crear el host de SquidAnalyzer en apache. Fuente. Creado por el autor.

Generar el reporte del día mediante el comando

```
root@internet: ~# /usr/local/bin/squid-analyzer > /dev/null 2>&1
```

3.1.2.6. Instalación de Sqstat.

Para utilizar esta aplicación es necesario

- PHP 4.1.0 o superior
- Squid 2.6 o superior

Comenzamos con descargar la herramienta

```
root@internet: ~# wget http://samm.kiev.ua/sqstat/sqstat-1.20.tar.gz
```

Descomprimir en la ruta /var/www/html/sqstat

```
root@internet: ~# tar –xzvf  sqstat-1.20.tar.gz
```

Copiar y renombrar el archivo config.inc.php.defaults hacia config.inc.php, luego editar el archivo config.inc.php y especificar la ip del Squid proxy server más el puerto. Quedaría más o menos así:

$squidhost[0]="127.0.0.1";	Ip del servidor
$squidport[0]=3128;	Puerto de squid
$cachémgr_passwd[0]="password";	Password de comunicación con squid
$resolveip[0]=true;	Para resolver los IPs

En el fichero *squid.conf* se debe declarar **cachémgr_passwd password all**

Se puede ver sqstat en el navegador web desde la url *http://ipdelservidor/sqstat/sqstat.php*

3.1.2.7. Iptables.

Las reglas de Iptables (Ver Anexos 8) se implementan sobre un script el cual se ejecuta en el min 1 cada 2 horas.

3.1.2.8. Ejecución de tareas diarias de forma automáticas con crontab.

En el archivo **/etc/crontab** podemos introducir tareas que se ejecutarán en un momento dado definido por el administrador del servicio.

Este está definido como: **min horas días meses año user command**

Ejemplo:

- squish.cron.sh se ejecutará cada 5 min en todo el día, de todos los meses de todos los años.
- Las cuotas se reinician a las 12:10 el 1 día de todos los meses de todos los años.

```
1  */5 * * * *   root  service squid reload
2  */5 * * * *   root  /var/www/html/squish/squish.cron.sh
3  3   * * * *   root  /var/www/html/lightsquid/lightparser.pl
4  50  11 * * *   root  /usr/local/bin/squid-analyzer > /dev/null 2>&1
5  10  0 1 * *   root  /root/scripts/clean-cuotes.sh
6  2   0 * * *   root  /root/scripts/save-log.sh
7  1 */2 * * *   root  /root/scripts/firewall-iptables.sh
```

Figura 27. Tareas definidas por el administrador a ejecutar con crontab. Fuente. Creado por el autor.

3.2. Integración entre los diferentes elementos del sistema.

3.2.1. Squid y los sistemas de revisión de trazas.

Cuando un usuario solicita un recurso de internet Squid guarda dicha petición en los archivos de logs, estos guardan IP de origen, url destino, IP destino, usuario, etc. Las herramientas de revisión de trazas Lighsquid y SquidAnalyzer lo que realizan es una comprensión más detallada de estos registros y de esta forma generar reportes más específicos los recursos solicitados.

3.2.2. Squid y Active Directory.

Squid se comunica con el Directorio Activo mediante módulos internos del propio Squid, en este caso se utiliza **basic_ldap_auth** el cual mediante un usuario y contraseña que se encuentran dentro del Directorio Squid puede comprobar las credenciales de los usuarios.

Para comprobar los permisos que contiene cada usuario que realiza alguna petición y de esta forma otorgarle los diferentes accesos que existen Squid utiliza otro módulo de ACL externa **ext_ldap_group_acl** el cual funciona igualmente por la comunicación de usuario y contraseña que permite la lectura de los diferentes grupos dentro del directorio**.**

3.2.3. Squid y Squish.

Estas dos herramientas se comunican de la forma más sencilla posible, mediante la creación de una ACL de tipo **proxy_auth** (usuarios autentificados) y la lectura del archivo **squished** donde Squish genera el consumo de cada usuario

Ejemplo:
acl cuotas proxy_auth -i "/etc/squid/squished"
http_access deny cuotas

3.3. Nuevas políticas sobre acceso a Internet y Red Nacional

3.3.1. Políticas de acceso a internet.

- Autenticación contra el Active Directory y obtención de los permisos otorgados por la administración del centro.
- Sitios nacionales e sitios de investigación del canal ICT redireccionados a través del archivo **proxy.pac** hacia el Proxy-Nacional.
- Archivo proxy.pac muestra las URLs a las que responden cada Proxy eliminando así que los usuarios sepan los IPs de cada servidor
- Denegación a través de SquidGuard de los dominios que se encuentre entre sus clasificaciones antes descritas.
- Denegación a las cuentas de usuario que se conecten por más de un IP al mismo tiempo.
- Autenticación obligatoria con una petición automática desde el servidor si el usuario no usa el sistema en 30 minutos.
- Creación de dos horarios utilizados para la restricción de ancho de banda y control de acceso.
    - Horario Laboral de 8:00-15:30
    - Horario No Laboral 15:30-8:00
- Squish no consumirá cuota a sitios de investigación, subred de servidores, URLs de desarrollo, meteorología, y dominios .CU, además de sitios tan visitados como universidades o revistas de otros países. A estas listas se pueden ir adicionando cada vez más sitios que ayuden a la investigación y desarrollo en el centro.

- Cuota básica de Internet de 1 GB ya que los formatos de archivos son cada vez más grandes dejando a los usuarios sin cuota rápidamente.
- Denegación a través de ACLs a las URLs de Correo Externo (Gmail, Yahoo!) a los usuarios que no tengan esos permisos.
- Permitir a través de ACLs a las URLs de Redes Sociales a todos los usuarios en cualquier horario.
- Denegación a través de ACLs a la navegación por IP.
- Denegación a través de ACLs al dominio interno .CU, excepto a los usuarios conectados desde la red WIFI ya que en los teléfonos móviles no son configurables para utilizar el archivo proxy.pac, el resto será direccionado al Proxy-Nacional.
- Denegación a través de ACLs a descargar archivos mp4, mpg, avi, iso, exe, etc., en Horario Laboral.
- Denegación a través de ACLs a las URLs que pueden contener virus, pornografía, violencia, spam, subversión, proxies anónimos, etc.
- Denegación a través de ACLs a las URLs que consumen demasiado tráfico y son consideradas como ocio y no productivas.
- Denegación a través de ACLs a las URLs de actualización como Windows Update o Navegadores Web
- Denegación a través de ACLs a los laboratorios de la carrera de Ingeniería Informática a aquellos usuarios que no tenga el permiso de Informática en el Active Directory.
- Control de ancho de banda solo en Horario Laboral.
    - Sitios de Investigación, Correo Externo, archivos de documentos investigativos, páginas web, imágenes de formatos pequeños tendrán todo el ancho de banda.
    - Redes Sociales 2 Mbps/s para toda la entidad aumentando así la rapidez de redes sociales, pero con un máximo de 320 Kbps por usuario.
    - Formatos de Audio y Video con un máximo de 100 Kbps por usuario ya que estos tipos de formato son en forma de ocio.
- Tamaño de caché de 70 GB.
- Tiempos de refrescos de caché en dependencias de los diferentes formatos de archivos.
- Más de 100 formatos de archivos para ser cachéados.

3.3.2. Políticas de acceso a Red Nacional.

- ❖ Autentificación contra el Active Directory
- ❖ Denegación a las cuentas de usuario que se conecten por más de un IP al mismo tiempo.
- ❖ Autenticación obligatoria con una petición automática desde el servidor si el usuario no usa el sistema en 30 minutos.
- ❖ Permite acceso solo a dominios .CU. IPs pertenecientes al Bloque de direcciones del canal Nacional.
- ❖ Redirección al proxy ICT perteneciente al MES de los sitios de Investigación de dicho proyecto.
  - Formatos de Audio y Video con un máximo de 100 Kbps por usuario ya que estos tipos de formato son en forma de ocio.
- ❖ Tamaño de caché de 70 GB.
- ❖ Tiempos de refrescos de caché en dependencias de los diferentes formatos de archivos.
- ❖ Más de 100 formatos de archivos para ser cachéados.

3.4. Análisis de resultados.

3.4.1. Ventajas del nuevo Sistema de Navegación.

Al ser evaluado el nuevo sistema de navegación se comprobaron las siguientes ventajas con respecto al que se encuentra activo en la Universidad de Matanzas:

- Mayor estabilidad y tolerancia a fallos, aún sin resolver problemas de índole energético que requieren todo un sistema de respaldo eléctrico.
- Monitoreo de forma organizada, precisa y en tiempo real que permite detectar eventos no deseados en el sistema.
- Facilidad a la hora de aplicar cambios a las configuraciones o insertar nuevos módulos o aplicaciones.
- Distribución correcta y acorde a las exigencias de la entidad del tráfico hacia internet y la red nacional.
- Mayor control del ancho de banda asignado a cada usuario en dependencia de los dominios solicitados.
- Mejor distribución del ancho de banda por diferentes horarios.
- Correcta configuración de los navegadores web de los usuarios.
- Plantea mejor distribución sobre los permisos otorgados a los usuarios en el Directorio Activo.

- Realización de salvas automáticas en servidores NAS de respaldo.
- Salvas automáticas de los archivos de registros en más de un servidor
- Correcta configuración de las Reglas del Servidor Firewall-PfSense en cuestiones tanto de puertos destino y ancho de banda asignado.
- Las reglas de Iptables lograrán darle un mayor nivel de seguridad al servidor. Los ataques que se puedan generar directamente al servidor tienen que ser desde la red administrativa siendo responsabilidad de los que ahí laboran.
- Las políticas establecidas dentro de Squid permiten tener un mejor control de acceso sobre los sitios permitidos o denegados a la comunidad universitaria.
- Dar prioridad a tareas del centro como sitios de Investigación o Correo Externo.
- Establecer listas de sitios tan utilizados en funciones laborales que no consuman cuotas a la hora de visitarlos.
- Al utilizarse software libre se podrán hacer cualquier cambio necesario sin tener que pagar por licencias ni soporte.
- Documentación existente en internet por comunidades de soportes con miles de usuarios.
- Al ocurrir cualquier fallo físico del servidor es solo copiar hacia otro servidor una de las salvas generadas automáticamente y encender el Container en menos de 10 minutos.
- Al implementar Squid 3.5 se podrá utilizar este sistema por más de 2 años.
- Este proyecto ayudará a los Administradores de Redes a tener un sistema más confiable en la red.
- Dotará de conocimientos sobre el tema tanto a usuarios no administrativos como a los que sí lo son.
- Este informe servirá de guía para una posible reestructuración del sistema propuesto en búsqueda de mejorar cada vez más los servicios.
- Este informe ayudará a conformar legalmente las políticas de navegación del centro.
- La falta de equipos de cómputo impuso obstáculos para la realización de clústeres de servidores Proxmox para mejorar la Disponibilidad y el Balanceo de Carga a los servicios de proxy tanto Internet o Red Nacional
- Las políticas del país junto con las del MES y la Universidad nos imponen restricciones debido a la infraestructura ya creada, establecimiento de herramientas como Squid con soporte SSL y de esta forma hacer uso de caché para sitios con protocolo HTTPS.

3.5. Conclusiones del Capítulo III.

Durante este capítulo se expone el proceso de instalación del sistema y las principales configuraciones de los elementos que lo conforman. Se aplican las técnicas para examinar las características de rendimiento y estabilidad del sistema, así como la correcta interoperabilidad entre los módulos instalados. Se aplican pruebas para validar la seguridad del sistema: ataques de denegación de servicios, fuerza bruta y otros, demostrándose la invulnerabilidad del sistema ante estos eventos. Se realiza una breve descripción de las funciones del sistema, destacándose la posibilidad de realizar nuevas configuraciones o agregar futuros módulos que aumenten las funcionalidades del sistema.

Conclusiones Generales

Como resultado de esta investigación para dar respuesta al problema planteado: *Ineficacia del sistema de navegación actual de la Universidad de Matanzas que imposibilita que se utilicen, de manera eficiente, los recursos de ancho de banda asignados*, se arribó a las siguientes conclusiones.

- El análisis y estudio de los antecedentes permitió comprobar que en el Sistema MES y en el resto del país no existía un sistema detallado y estructurado de Navegación orientado a gestionar los diferentes canales de comunicación que se ofrecen a cada centro universitario.
- El estudio de las diferentes tecnologías de virtualización, sistemas operativos, aplicaciones, así como los recursos con que se cuentan en nuestra universidad, nos aportó los elementos necesarios para la correcta selección de las herramientas necesarias para la implementación del Sistema. Se utiliza como sistema de virtualización Proxmox, como Sistema Operativo Debian 9 y como herramienta para los procesos de proxy a Squid.
- Se diseñó un algoritmo para la recolección de la información de navegación, donde se distingue por usuarios, fechas y sitios visitados. Con el uso de la herramienta SquidAnalyzer se realiza la visualización de la información recolectada.
- Con el desarrollo de las pruebas funcionales, se optimizaron los módulos de configuración del nuevo sistema, obteniéndose valores óptimos en cuanto a la memoria Caché y ancho de banda asignado a cada tipo de información, en correspondencia con las nuevas políticas de informatización del país.
- Con el desarrollo de las pruebas de seguridad aplicadas al sistema y los resultados obtenidos se verifica una correcta seguridad y funcionamiento del mismo.
- Se implantó el sistema para un grupo específico de usuarios y se encuentra en explotación en la actualidad. Siendo un sistema en espera de aprobación por la administración de nuestro centro para su futura explotación.

Recomendaciones:

Con la conclusión del trabajo de diploma queda elaborada una primera versión del sistema y teniendo en cuenta las características dinámicas de las exigencias en cuanto a navegación, se recomienda:

- Realizar la actualización periódica de los módulos que lo conforman, eliminando así posibles vulnerabilidades que puedan surgir.
- Mejorar las condiciones de hardware del sistema: incluir un disco duro de estado sólido para aumentar la velocidad de transferencia de información interna del sistema.
- Proteger el sistema con un respaldo energético funcional para evitar fallos de hardware.

Índice de Figuras

Referencias

1. Vinton , Gray Cerf. Internet Society. *Breve historia de internet.* [En línea] Internet Society, 2018. [Citado el: 21 de abril de 2018.] https://www.internetsociety.org/es/breve-historia-de-internet/.

2. Rodríguez Brito, Anidelys . La ruta de Internet en Cuba. [En línea] Periodismo de Barrio en colaboración con el Observatorio de Políticas Públicas de Internet de la Universidad de Pennsylvania, 2018. [Citado el: 20 de abril de 2018.] https://www.periodismodebarrio.org/internetencuba/2018/04/13/la-ruta-de-internet-en-cuba/.

3. Método Hipotético-Deductivo. [En línea] [Citado el: 24 de abril de 2018.] http://www.e-torredebabel.com/Psicologia/Vocabulario/Metodo-Hipotetico-Deductivo.html.

4. Navarro Cholanco, Jorge Anibal. IMPLEMENTACIÓN *DE UN PROXY EN PLATAFORMA LINUX PARA CONTROL DE TRANSFERENCIA DE ARCHIVOS CON FTP, E-MAIL Y FIREWALL PARA EL LABORATORIO DE SOFTWARE.* Escuela Politécnica Nacional. Quito-Ecuador : Escuela de Formación de Tecnólogo, 2009. pág. 150.

5. VMware. [En línea] VMware, Inc, 2018. [Citado el: 26 de Abril de 2018.] https://www.vmware.com/es/products/esxi-and-esx.html.

6. Gómez Fernández, Félix. *AUTOMATIZACIÓN DE INSTALACIÓN Y CONFIGURACIÓN DE APLICACIONES PEER-TO-PEER EN UN ENTORNO VIRTUALIZADO BASADO EN MODELNET Y PROXMOX.* Departamento de Ingeniería Telemática, Universidad Carlos III de Madrid. Madrid-España : s.n., 2010. pág. 157, Proyecto Fin De Carrera.

7. Lacunza, Eneko . Tecnologías de Virtualización, Proxmox como alternativa a Wmware e HiperV. [En línea] [Citado el: 26 de Abril de 2018.] http://www.spri.eus/euskadinnova/es/enpresa-digitala/agenda/tecnologias-virtualizacion-proxmox-como-alternativa-wmware-hiperv/8348.aspx.

8. Proxmox. Linux Container. [En línea] Proxmox, 16 de Mayo de 2018. [Citado el: 20 de Mayo de 2018.] https://pve.proxmox.com/wiki/Linux_Container.

9. Qemu/KVM Virtual Machines. [En línea] Proxmox Server Solutions GmbH, 16 de Mayo de 2018. [Citado el: 2018 de Mayo de 20.] https://pve.proxmox.com/wiki/Qemu/KVM_Virtual_Machines.

10. Microsoft . Introducción a Active Directory. [En línea] Microsoft , 2018. [Citado el: 20 de Mayo de 2018.] https://support.microsoft.com/es-es/help/196464.

11. LDAP (Lightweight Directory Access Protocol) . [En línea] Noviembre de 2008. [Citado el: 26 de Abril de 2018.] https://searchmobilecomputing.techtarget.com/definition/LDAP.

12. Esparza Morocho, Juan Pablo. *IMPLEMENTACIÓN DE UN FIREWALL SOBRE PLATAFORMA LINUX EN LA EMPRESA DE CONTABILIDAD ARMAS & ASOCIADO.* Escuela de Formación de Técnologos, Escuela Politécnica Nacional. Quito-Ecuador : s.n., 2013. pág. 138, Proyecto de Pregrado.

13. Delgado Zambrano, Pablo Ricardo y Loor Loor, Luis Antonio. *SISTEMA PERIMETRAL FIREWALL Y FORTALECIMIENTO DE LA SEGURIDAD EN EL DATA CENTER DE LA ESPAM MFL.* CARRERA DE INFORMÁTICA, ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ. Calceta,Ecuador : s.n., 2017. pág. 128, Tesis.

14. Benedico Aguilera, Yoel . *Sistema Para El Control De Trazas De Un Servidor Proxy (Sctrazas).* Universidad de Ciego de Ávila. Ciego de Ávila,Cuba : Universidad de Ciego de Ávila, 2017. pág. 16. 227-2690.

15. Telemetry, Firefox. Let's Encrypt . [En línea] Linux Foundation Projects, enero de 2018. [Citado el: 10 de 05 de 2018.] https://letsencrypt.org/stats/#percent-pageloads.16. Ferrer Berbegal, Mònica . *Firewalls*

software: Estudio, instalación, configuración de escenarios y comparativa. Escola Politécnica Superior de Castelldefels, Universidad Politécnica de Catalunya. España : s.n., 2006. pág. 151, Trabajo De Fin De Carrera.

17. *Caverna Linux.* [En línea] [Citado el: 13 de Marzo de 2018.] https://cavernalinux.blogspot.pe/2018/03/configuracion-de-iptables.html.

Glosario de Términos

CACHÉ: es un componente de hardware o software que almacena datos para que las solicitudes futuras de esos datos se puedan atender con mayor rapidez.

CGI: (en inglés ***Common Gateway Interface***) es un método por el cual un servidor web puede interactuar con programas externos de generación de contenido

DHCP: Dynamic Host Configuration Protocol, es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente.

DNS: Domain Name System o Sistema de Nombres de Dominio, es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet.

FIREWALL: es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

FTP: File Transfer Protocol, es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor

GOPHER:es un servicio de Internet consistente en el acceso a la información a través de menús.

HARDWARE: partes físicas tangibles de un sistema informático.

HTTP: El protocolo de transferencia de hipertexto es usado en cada transacción de la Web (WWW). El hipertexto es el contenido de las páginas web, y el protocolo de transferencia es el sistema mediante el cual se envían las peticiones de acceso a una página y la respuesta con el contenido

HTTPS: Es la versión segura del protocolo HTTP. El sistema HTTPS utiliza un cifrado basado en las Secure Socket Layers (SSL) para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP. Cabe mencionar que el uso del protocolo HTTPS no impide que se pueda utilizar HTTP. El puerto estándar para este protocolo es el 443.

ICMP. (Internet Control Message Protocol). El Protocolo de Control de Mensajes Internet permite el envío de mensajes de control y error entre distintos gateways, routers o hosts.

IP: Internet Protocol o Protocolo Internet, es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

IPTABLES: es un poderoso firewall integrado en el kernel de Linux

KERNEL: es un software que constituye una parte fundamental del sistema operativo, y se define como la parte que se ejecuta en modo privilegiado (conocido también como modo núcleo)

LAN: Local Area Network. Red de área local. Es una red de dispositivos conectados (como PCs, impresoras, servidores y hubs) que cubren un área geográfica relativamente pequeña (generalmente no más grande que una planta o un edificio).

LOGS: En informática, se usa el término log, historial de log o registro a la grabación secuencial en un archivo todos los acontecimientos que afectan a un proceso particular.

PERL: es un lenguaje de programación diseñado por Larry Wall en 1987.

SCRIPTS: archivo de órdenes.

SNMP: (Simple Network Management Protocol). El Protocolo Simple de Administración de Red es un protocolo diseñado para dar al usuario la capacidad de administrar remotamente dispositivos de red.

SOFTWARE: soporte lógico de un sistema informático.

SSL: (en inglés ***Secure Sockets Layer***) protocolo criptográfico, que proporcionan comunicaciones seguras por una red.

TCP: Transmission Control Protocol o Protocolo de Control de Transmisión, este protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. Las conexiones TCP se componen de tres etapas: establecimiento de conexión, transferencia de datos y fin de la conexión.

TESTING: Las **pruebas de software** (en inglés *software testing*) son las investigaciones empíricas y técnicas cuyo objetivo es proporcionar información objetiva e independiente sobre la calidad del producto.

TLS: (en inglés ***Transport Layer Security***) protocolos criptográfico, que proporcionan comunicaciones seguras por una red

UDP: User Datagram Protocol, es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama

UNIX: (UNIX®) es un sistema operativo portable, multitarea y multiusuario.

UNSTABLE: software que presenta problemas (en español *software inestable)*

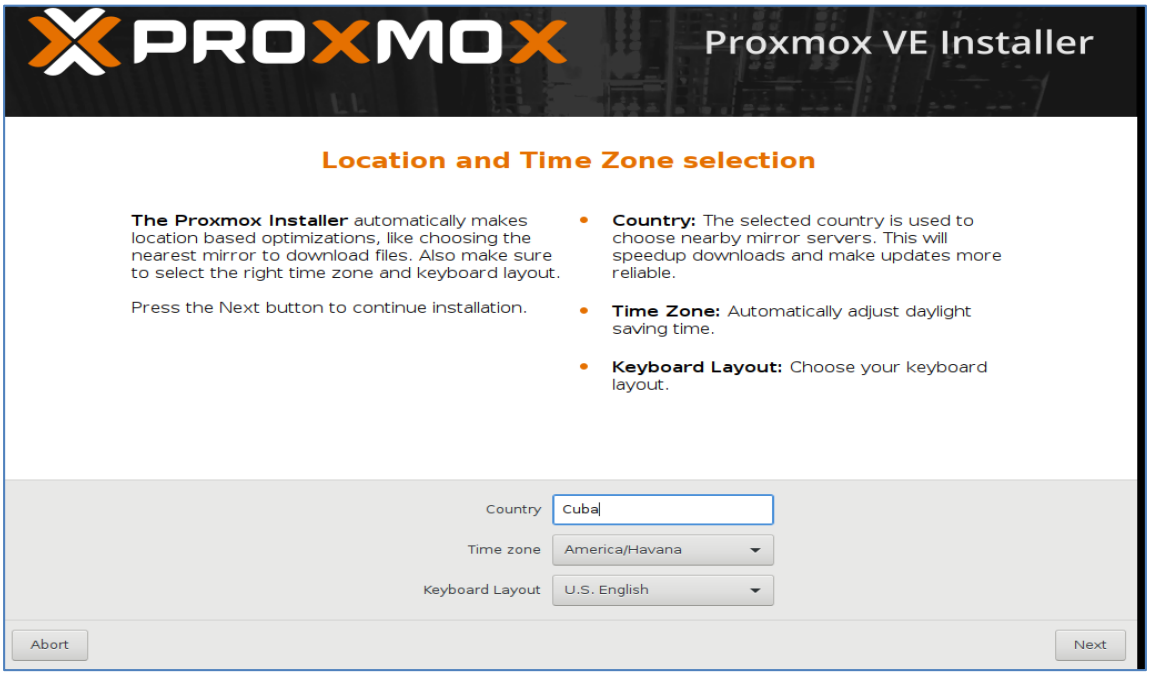
VIRUS: es un programa que permanece oculto, reproduciéndose hasta que se activa y causa daño.

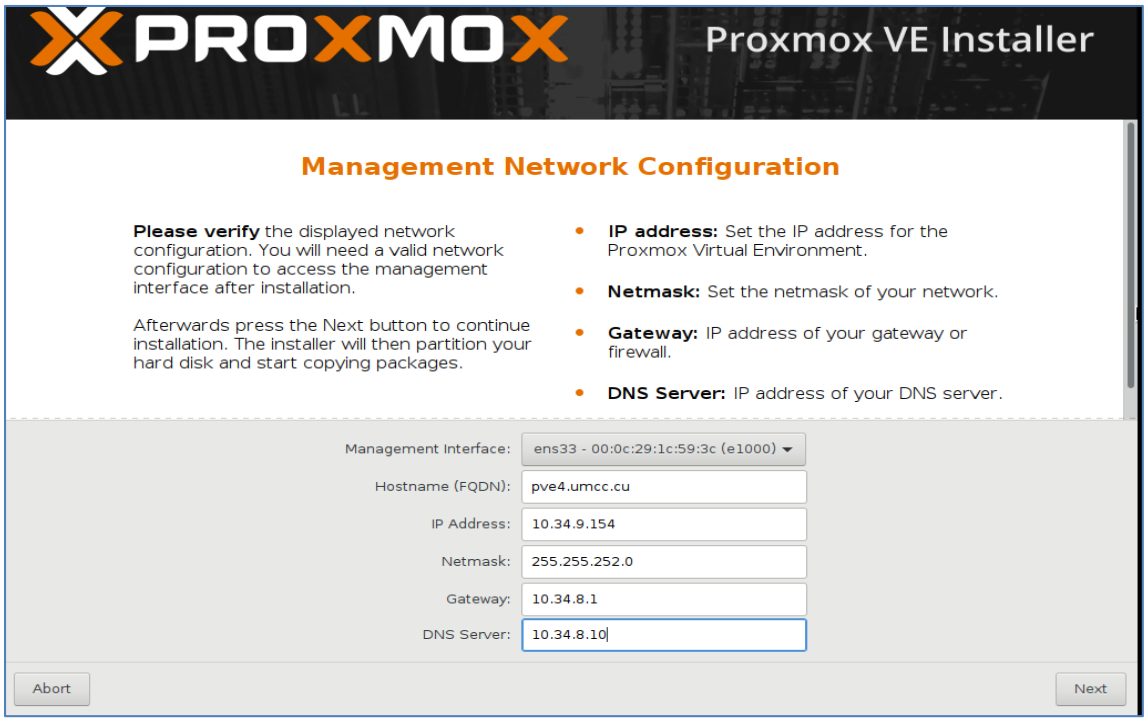
WAIS: (en inglés ***Wide Area Information Servers)***, es un sistema de búsqueda de texto distribuido, que usa el protocolo estándar cliente-servidor para buscar bases de datos indexadas en computadoras remotas.

WAN. (Wide Area Network). Es una interconexión de dispositivos que cubren un área geográfica grande (ciudades, países, continentes).

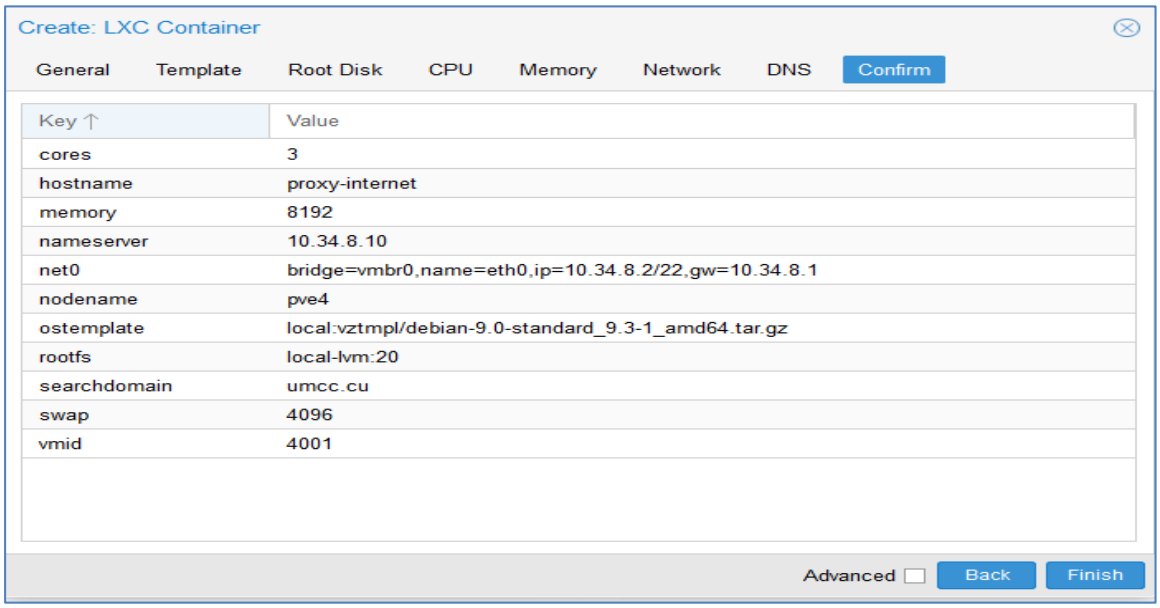
Anexos

Anexo 1. Instalación de Proxmox.

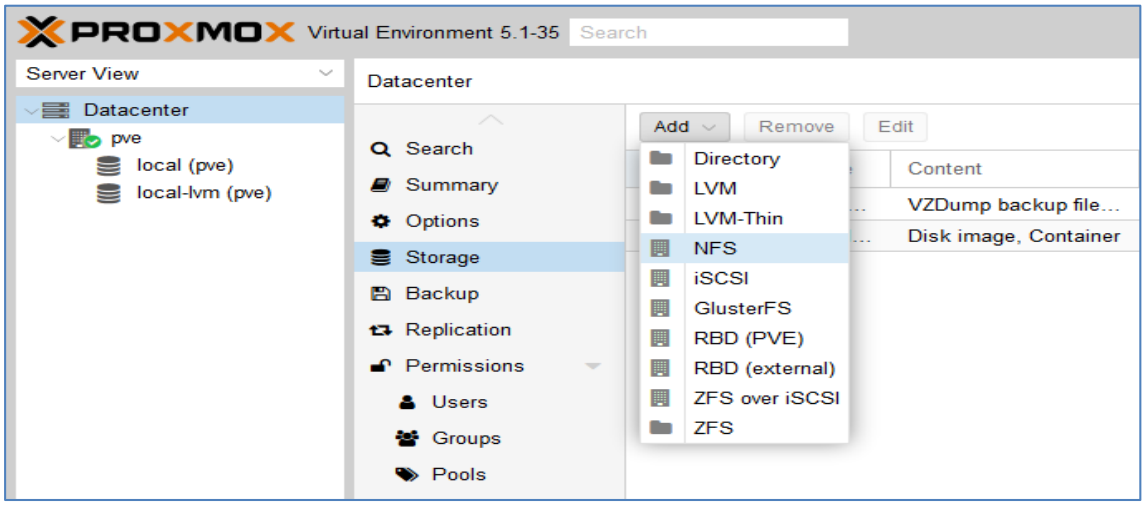

PROXMOX
Proxmox VE Installer
Location and Time Zone selection
The Proxmox Installer automatically makes location based optimizations, like choosing the nearest mirror to download files. Also make sure to select the right time zone and keyboard layout.
Press the Next button to continue installation.
Country: The selected country is used to choose nearby mirror servers. This will speedup downloads and make updates more reliable.
Time Zone: Automatically adjust daylight saving time.
Keyboard Layout: Choose your keyboard layout.
Country
Cuba
Time zone
America/Havana
Keyboard Layout
U.S. English
Abort
Next

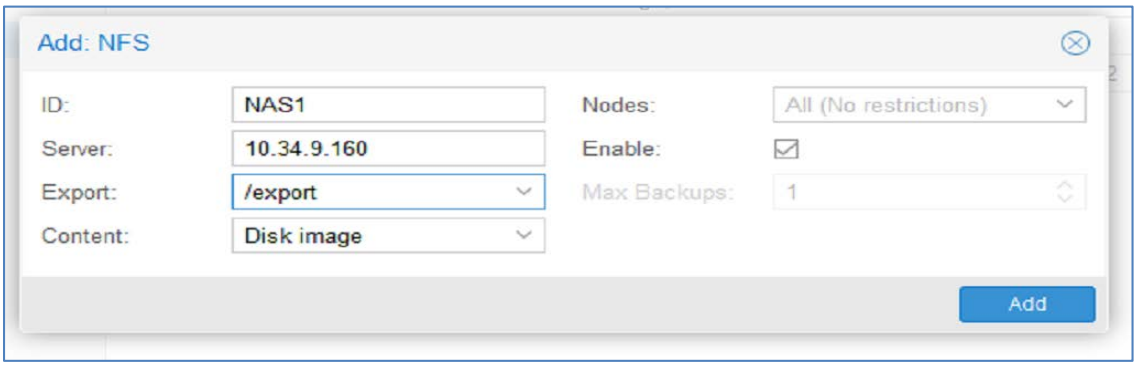

PROXMOX
Proxmox VE Installer
Management Network Configuration
Please verify the displayed network configuration. You will need a valid network configuration to access the management interface after installation.
Afterwards press the Next button to continue installation. The installer will then partition your hard disk and start copying packages.
IP address: Set the IP address for the Proxmox Virtual Environment.
Netmask: Set the netmask of your network.
Gateway: IP address of your gateway or firewall.
DNS Server: IP address of your DNS server.
Management Interface:
ens33 - 00:0c:29:1c:59:3c (e1000)
Hostname (FQDN):
pve4.umcc.cu
IP Address:
10.34.9.154
Netmask:
255.255.252.0
Gateway:
10.34.8.1
DNS Server:
10.34.8.10
Abort
Next

Anexo 2. Crear un Container en Proxmox.

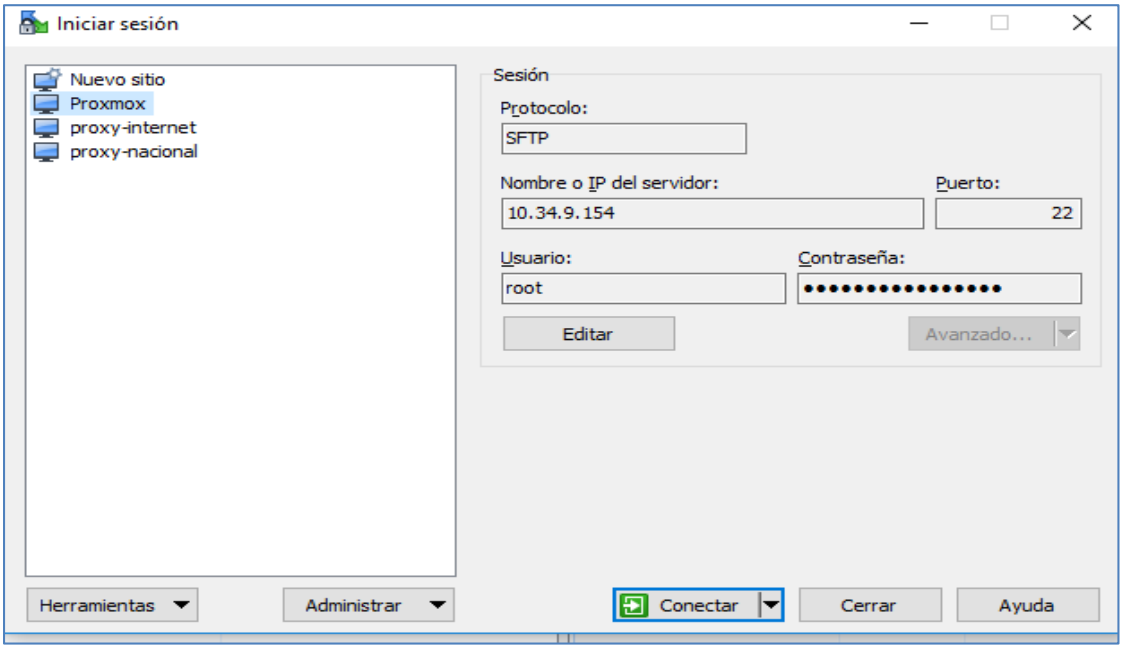


Anexo 3. Adicionar un Servidor NAS como Disco Duro en Proxmox.

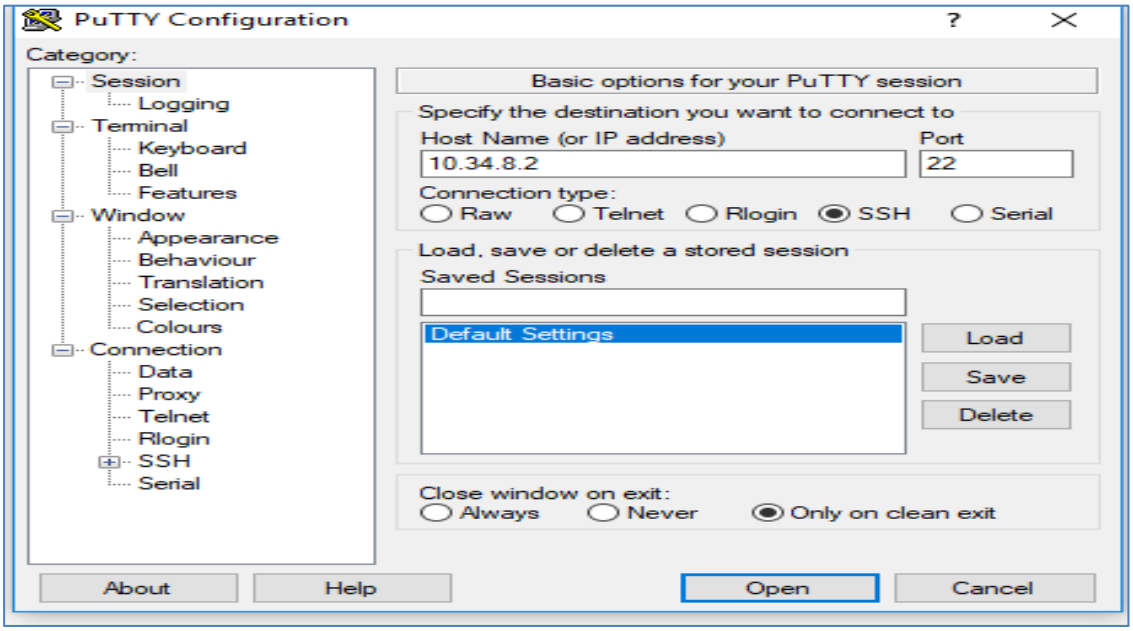




Anexo 4. Herramienta WinSCP.



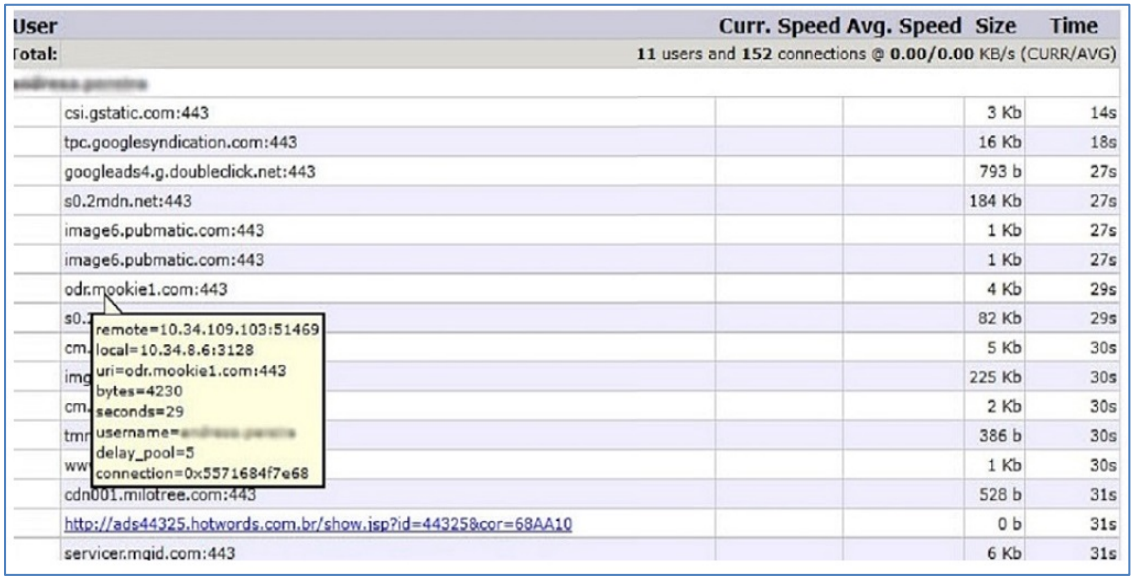
Anexo 5. Herramienta de administración SSH Putty.



Anexo 6. Configuración de SquidGuard.

```
###-----Configuración de SquidGuard-------
###
###---Cuidado:No use comentarios dentro de  { }
###--Directorio BD---###
dbhome /var/lib/squidguard/db
###--Directorio de los Logs---###
logdir /var/log/squidguard
###----Categorias-----------###
dest porn {
    domainlist porn/domains
}
dest proxy {
    domainlist proxy/domains
}
dest webmail {
    domainlist webmail/domains
}
dest socialnetworking {
    domainlist socialnetworking/domains
}
dest games {
    domainlist games/domains
}
acl {
default {
            pass !porn !proxy !webmail !socialnetworking !games !dialers all
            redirect http://localhost/denied.png
          }
}
```

Anexo 7. Monitoreo en tiempo real con Sqstat.



Anexo 8. Reglas de Iptables.

```
#!/bin/sh
## IPTABLES SCRIPT.
echo Aplying Firewall Rules...
## Rules...
## Flush all rules.
echo Deleting all rules...
iptables -F
iptables -X
iptables -Z
## Flush all rules in nat table.
iptables -t nat -F
echo [OK]
## Set default rules settings...
##   Set ACCEPT or DROP for default policy.
##   The DROP policy is better for increase security, but needed expert user.
echo Seting default policy...
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP
echo [OK]
## Begin filter rules
## Accept all loopback (lo) traffic.
echo Accepting all lookback traffic...
iptables -A INPUT -i lo -j ACCEPT
echo [OK]
## Allow ICMP ping command.
echo Accepting ICMP ping traffic...
iptables -A INPUT -i eth0 -s 10.34.8.121 -p icmp -m icmp --icmp-type 8 -j ACCEPT
echo [OK]
```

```
## Accept SSH connection (port 22 TCP) in the admin network.
echo Accepting SSH connection from admin network...
iptables -A INPUT -i eth0 -s 10.34.0.0/22 -p tcp --dport 22 -j ACCEPT
echo [OK]
## Accept HTTP traffic (port 80 TCP) in the admin network
echo Accepting HTTP connection from admin network
iptables -A INPUT -i eth0 -s 10.34.0.0/22 -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -i eth0 -s 10.34.8.0/22 -p tcp --dport 80 -j ACCEPT
echo [OK]
## Accept Proxy traffic (port 3128 TCP) from admin network
echo Accepting PROXY connection from admin network
iptables -A INPUT -i eth0 -s 10.34.0.0/15 -p tcp --dport 3128 -j ACCEPT
echo [OK]
## Accept RELATED and ESTABLISHED traffic.
echo Accepting RELATED and ESTABLISHED traffic
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
echo [OK]
echo Firewall is configured.
echo Verify this configuration typing "iptables -L -n"
```