REPÚBLICA DE CUBA

UNIVERSIDAD DE CIENFUEGOS
"CARLOS RAFAEL RODRÍGUEZ"

FACULTAD DE INGENIERÍA
CARRERA DE INGENIERÍA INFORMÁTICA

TÍTULO:

"IMPLEMENTACIÓN DE UN SISTEMA PROXY DE NAVEGACIÓN SEGURA EN EL GET DE CIENFUEGOS"

Presentado por:

Frank Manuel López Pérez-Borroto

Tutor:

Ing. Juan Manuel Castellanos Hernández

Cienfuegos, junio de 2017

AGRADECIMIENTOS Y DEDICATORIA

Agradezco a Dios primeramente y luego a toda mi familia, en especial mis padres y a mi esposa, que estuvieron al tanto de todo en esta ardua tarea que fue la Universidad, a mi tutor Juanma por haberme brindado sus conocimientos de manera incondicional. Esta tesis está dedicada a mis segundos padres que son mi abuela Ondina y mi tío Manuel donde quiera que estén gracias por todo, sin ustedes no sería quien soy y a mi hijo que cada día me ofrece más razones para vivir.

RESUMEN

Se propone implementar un sistema de navegación segura en el Grupo de Electrónica para el Turismo (GET) de Cienfuegos. En el existe un proxy de navegación privativo que impide actualización de parches de seguridad por motivos del pago de licencias, por lo que se necesita del uso de programas bajo licencias gratuitas que proporcionan una mayor seguridad y control de la entidad permitiendo actualizar esos programas. Se identificarán una serie de programas complementarios al proxy. Siendo todo esto validado una vez puesto en práctica a través de pruebas sobre su funcionamiento.

ÍNDICE

Contenido

Introducción

En la actualidad la seguridad es requisito indispensable para el correcto funcionamiento de las redes de computadoras. Muchas son las empresas en el mundo que tienen implementado un servidor proxy donde ofrecen la posibilidad de tener un control determinado sobre la red y los usuarios en general. En la computación y en especial en las redes de computadoras, el tema de seguridad es bastante amplio. En este están involucradas la información y las acciones que se pueden realizar sobre esta. Para mantener la seguridad de cualquier entorno de software se deben tener en cuenta diferentes conceptos:

- Autenticación:Es el servicio que trata de asegurar que una comunicación sea auténtica, es decir, verificar que el origen de los datos es el correcto, quién los envió, cuando fueron enviados y recibidos.[1]
- Autorización: Es el proceso de evaluación durante el cual se decide si la persona que está autenticada tiene derecho a hacer algo en determinadas circunstancias.
- Privacidad: En este proceso se garantiza el secreto y la privacidad de los datos. O sea, asegura que ninguna persona lea sus mensajes durante la conversación con el servidor.
- Disponibilidad: Se encarga de dar un servicio continuo e ininterrumpido. Mediante distintos mecanismos asegura que el fallo de un nodo no afecte las funcionalidades de un sistema.
- Integridad: Se encarga de asegurar que la información no sea cambiada o corrompida por terceras personas.

En el mundo actual se hace cada vez más común el uso de un servidor proxy , un servidor intermediario entre las computadoras de la red y el enrutador de conexión a Internet, de forma que cuando un usuario quiere acceder a Internet, su computadora realiza la petición al servidor proxy y es el proxy quien realmente accede a Internet, el servidor proxy se instala en un único ordenador de su red local, y permite que varios ordenadores conectados a una misma red local puedan compartir un mismo acceso a Internet o conexión a Internet de manera simultánea.

El ordenador en el que se debe instalar el servidor proxy puede ser un servidor profesional, o también puede ser un servidor normal o sea una máquina personal. El servidor proxy dará servicio a todos los ordenadores de su red local, sean estos de Windows, o cualquier otro sistema operativo. Esto es posible ya que el protocolo de red TCP/IP(protocolo de control de transmisión/protocolo de internet) fue creado precisamente para permitir la interconexión de redes y sistemas heterogéneos.[2].

La introducción de la informática en Cuba se hizo fundamentalmente sobre la base de programas privativos, aunque desde el año 2004 el Consejo de Ministros acordó la migración a plataformas de código abierto de forma continua y organizada. Actualmente existe una estrategia nacional, con acciones y tareas específicas, tanto organizativas como técnicas, legales y de capacitación, pero es un proceso que se desarrolla con altibajos.

Para Cuba es indispensable la migración a software libre porque garantizaría su independencia tecnológica y su soberanía. Desde el punto de vista económico ahorraría el pago de millonarias sumas de dinero por concepto de licencias de propiedad intelectual, lo cual limitaría el proceso de informatización de la sociedad. Al mismo tiempo, y contrariamente a lo que se cree, las plataformas de código abierto son más estables cuando se utilizan en las redes, seguras (reciben pocos ataques de virus), y demandan máquinas de menos prestaciones.

En Cuba muchas empresas tienen implementados estos servidores como una solución viable y factible a la navegación segura. El Grupo de Electrónica para el Turismo (GET) de Cienfuegos es una de las excepciones pues se implementa Kerio un proxy privativo por lo que se sienten necesitados de migrar a software libre, porque están muy limitados a una mejoría en cuanto a versiones más avanzadas obviando soporte actualizado dejando un tanto insegura la red actual.

Situación problémica:

Actualmente el GET de Cienfuegos no cuenta con el servicio de un sistema proxy de navegación segura gratuito y con código abierto que le permita explotar todas las ventajas que este brinda, además la dependencia de soporte es absoluta y costosa al tratarse de un proxy privativo por lo tanto evita que se actualicen parches de seguridad entre otras ventajas.

A partir de la situación problémica se enunció el siguiente **problema científico:**

¿Cómo implementar un sistema de proxy de navegación segura en el GET de Cienfuegos acorde a sus necesidades?

Identificándose como **objeto de estudio:** la seguridad en los sistemas proxy web y **campo de acción** la seguridad en los sistemas proxy web en el GET de Cienfuegos

Justificación del estudio:

No existe en el GET de Cienfuegos un sistema proxy de navegación segura gratuito.

Objetivos:

Objetivo general:

- Implementar un sistema de proxy de navegación segura en el GET de Cienfuegos.

Objetivos específicos:

- Identificar programas y protocolos adecuados para una mayor seguridad y control del sistema proxy en el GET de Cienfuegos.
- Selección de herramientas a utilizar en el sistema.
- Diseñar el sistema proxy de navegación segura.
- Validar el sistema proxy de navegación segura.

Interrogantes Científicas.

¿Cuáles son los programas y protocolos necesarios para una mayor seguridad y control en el GET de Cienfuegos?

¿Qué diseñó proponer para el sistema proxy de navegación segura en el GET de Cienfuegos?

¿Cómo implementar y validar el sistema proxy de navegación segura en el GET de Cienfuegos?

Tareas de investigación.

- Estudio de los protocolos referentes a la seguridad en el sistema proxy.
- Selección de las características a analizar en la red de datos
- Configuración del sistema proxy.
- Implementación del sistema proxy.
- Validación del sistema proxy.

Aporte práctico:

Con la ejecución del proyecto se dan soluciones con herramientas actualizadas a la problemática existente, permitiendo facilidades en el control de acceso de los usuarios a internet del GET de Cienfuegos, sin depender de un gasto adicional en las licencias requeridas para los programas. Además, estando todo legalizado bajo las licencias gratuitas de programas libres, creando la posibilidad de actualizar los programas implementados y modificarlos sin ninguna restricción. Además, ahorrando 285 USD anuales por la licencia y por cada usuario se incrementaría 30 USD más.

Para una mejor comprensión del trabajo el mismo está estructurado de la forma siguiente: Introducción, Capítulos, Conclusiones y Recomendaciones.

Estructura del Trabajo:

Introducción

Capítulo 1: Fundamentos teóricos.

Se realiza un estudio de los protocolos y programas referentes a la seguridad en los proxys web, evaluándose su utilización en diferentes casos de uso, a partir de los cuales se seleccionará los más convenientes para el GET de Cienfuegos.

Capítulo 2: Diseño de un sistema de proxy web seguro en el GET de Cienfuegos.

Se selecciona la variante a emplear y se describen las características y especificidades del GET de Cienfuegos. Se realiza una comparación de acuerdo a las ventajas y desventajas que presentan los programas que se integran en el sistema, el programa más adecuado como proxys web, filtrado web, control detallado de logs, los que se usan para limitar las cuotas a los usuarios y el método de autenticación más apropiado.

Capítulo 3: Implementación y validación del sistema proxy web segura en el GET de Cienfuegos.

Se implementa el sistema proxy de navegación segura web propuesto de acuerdo con el estudio realizado con las herramientas adecuadas para el GET de Cienfuegos, se comprueba que todo lo implementado esté funcionando tal y como se quiere.

Capítulo 1 Fundamentos teóricos

1.1 Introducción

El uso de un sistema proxy de navegación segura hoy en día se ha convertido en algo imprescindible. El hecho de tener la mejor tecnología no garantiza seguridad y fiabilidad, se necesita de una buena estructura en la implementación de un buen proxy de navegación y programas que lo complementen.

1.2 Servidores Proxys

Un proxy permite conectarnos a un equipo de forma indirecta. Cuando un equipo conectado a una red desea acceder a una información o recurso de Internet (llámese ver una página electrónica, descargar un fichero mp3, avi o de cualquier formato), es realmente el proxy quien realiza la comunicación y a continuación envía el resultado al equipo que solicitó dicha información.[3]

Los servidores proxy también permiten proteger y mejorar el acceso a las páginas web al conservarlas en la caché. De este modo, cuando un navegador envía una petición para acceder a una página electrónica, que previamente ha sido almacenada en la caché, la respuesta y el tiempo de visualización es más rápido. [4]

1.2.1 Squid:

Es un servidor web proxy-caché con Licencia Pública General (GPL,*General Public Licence*) cuyo objetivo es funcionar como proxy de la red y también como zona caché para almacenar páginas web entre otros. [5]

Hay que tener en cuenta que la mayoría de los servidores web permiten la configuración como proxy-caché, pero Squid sólo es un proxy y no puede servir páginas por sí mismo.

Cuando se dice que Squid también funciona como caché significa que está guardando copia de los datos obtenidos de otras peticiones y de esa forma acelera el acceso a estos datos si se producen peticiones similares. Sólo se accederá de nuevo a las páginas originales cuando se detecte que se han producido modificaciones, es decir los datos almacenados difieren de los datos en el servidor de Protocolo de Transferencia de Hipertexto (*HTTP,Hypertext Transfer Protocol*) de origen. Normalmente no existe una sola caché, sino que se tienen varios servidores (en máquinas diferentes) relacionados entre sí mediante una estructura en árbol.

Como resumen, las principales funciones de Squid son las siguientes:

- Permite el acceso web a máquinas privadas que no están conectadas directamente a Internet.
- Controla el acceso web aplicando reglas.
- Registra el tráfico web desde la red local hacia el exterior.
- Controla el contenido web visitado y descargado.
- Controla la seguridad de la red local ante posibles ataques, en el sistema, etc.
- Funciona como una caché de páginas electrónicas, es decir, almacena las páginas visitadas por los usuarios y de esta manera las pueden enviar a otros usuarios sin tener que acceder a Internet de nuevo.
- Guarda en caché las peticiones al Sistema de Nombres de Dominio (DNS, *Domain Name System Server*) e implementa una caché para las conexiones fallidas.
- Registra logs de todas las peticiones cursadas.
- Soporta el Protocolo de Caché de Internet (ICP*, Internet Cache Protocol*) que permite integrar varias caché que colaboran y permite crear jerarquías de cachés y el intercambio de datos.

Como consecuencia de estas funciones, la implantación de un servidor proxy-caché en una red proporciona las siguientes ventajas:

Reduce los tiempos de respuesta:

Si la página web que se solicita está en la caché del servidor, ésta se sirve sin necesidad de acceder de nuevo al servidor original, con lo cual se ahorra tiempo.

Disminuye el tráfico en la red y el consumo de ancho de banda:

Si la página web está almacenada en la caché del servidor, la petición no sale de la red local y no será necesario hacer uso de la línea exterior consiguiendo así un ahorro en la utilización del ancho de banda.

Cortafuegos:

Cuando se utiliza un servidor proxy-caché, éste comunica con el exterior, y puede funcionar como cortafuegos, lo cual aumentará la seguridad del usuario respecto a la información a la que se acceda.

Filtrado de servicios:

Es posible configurar el servidor proxy-caché dejando sólo disponibles aquellos servicios de Protocolo de Transferencia de Hipertexto (HTTP *,Hypertext Transfer Protocol*) y el Protocolo de Transferencia de Archivos (FTP*,File Transfer Protocol*,) que se consideren necesarios, impidiendo la utilización del resto.

1.2.2 Tinyproxy:

Tinyproxy es un programa flexible que puede manejar muchas de las mismas funciones de un proxy Squid. Se trata de un pequeño programa en particular, que puede ser apropiado para un servidor menos robusto que no puede manejar un squid. Tinyproxy es un sistema modular, así que sus principales componentes se instalan inicialmente, y luego se añaden características específicas, si se desea.[6]

Esto hace que sea posible utilizar el mínimo de recursos del sistema, así como el espacio en disco duro para el programa. Una ventaja adicional a un entorno modular es el grado de personalización que permite a este programa. Y es posible configurar Tinyproxy para personalizar su servidor, la red, la base de usuarios y funciones requeridas sin la participación de las herramientas o utilidades adicionales que no se utilizan.

1.2.3 WebCleaner:

WebCleaner es un servidor proxy HTTP que además de optimizar tus páginas Webs permite usar normas de filtrado de Lenguaje de Marcas de Hipertexto (*HTML*

,*HyperText Markup Language*) e incluso bloquear ciertas animaciones y pop-ups, aumentando así la seguridad.[7]

Este programa está bajo licencia GPL por lo que se puede hacer un uso máximo productivo del mismo. Puede deshabilitar el Formato de Intercambio Gráfico (*GIF*, *Graphics Interchange Format*) animados, comprimir documentos sobre la marcha (con gzip), agregar y quitar encabezados HTTP, y eliminar HTML no deseado (anuncios, JavaScript, etc.).

1.2.4 Kerio:

Es un servidor proxy privativo que cuenta con la prevención de intrusiones, filtrado de contenido, el informe de actividades, gestión de ancho de banda y redes privadas virtuales. Dentro de sus características principales se encuentran:

- Inspección profunda de paquetes
- Inspección de protocolo
- Servidor de Protocolo de Configuración Dinámica de Host (*DHCP, Dynamic Host Configuration Protocol*)
- Posee un filtrado de dirección física (MAC*, Media Access Control*)
- Detección de intrusos
- Reglas basadas en tiempo
- Informes detallados de uso: Sitios web, protocolos y ancho de banda
- Múltiples direcciones IP en una única interfaz de red
- Sistema de Nombres de Dominio (DNS,Domain Name System) dinámico
- Tabla de enrutamiento personalizable
- Monitoreo de actividades del host en tiempo real
- Monitoreo de uso de ancho de banda de interfaz en tiempo real
- Autenticación Kerberos/NTLM

1.3 Programas para el filtrar contenidos de la web

El filtrado es una de las piedras angulares de la seguridad en aplicaciones web. Es el proceso por el cual se prueba la validez de los datos. Si se asegura que los datos son filtrados apropiadamente al entrar, puedes eliminar el riesgo de que datos contaminados sean usados para provocar funcionamientos no deseados en la aplicación.

Existen muchos puntos de vista diferentes sobre cómo realizar el filtrado o proceso de limpieza. Lo que usualmente se recomienda es ver al filtrado como un proceso de inspección, no se deberá tratar de corregir los datos, es mejor forzar a los usuarios a jugar con las reglas válidas.[8]

Al usar listas blancas se asume que los datos son inválidos a menos que prueben ser validos al encontrarse patrones coincidentes. Una limitante de usar este punto de vista es considerar inválidos datos que debieron considerarse válidos pero que no fueron tomados en cuenta patrones similares al construir la lista blanca.

1.3.1 DansGuardian

Es un programa de control de contenidos, diseñado para controlar el acceso a sitios web. Incluye un filtro de virus, importante en cualquier sistema operativo, es usado principalmente en instituciones de educación, gobierno y empresas. Se caracteriza por su alto grado de flexibilidad y adaptación de la implementación.[9]

Tiene la particularidad de trabajar conjuntamente con algún servidor Proxy, como por ejemplo Squid u otro Proxy caché similar a este que se encuentre obviamente dentro de nuestra red local. Se encuentra en una posición intermedia de comunicación entre el Navegador web del cliente y el servidor Proxy, de esta manera intercepta y modifica toda petición que se realiza y que el servidor atienda. Es aquí en donde su trabajo de filtrado de contenido funciona con facilidad.

Va a permitir controlar y habilitar el contenido que va a ser navegable desde nuestra red, es de gran utilización dentro de cualquier empresa para evitar distracciones de los empleados en el área laboral como así también en el hogar, sobre todo cuando se encuentran niños frente a los ordenadores expuesto a todos los contenidos que se encuentra en la red, como por ejemplo contenido para adultos u otro contenido que la empresa quiera restringir.

Características de DansGuardian:

Esta herramienta comparte y fomenta la filosofía de código abierto, por tal motivo se puede ver y editar los códigos fuentes de la aplicación escrita en el lenguaje de programación C++, por último, una particularidad mucho mayor es que permite realizar una configuración sumamente flexible para adaptarse a las necesidades de los usuarios.

Una de las ventajas que posee DansGuardian y que se repite muchas veces con otros Servicio o Servidores que se instalan en los sistemas GNU, es que provee una configuración por defecto totalmente funcional de hecho ya es posible ver como filtra los sitios prohibidos para menores, pero recordar que existe la posibilidad de realizar una configuración totalmente personalizada a través de sus diferentes archivos de configuración.

1.3.2 E2Guardian:

E2guardian es un filtro de contenido web de código abierto, filtra los contenidos de páginas basado en muchos métodos incluyendo la correspondencia de frase, encabezado, filtrado de Localizador Uniforme de Recursos (*Uniform Resource Locator,* URL**),** etc.[10] No puramente el filtro basado en una prohibida lista de sitios. Es un proxy de filtrado de contenido que funciona en conjunto con proxy de almacenamiento en caché como Squid u Oops.E2guardian es un tenedor de DansGuardian con características adicionales.

Posee un Sistema integrado de plugins de escáner de contenido, que incluye:

- Dominios y *URL* de la lista blanca
- Dominios de la lista negra y *URL*
- Dominios y *URL* de *Greylist*
- Negar expresiones regulares en *URL*, contenido corporal y encabezado (también en modo *Greylist*)
- Reemplazo de expresión regular de URL para que pueda, por ejemplo, forzar la búsqueda segura en los motores de búsqueda

- Exploración profunda de *URL*, por ejemplo, bloquear imágenes en imágenes de Google
- Bloqueo avanzado de anuncios
- Actualizaciones para manejar todas las tendencias actuales de la tecnología web
- Bloqueo de Capa de Puertos Seguros (*SSL,Secure Sockets Layer*)
- Limitar el tamaño del POST (subir)
- La derivación temporal proporciona una capacidad de "clic para reconocer"
- Referir las excepciones basadas en la *URL* en la *URL* de referencia

1.3.3 Nxfilter:

Es una aplicación de filtrado de DNS que te permite bloquear con rapidez cualquier sitio web malintencionado que podría afectar la seguridad de tu ordenador. Pero la utilidad va un poco más lejos y también te permite supervisar el uso de la red.[11]

Además, controla el tráfico hacía nuestro equipo desde sitios y páginas electrónicas e impide el acceso de lo que no se considera seguro. Trabaja controlando nombres de dominio y categorías de contenido. Permite así mismo la inspección de paquetes DNS con el fin de proteger el ordenador ante la actividad de virus. Funciona con uno o con varios ordenadores al mismo tiempo.

Sólo hay que instalar NxFilter en una computadora, en donde actuará como un servidor proxy DNS. De esta forma todo el tráfico entrante desde Internet se dirigirá a todos los equipos a través de este servidor. Se debe cambiar la configuración DNS de todos los ordenadores, conectados a la red, que se quieran proteger. Habrá que utilizar la que proporciona el proxy creado por NxFilter.

1.3.4 SquidGuard:

SquidGuard es un programa de redireccionamiento de *URL,* que puede utilizarse para el control de contenido de sitios web a los que los usuarios pueden acceder. Se escribe como un complemento para Squid y utiliza listas negras para definir sitios para los que se redirige el acceso. SquidGuard debe instalarse en un equipo Unix o

Linux, como un equipo servidor. El filtrado del programa se extiende a todos los equipos de una organización, incluidos los equipos Windows y Macintosh.

Principales características:

• Autenticación contra base de datos mysql.

•Comportamiento predeterminado configurable.

•Otras mejoras y correcciones de errores.

1.4 Programas para el control de las cuotas de usuarios

1.4.1 Squish:

Un programa bajo Licencia General Pública (GPL, General Public License) ofrece el código fuente y es libre de costo alguno, permite un mayor control de los usuarios de forma tal que se puede restringir el tiempo de navegación y el ancho de banda por la que se navega por Internet, además limitar la cantidad de datos que se descargan, esto se especificar por día, por semanas o por mes.

1.5 Programas para el análisis de logs

1.5.1 Sarg

Generador de informes del Squid **(***Sarg,Analysis Report Generator***)**: es una herramienta, basada en programa libre, de análisis de registros (logs) de Squid, tiene soporte para generar reportes automatizados o manualmente.[12]

Principales características:

- Es una herramienta de código abierto
- Permite analizar los archivos de registro del Squid
- Genera informes muy completos en formato HTML con información sobre usuarios, direcciones IP, sitios de acceso máximo, uso total de ancho de banda, tiempo transcurrido, descargas, sitios electrónicos denegados, informes diarios, e informes mensuales.

1.5.2 Free-Sa:

Es el analizador estadístico para los demonios de los archivos de registro similares a SARG. Sus principales ventajas están en la velocidad, trabajo en multiplataforma y el cumplimiento de código generado HTML / Hojas de Estilo en Cascada (*CSS,Cascading Stylesheets*) en sus informes. [13]

Sus características principales son:

- Facilidad de uso
- Control del uso del tráfico de los usuarios
- Ayuda a controla las políticas de seguridad

1.5.3 Lightsquid:

Es un Analizador estadístico de logs sencillo, dentro de sus características se encuentran:

- Instalación rápida y sencilla
- Analizador de registro rápido genera poco por archivo de datos de usuario
- Plantilla *HTML* para el diseño
- No se requiere base de datos
- Sin módulo Perl adicional informes diversos
- Soporte de grupos de usuarios
- Informe de gráficos (v 1.6+)
- Nombre real (v 1.6+)
- Interfaz multilingüe[13]

1.6 Protocolos para la seguridad en la autentificación

La seguridad e integridad de sistemas dentro de una red puede ser complicada. Puede ocupar el tiempo de varios administradores de sistemas sólo para mantener la pista de cuáles servicios se están ejecutando en una red y la manera en que estos servicios son usados. Más aún, la autenticación de los usuarios a los servicios de red puede mostrarse peligrosa cuando el método utilizado por el protocolo es inherentemente inseguro, como se evidencia por la transferencia de contraseñas sin encriptar sobre la red bajo los protocolos FTP y el protocolos para acceder de manera remota a otra computadora (*Telnet,Telecommunication Network*) o. Kerberos es una forma eliminar la necesidad de aquellos protocolos que permiten métodos de autenticación inseguros, y de esta forma mejorar la seguridad general de la red.

1.6.1 Kerberos

Es un protocolo de seguridad donde que usa una criptografía de claves simétricas para validar usuarios con los servicios de red — evitando así tener que enviar contraseñas a través de la red. Al validar los usuarios para los servicios de la red por medio de Kerberos, se frustran los intentos de usuarios no autorizados que intentan interceptar contraseñas en la red.

Niveles de protección de Kerberos

Autenticación: Prueba que el usuario es quien dice ser. Puede ser que la autenticidad se establezca al inicio de la Conexión de red y luego se asuma que los siguientes mensajes de una Dirección de red determinada se originan desde la parte autenticada.

Integridad de datos: Asegura que los datos no se modifican en tránsito. Se requiere autenticación de cada mensaje, sin importar el contenido del mismo. Esto se denomina mensajes seguros.

Privacidad de datos:

Asegura que los datos no son leídos en tránsito. En este caso, no sólo se autentica cada mensaje, sino que también se cifra. Estos mensajes son privados.

Arquitectura de Kerberos: Un servidor Kerberos se denomina KDC (Centro de Distribución Kerberos), y provee dos servicios fundamentales: el de autenticación (AS, Authentication Service) y el de tickets (TGS, Ticket Granting Service). El primero tiene como función autenticar inicialmente a los Clientes y proporcionarles un ticket para comunicarse con el segundo, el servidor de tickets, que proporcionará a los clientes las credenciales necesarias para comunicarse con un servidor final que es quien realmente ofrece un servicio. Además, el servidor posee una Base de datos de sus clientes (usuarios o Programas) con sus respectivas claves privadas, conocidas únicamente por dicho servidor y por el Cliente que al que pertenece. La arquitectura de Kerberos está basada en tres objetos de seguridad: Clave de Sesión, Tique y Autenticador.[14]

Kerberos se diferencia de los métodos de autenticación de tipo nombre de usuario/contraseña. En lugar de autenticar cada usuario en cada servicio de red, Kerberos utiliza encriptaciones simétricas y un servicio adicional confiable (un KDC), para autenticar usuarios en conjunto de servicios de red. Cuando un usuario se autentica en el KDC, el KDC devuelve a la máquina del usuario en cuestión un comprobante específico para esa sesión, y cualquier servicio fuera de Kerberos busca el comprobante en la máquina del usuario, en lugar de pedir que el usuario se autentique utilizando una contraseña.

Cuando un usuario de una red se autentica en su estación de trabajo, su principal es enviado al KDC como parte de un pedido para un TGT del servidor de Autenticación. Este pedido puede ser enviado por el programa de autenticación de modo que sea transparente para el usuario, o puede ser enviado por el programa Kinit luego que el usuario se haya autenticado.

El KDC entonces verifica con el principal en su base de datos. Si el principal es encontrado, el KDC crea un TGT, que se encripta usando la clave del usuario y se lo devuelve a ese usuario.

La autenticación, o programa Kinit en el cliente, se encarga de desencriptar el TGT utilizando la clave del usuario, que se analiza desde la contraseña del usuario. La clave del usuario es utilizada sólo en la máquina cliente y *no* se transmite en la red.

El TGT es configurado para que caduque en un determinado período de tiempo (generalmente de diez a veinticuatro horas), y es almacenado en el caché de credenciales en la máquina del cliente. Un tiempo de expiración es definido para que, en el supuesto caso que exista un TGT vulnerado, pueda ser utilizado por un atacante sólo durante un breve período de tiempo. Luego que se ha emitido un TGT, el usuario no necesita reingresar su contraseña hasta que este no expire, o hasta que haya finalizado su sesión, y haya vuelto a iniciarla.

Siempre que el usuario necesite acceso a un servicio de red, el programa del cliente utiliza el TGT para pedirle al TGS un nuevo comprobante específicamente para ese servicio. El comprobante del servicio es entonces utilizado para autenticar de manera transparente al usuario frente al servicio en cuestión.

El sistema Kerberos se vuelve vulnerable cada vez que un usuario en la red se valida contra un servicio no mercerizado y envía una contraseña en la red en texto plano. Por lo tanto, no se recomienda el uso de servicios fuera de Kerberos. Estos servicios incluyen Telnet y FTP. Se acepta el uso de otro tipo de protocolos encriptados, tales como SSH o servicios seguros SSL, pero no es ideal.

1.6.2 NTLM

NTLM es un conjunto de protocolos de seguridad de sesión y autenticación utilizados en varias implementaciones de protocolo de red de Microsoft y soportado por NTLM *Security Support Provider* ("NTLMSSP"). Originalmente utilizado para la autenticación y negociación de DCE / RPC seguro, NTLM también se utiliza en todos los sistemas de Microsoft como un mecanismo de inicio de sesión único integrado. Probablemente es mejor reconocido como parte de la pila "Autenticación integrada de Windows" para la autenticación HTTP; Sin embargo, también se utiliza en las implementaciones de Microsoft el protocolo para Transferencia Simple de Correo (SMTP,*Simple Mail Transfer Protocol*) , o Protocolo de Oficina de Correo(POP3,*Post Office Protocol*), Protocolo de Acceso a Mensajes de Internet(IMAP,*Internet Message Access Protocol*) (todo parte de Exchange), CIFS(*Common Internet File System*) / SMB un protocolo de red que permite compartir archivos, Telnet, Protocolo de Inicio de Sesiones (SIP, *Session Initiation Protocol*) y posiblemente otros.[15]

El proveedor de soporte de seguridad de NTLM proporciona servicios de autenticación, integridad y confidencialidad dentro del marco de interfaz de proveedor de soporte de seguridad de Windows (SSPI). SSPI especifica un conjunto básico de funcionalidad de seguridad que se implementa mediante el apoyo a los proveedores;

Autenticación: NTLM proporciona un mecanismo de autenticación de desafío-respuesta, en el que los clientes pueden probar sus identidades sin enviar una contraseña al servidor.

Firma - El NTLMSSP proporciona un medio de aplicar una "firma" digital a un mensaje. Esto asegura que el mensaje firmado no ha sido modificado (accidental o intencionalmente) y que esa parte firmante tiene conocimiento de un secreto compartido. NTLM implementa un esquema de firma simétrica MAC; Es decir, una firma válida sólo puede ser generada y verificada por partes que poseen la clave compartida común.

Sellado - El NTLMSSP implementa un mecanismo de cifrado de clave simétrica, que proporciona confidencialidad del mensaje. En el caso de NTLM, el sellado también implica la firma (un mensaje firmado no es necesariamente sellado, pero todos los mensajes sellados están firmados).

NTLM ha sido en gran medida suplantado por Kerberos como el protocolo de autenticación de elección para los escenarios basados en el dominio. Sin embargo, Kerberos es un esquema de terceros de confianza y no se puede utilizar en situaciones en las que no existe un tercero de confianza; Por ejemplo, servidores miembros (servidores que no forman parte de un dominio), cuentas locales y autenticación a recursos en un dominio no confiable. En estos escenarios, NTLM sigue siendo el principal mecanismo de autenticación (y probablemente será durante mucho tiempo).

1.6.3 Digest

Es un método de autenticación que mejora la autenticación básica proporcionando una manera de autenticar sin tener que transmitir la contraseña de manera clara en un texto a través de la red.[16]

La autentificación Digest fue desarrollada de forma compatible y como una alternativa más segura a la autentificación básica pero no es uno de los protocolos denominados seguros comparados con aquellos que utilizan mecanismos de clave pública SSL o mecanismos de cambio de tique como el Kerberos. La autentificación Digest no posee una fuerte autentificación ni ofrece protección de confidencialidad fuera de la protección de la contraseña el resto de la petición y respuesta van en texto plano.

1.6.4 LDAP

Protocolo Ligero de Acceso a Directorios es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. También es considerado una Base de datos a la que pueden realizarse consultas. Está basado en el estándar X.500. 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, entre otros datos). Además es un protocolo de acceso unificado a un conjunto de información sobre una red.[17]

En resumen, es un método de autenticación en el que una solicitud de un usuario potencial es recibida por un servidor de red y luego enviada a un controlador de dominio. El controlador de dominio envía una clave especial, llamada clave de sesión de resumen al servidor que recibió la solicitud original. El usuario debe entonces producir una respuesta, que se cifra y se transmite al servidor. Si la respuesta del usuario es correcta, el servidor concede al usuario acceso a la red, al sitio Web o a los recursos solicitados para una única sesión.

1.7 Conclusiones Parciales

Existe una variedad en los programas existentes tanto para proxys web, filtrado web, control de logs y protocolos para la seguridad por lo que se necesita de una comparación que permita escoger los que más se adecuen al GET de Cienfuegos.

Capítulo 2 : Diseño de un sistema de proxy web seguro en el GET de Cienfuegos

2.1 Introducción.

Hoy en día en el mundo existe una gran variedad de aplicaciones destinadas a la implementación de proxys de navegación, filtrado de contenido web, análisis de los logs del proxy, tanto, privativas como de carácter libre. Entre esta gran variedad se elegirán a partir de una comparación de las mismas las más adecuadas para el GET de Cienfuegos y sobre todo centradas en programas libres, ya que en nuestro país se dificultan el uso de programas privativos por lo costoso del pago de licencias.

2.2 Caracterización de la red de Datos del Grupo Electrónico para el Turismo de Cienfuegos.

En el GET de Cienfuegos existen un total de 12 usuarios donde 6 de ellos tienen acceso a navegación internacional y los restantes Nacional. Cuentan con 3 máquinas corei3 con 4gb de memoria, estas como servidores. Todas tienen instalado el programa Proxmox que se utiliza para virtualizar máquinas en la red, se encuentran con la versión más actualizada hasta el momento. El primer servidor Proxmox tiene virtualizado 4 servicios, el servidor de dominio Windows server R2, el servicio de VoIP se usa para establecer llamadas por la red, el Squid como servidor Proxy, el chat(*openfire*) y el cortafuego implementado a través de IPtables. El segundo servidor tiene virtualizado el Windows Server 2016 que se va a usar para actualizar los parches de seguridad del servidor de dominio principal.

El tercer servidor tiene además un sistema de detección de intrusos, el analizador de logs (SARG) y una lista de repositorios de Linux. Todos estos servidores conectados a un enrutador. Existen también 12 ordenadores en la red,4 teléfonos y 2 disco duros en la red llamados *own cloud.* La salida de esta red está dada por un módem de Línea de Abonado Digital Asimétrica (ADSL, *Asymmetric Digital Subscriber Line)*que se conecta directamente con un Squid proxy padre que es el que permite la conexión a internet y además se encuentra conectado con la Intranet del Ministerio del Turismo 10.12.0.0/16 ver todo en la figura 1.

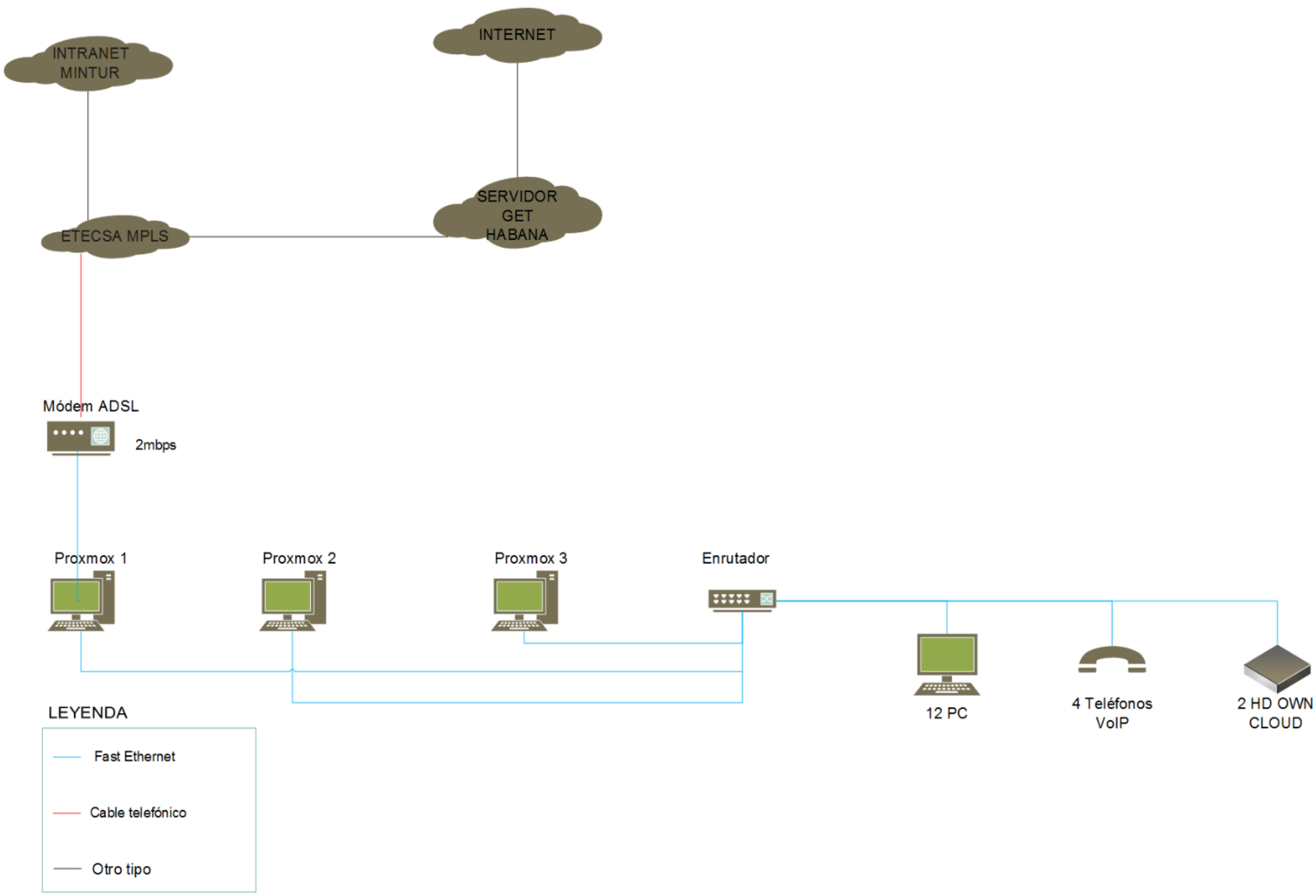


Figura 1: Caracterización de la red de GET de Cienfuegos

2.3 Comparación entre los proxys de navegación.

2.3.1 Ventajas y Desventajas del Kerio

Ventajas:

- Inspección profunda de paquetes
- Inspección de protocolos
- Inspección del estado de los paquetes
- Servidor DHCP

- Reenvío de *DNS*
- Asignación de Traducción de Direcciones de Red (NAT,*Network Address Translation*)
- Filtrado de *MAC*
- Detección de intrusos
- Red de invitado con portal cautivo
- Asistente de configuración de reglas de tráfico
- Reglas basadas en tiempo
- Inspección de *Protocolo Seguro de Transferencia de Hipertexto(HTTPS, Hypertext Transfer Protocol Secure*)
- Capacidad de excepción de la regla
- Límites de conexión
- Múltiples direcciones IP en una única interfaz de red
- DNS dinámico
- Tabla de enrutamiento personalizable
- Proxy inverso
- IPv4 simultáneo y soporte IPv6
- Traducción de prefijo de red IPv6

- La división de túnel u opción de túnel forzada
- Túneles de sitio a sitio múltiples/simultáneas
- Posee una Red Privada Virtual (Virtual Private Network , VPN) de cliente a sitio y de sitio a sitio
- Conexión opcional persistente
- Múltiples conexiones VPN almacenadas
- Fuerte encriptación SSL
- Soporta *VPN*
- Soporta *NAT*
- Enrutamiento automático o personalizado
- Módulo de reportes estadísticos de Kerio Control

- Informes detallados de uso: Sitios web, protocolos y ancho de banda
- Reportes individuales por usuario, grupos, o toda la red
- Reportes automatizados de correos diario/semanal/mensual
- Sitios más visitados y clasificación de usuarios por categoría web
- Reporte de tráfico por hora por usuario
- Palabras clave de búsqueda en Google
- Informe de filtrado web de Kerio Control
- Registro externo para syslog
- Monitoreo SNMP (El Protocolo Simple de Administración de Red)
- Gráficas de tráfico
- Tablero de administración
- Clasificación de tráfico (multimedia, mensajería, transferencia de archivos grandes)
- Monitoreo de actividades del anfitrión en tiempo real

Desventajas:

- Se necesita del pago de una licencia para su utilización por ser un programa de carácter privativo.
- Si la compañía del fabricante del programa desaparece, la posibilidad de tener versiones mejoradas y corregir errores, es nula.

2.3.2 Ventajas del Squid

- Proporciona un servicio de Proxy que soporta peticiones HTTP, HTTPS y FTP a equipos que necesitan acceder a Internet y a su vez provee la funcionalidad de caché especializado en el cual almacena de forma local las páginas consultadas recientemente por los usuarios. De esta forma, incrementa la rapidez de acceso a los servidores de información Web y FTP que se encuentra fuera de la red interna.
- También es compatible con SSL con lo que también acelera las transacciones cifradas, y es capaz de ser configurado con amplios controles de acceso sobre las peticiones de usuarios.

- Puede formar parte de una jerarquía de caches. Diversos proxys trabajan conjuntamente sirviendo las peticiones de las páginas. Un navegador solicita siempre las páginas a un sólo proxy, si este no tiene la página en la caché hace peticiones a sus hermanos, que si tampoco las tienen las hacen a su/s padre/s.
- Sigue los protocolos ICP, protocolo para la consulta (HTCP, *Hyper Text Caching Protocol,*), Protocolo de Selección de Enrutamiento de Caché (CARP, *Cache Array Routing Protocol*) y caché digests que tienen como objetivo permitir a un proxy preguntarle a otros proxys caché si poseen almacenado un recurso determinado.
- Puede ser configurado para ser usado como proxy transparente de manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia. De modo predefinido Squid utiliza el puerto 3128 para atender peticiones, sin embargo, se puede especificar que lo haga en cualquier otro puerto disponible o bien que lo haga en varios puertos disponibles a la vez.
- A partir de la versión 2.3 implementa el Protocolo de Control de Cache Web (WCCP, *Web Cache Control Protocol*). Permite interceptar y redirigir el tráfico que recibe un enrutador hacia uno o más proxys caché, haciendo control de la conectividad de los mismos. Además, permite que uno de los proxys caché designado pueda determinar cómo distribuir el tráfico redirigido a lo largo de todo el arreglo de proxys caché.
- Ofrece la posibilidad de establecer reglas de control de acceso. Esto permite establecer políticas de acceso en forma centralizada, simplificando la administración de una red.
- Cuando un usuario hace petición hacia un objeto en Internet, este es almacenado en el caché, si otro usuario hace petición hacia el mismo objeto, y este no ha sufrido modificación alguna desde que lo accedió el usuario anterior, se muestra el que ya se encuentra en el caché en lugar de volver a descargarlo desde Internet. Esta función permite navegar rápidamente

cuando los objetos ya están en el caché y además optimiza enormemente la utilización del ancho de banda.

- Permite activar el Protocolo Simple de Administración de Red (*SNMP, Simple Network Management Protocol*) este proporciona un método simple de 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.
- Está compuesto también por el programa servidor DNS, que se encarga de la búsqueda de nombres de dominio. Cuando Squid se ejecuta, produce un número configurable de procesos del servidor DNS, 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.
- Tiende a ser muy eficiente (porque muchas personas lo optimizan y mejoran).
- Tiende a ser muy diverso: las personas que contribuyen tienen varias necesidades y esto hace que el programa esté adaptado a una cantidad más grande de problemas.
- Libertad de usar el programa, con cualquier propósito.
- Libertad de acceso al código fuente del programa.
- Libertad de copia y distribución.
- Libertad de modificar y mejorar el programa.
- Modo anónimo: Permite especificar los encabezados HTTP individuales que se deben permitir y que deben bloquearse.

2.3.3 Ventajas del TinyProxy

- Soporte HTTPS: Permite el reenvío de conexiones HTTPS sin modificar el tráfico de ninguna manera.
- Monitoreo remoto: Puede monitorearse remotamente para ver registros y detalles de acceso.
- Supervisión del promedio de carga: Puede configurarse para rechazar conexiones después de que la carga del servidor llegue a cierto punto.

- Control de acceso: Puede ser configurado para permitir solamente conexiones de ciertas subredes o direcciones IP.
- Seguro: Con cierta configuración, se puede ejecutar sin privilegios especiales, minimizando así la posibilidad de que el sistema se comprometa. Además, se diseñó con un ojo hacia la prevención de desbordamientos de búfer.
- Requiere muy poco en los recursos del sistema: Por lo tanto, se puede ejecutar en una máquina de bajas prestaciones ningún impacto en el rendimiento.
- Filtrado basado en *URL*: Permite la lista negra y blanca basada en *URL* y dominio.
- Proxy transparente: Se puede configurar como un proxy transparente, por lo que un proxy se puede utilizar sin necesidad de ninguna configuración del lado del cliente.
- Encadenamiento de proxy: puede utilizar un servidor proxy ascendente para conexiones salientes, en lugar de conexiones directas al servidor de destino, creando una llamada cadena proxy.

2.4 Comparación entre filtros de contenido web

2.4.1 Ventajas y desventajas del Kerio

- Limita el acceso según la dirección URL.
- Deniega el acceso sobre la base de ocurrencia de palabras prohibidas.
- Limita el acceso a ciertos servidores FTP.
- Limita basado en los nombres de archivo.

Desventajas:

- Posee un filtrado web muy pobre porque se necesita insertar manualmente todos sitios prohibidos por lo que dificulta mucho el trabajo cuando existen programas para esta función que evitan esta extensa tarea y mejoran el trabajo.

2.4.2 Ventajas del E2Guardian

- Incorporado en el sistema de complemento del escáner de contenido que incluye escaneado con Antivirus.
- Se puede configurar para tener varias configuraciones de filtro para proporcionar diversos grados de filtrado web a diferentes grupos de usuarios.
- NTLM y soporte de conexión persistente.
- Soporte de autenticación de resumen.
- Soporte de autenticación básica.
- Soporte de autenticación IP.
- Soporte de autenticación de DNS.
- Análisis de cabecera y manipulación - también puede manipular las cookies.
- Soporte para descarga y escaneado de archivos grandes más de 2 GB.
- Dominios y URL de la lista blanca.
- Dominios y url de lista negra.
- Greylist dominios y *urls*.
- Negar expresiones regulares en *urls*, contenido corporal y encabezados.
- Reemplazo de la expresión regular de *URL* para que pueda, por ejemplo, forzar la búsqueda segura en los motores de búsqueda.
- Exploración profunda de *URL*,por ejemplo, bloquear imágenes en imágenes de Google.
- Bloqueo avanzado de anuncios.
- Diversas mejoras en el rendimiento.
- Actualizaciones para manejar todas las tendencias actuales de la tecnología web.
- Bloqueo de SSL para bloquear proxys anónimos
- Limitar el tamaño del POST (subir).

2.4.3 Ventajas del SquidGuard

- Excepciones basadas en URL de referencia.
- Bloqueo basado en tiempo.
- Bloquea todo el acceso a los sitios de la categoría de destino.
- Controles finos: configura usuarios y grupos individuales.
- Redirecciona a las *URL* de su elección.
- Filtrar en *URL* o nombres de dominio.
- Bloquea banners (redirecciona a formato de fotos .png vacío).
- Ofrece la posibilidad de crear reglas acceso por hora del día y fecha.
- Definen reglas de acceso para diferentes grupos de usuarios

2.5 Ventajas de los recopiladores de logs

2.5.1 Sarg

- Herramienta de código abierto
- Permite analizar los archivos de registro del Squid
- Genera hermosos informes en formato HTML con información sobre usuarios, direcciones IP, sitios de acceso máximo, uso total de ancho de banda, tiempo transcurrido, descargas, Informes semanales y mensuales.

2.5.2 FreeSa

- Controla el uso del tráfico de los usuarios.
- Ayuda a controlar las políticas de seguridad del acceso a Internet e investigar los incidentes de seguridad.
- Evalúa la eficiencia del servidor para detectar problemas con la configuración y además es multiplataforma.

2.5.3 LigthSquid

- Instalación rápida y sencilla.
- Analizador de registro rápido.
- Script basado en Perl para páginas de informes generadas dinámicamente.
- No se requiere base de datos.
- Soporta grupos de usuarios.
- Posee una Interfaz multilingüe.

2.6 Ventajas y Desventajas de los protocolos en la autentificación de los proxys web

2.6.1 Desventajas de la Autenticación Básica:

- La mayor vulnerabilidad que presenta este método es que las credenciales son transmitidas en texto claro, solo codificadas en Base64 lo que permite que un atacante pueda decodificarla con facilidad si son capturadas.
- Otra vulnerabilidad consiste en que tampoco posee ningún mecanismo que obligue a realizar la transmisión sobre un canal encriptado.
- Por último y no menos grave, la Autenticación Básica no establece un proceso para desconectar al usuario.

2.6.2 Desventajas Autenticación Digest:

- La autentificación Digest no posee una fuerte autentificación ni ofrece protección de confidencialidad fuera de la protección de la contraseña el resto de la petición y respuesta van en texto plano.

2.6.3 Ventajas de NTLM:

- Acceso a la solicitud del usuario
- Servidor enviar mensaje de desafío
- Clientes envían respuesta de mensajes

- Servidor enviar desafío y respuesta al controlador de dominio
- Controlador de dominio compara cambios y respuestas del usuario autenticado
- El servidor envía una respuesta al cliente

Esta seguridad mejorada proporciona claves separadas para confidencialidad e integridad del mensaje, proporciona una entrada al cliente al desafío para impedir ataques específicos de texto plano, y usa función basada en el algoritmo MD5 y el código de autenticación de mensaje para la comprobación de la integridad del mensaje. Además, utiliza autenticación Windows por lo que se hace necesario introducir la computadora en el dominio a través de los componentes samba, Windbind y Kerberos, el primer objetivo de Kerberos es el de eliminar la transmisión a través de la red de información de autenticación. Un uso correcto de Kerberos erradica la amenaza de analizadores de paquetes que intercepten contraseñas en su red. En conjunto ellos realizan una autenticación de la computadora en Linux con el dominio de Windows. Esto se realiza para que esa computadora sea confiable con el dominio de Windows y exista una buena comunicación.

2.7 Diseño de la propuesta de sistema proxy a implementar

La propuesta que se quiere implementar con los programas adecuados sería una computadora con el Squid instalado que a ella se le integran el E2guardian como filtrado web y el Squish para el control de cuotas. Esta computadora se conecta a otra en La Habana que es la que te brinda el servicio de Internet con Squid instalado. Además, se tiene una computadora adicional con el Sarg instalado para el control de los logs del Squid todo se puede apreciar en la figura 2.

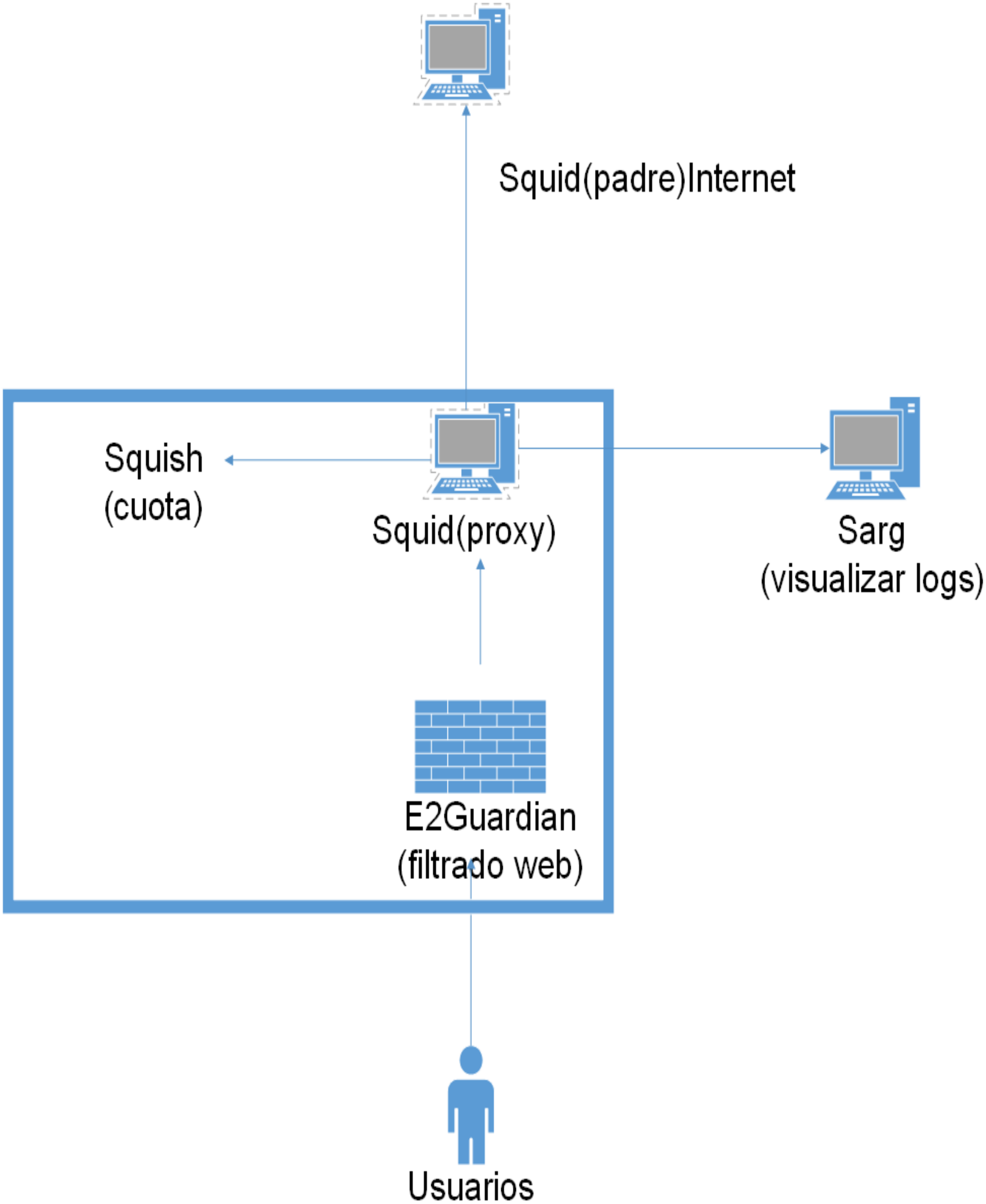


Figura 2: Diseño de la propuesta de sistema proxy a implementar

2.8 Conclusiones parciales.

A través del estudio realizado en el GET de Cienfuegos se llegó a la conclusión de que el proxy web más adecuado a implementar en la empresa es el Squid por sus características que lo amparan como son programa libre, además permite integrarse con otros programas y posee una extensa bibliografía, así como el Squish para el control de cuotas único de su tipo que sea de código abierto ya que en el mundo no se usa el control de cuotas, tema muy importante para el GET. Además, se escogió el Sarg por ser muy potente a la hora de organizar y visualizar los logs, donde además no ofrece una interfaz muy buena y agradable a la vista del usuario. Como método de autentificación se usó el NTLM por tener mayor seguridad que los demás métodos como lo son la básica y la digest,se usará el Kerberos por su seguridad en la autenticación.

Capítulo 3 : Implementación del sistema navegación segura en el GET de Cienfuegos.

3.1 Introducción.

Conociendo los programas más adecuados para la implementación del sistema de proxy de navegación segura, en este capítulo se procederá a implementar los mismos. Se abordará el tema de la instalación de los programas y la puesta en marcha sobre el funcionamiento del sistema, así como los pasos a para su implementación que se hicieron sobre el sistema operativo Centos 7 por su gran seguridad en el aspecto de servidor de redes.

3.2 Configuración del Squid

En los Anexos 7, 8, 9,10, 11, 12 ,13 aparece una guía detallada de cómo se instaló el sistema. En la configuración del Squid se crean las ACL (listas de control de accesos) son variables que se declaran, en este caso se declararon:

acl ntlm_auth proxy_auth REQUIRED

Significa que vas a requerir una autenticación del proxy que puede ser básica, Ntlm o Digest en este caso Ntlm. Luego *http_access allow ntlm_auth* es donde se le dice que solo se autentica con Ntlm. Se declararon las siguientes para diferenciar el horario laboral del no laboral para hacer restricciones dependiendo el horario para evitar lentitud en la red de lunes a viernes en este caso.

acl work time MTWHF 08:00-14:00

acl work time 00:00-06:00

acl mwork time MTWHF 08:00-14:00

Se creó otra ACL para expresiones regulares porque cuando se navega en Internet se puede hacer por un dominio o por una IP y aquí se declaró que nadie puede navegar por IP, esto está dado por la complejidad de bloquear las reglas por IP. Se direrencia de las IP nacionales porque estas si pueden navegar

acl urlIP url_regex ([0-9]{1,3})\.([0-9]{1,3})\.([0-9]{1,3})\.([0-9]{1,3})

acl CubaIPs dst 10.120.0.0/16

Aquí se declara una ACL para que bloquee todo lo que contenga la palabra Facebook y proxy al navegar a pesar de ser una redundancia porque en el

E2guardian también se debe hacer por si una de las dos fallas. En la primera se bloquea el dominio y la otra el camino.

acl forbidens url_regex facebook proxy

acl forbidens-words urlpath_regex facebook proxy

Con esta ACL *acl numbercon maxconn 5* se dice que el máximo de conexiones a un mismo lugar es 5 para evitar que la red colapse.

acl extlimit url_regex -i "/etc/squid/scripts/ext" se declara para evitar que te descarguen extensiones que tu no desees, en la carpeta ext se encuentra una lista de estas extensiones.

reply_body_max_size 30 MB extlimit work

reply_body_max_size 50 MB extlimit! work

Estas dos ACL contribuyen a que en el horario de trabajo la red esté más libre porque en el horario de trabajo solo se puede descargar un fichero que su tamaño como máximo sea 30 MB y fuera del horario de trabajo 50MB.Se deniega todo lo que sea una IP excepto las nacionales: *http_access deny urlIP !CubaIPs localnet* en esta es básicamente lo mismo pero por el puerto HTTPS que muchas veces burla la seguridad *http_access deny CONNECT urlIP !CubaIPs localnet*

Se deniegan estas ACL creadas anteriormente.
http_access deny forbidens localnet mwork
http_access deny forbidens-words localnet mwork
http_access deny CONNECT forbidens localnet mwork
http_access deny CONNECT forbidens-words localnet mwork
http_access deny localnet numbercon
En esta última se deniega denegando número de conexiones de *localnet* que esta es una ACL que se te por defecto y que se le asigna la dirección de la red local.

```
  GNU nano 2.3.1                  File: /etc/squid/squid.conf

#acl ip-wsus src 10.120.2.11/32
#acl ip-wsus src 10.120.2.22/32
#http_access allow ip-wsus

http_port 8888

#cache_peer localhost parent 82 0 proxy-only login=PASS no-query no-delay
cache_peer 192.168.4.65 parent 81 0 default
#cache_peer proxy.tur.cu parent 81 0 default
#cache_peer  10.120.0.10 parent 3128 0 login=getcfg:getcfg05 no-query no-delay
#cache_peer 127.0.0.1 parent 8081 0 proxy-only no-query login=PASS no-digest
#acl QUERY urlpath_regex cgi-bin \?
#no_cache deny QUERY
#auth_param basic program /usr/lib/squid3/ncsa_auth /etc/squid3/reglas/passwd
#auth_param basic program /usr/lib/squid3/squid_ldap_auth -R -b "dc=get,dc=cfg" -D "cn=getadm,cn=Users,dc=get,dc=cfg" -w "2013roam.*about" -f$
auth_param basic program /usr/lib64/squid/basic_ldap_auth -R -b "dc=get,dc=cfg" -D ldap@get.cfg -W /etc/squid/pass/ldappass -f sAMAccountName$
auth_param basic children 10
auth_param basic realm UEB GET Cfgos
auth_param basic credentialsttl 2 hours
#maximun_object_size 5048 KB
visible_hostname Proxy.Get.Cfgos

#logformat squid %tg %6tr %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
#logformat squid %tg.%03tu %6tr %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
cache_dir aufs /var/spool/squid 512 16 256
cache_access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
cache_store_log /var/log/squid/store.log
cache_mem 64 MB
cache_mgr juanma@get.cfg.tur.cu
error_directory /usr/share/squid/errors/es-es
access_log syslog:local6.info squid
dns_v4_first on

dns_nameservers 192.168.1.11
logfile_rotate 3
                              [ Read 210 lines ]
^G Get Help    ^O WriteOut    ^R Read File   ^Y Prev Page   ^K Cut Text    ^C Cur Pos
^X Exit        ^J Justify     ^W Where Is    ^V Next Page   ^U UnCut Text  ^T To Spell
```

Figura 3: Fichero de configuración squid.conf

3.3 Configuración del E2guardian

Se agregan los usuarios y a que filtro pertenecen, los que no aparecen son los que están en el filtro 1 que es el de los denegados, wsus que pertenece al filtro de los servidores, este último se utiliza para otros permisos adicionales como descargar actualizaciones de antivirus entre otros privilegios que no tienen los usuarios. Ver en la figura 4

```
  GNU nano 2.3.1                    File: /etc/e2guardian/lists/filtergroupslist

#No edite este fichero se modifica automaticamente del AD
#
#Mon Feb 20 10:01:04 CST 2017
#
juanma=filter2
diana=filter2
maribel=filter2
dorian=filter2
ejose=filter2
yeny=filter2
juana=filter2
dayami=filter2
greneter=filter2
martica=filter2
rpadilla=filter2
betsy=filter2
wsus=filter3
```

Figura 4: Fichero de configuración de filtros por usuario.

Se configuran tres ficheros para los distintos filtros de grupo e2guardianf1.conf para los denegados,e2guardianf2.conf para los usuarios y e2guardianf3.conf que es para servidores, cada filtro posee un fichero diferente, en la figura 5 se puede apreciar la configuración del filtro del grupo de los usuarios, ficheros a los que el apunta, ejemplo de esto *exceptioniplist* va a apuntar al fichero '/etc/e2guardian/lists/usuarios/exceptioniplist' este fichero tiene una lista de ip que él no va a filtrar o sea que van a ser excepciones sobre esa lista, bannedphraselist apunta al fichero '/etc/e2guardian/lists/usuarios/ bannedphraselist' va a contener las frases que están bloqueadas, en el fichero '/etc/e2guardian/lists/usuarios/weightedphraselist 'se encuentran las frases ponderadas que esto significa que cualquier frase que se encuentre en esa lista las va a prohibir por encima de todo. En el fichero '/etc/e2guardian/lists/usuarios/ exceptionphraselist 'se agrega una lista de frases que no se van a filtrar o sea que son permitidas, '/etc/e2guardian/lists/usuarios/bannedsitelist 'va a contener una lista de sitios prohibidos. Este fichero '/etc/e2guardian/lists/usuarios/greysitelist 'contiene una lista de sitios que son bloqueados, pero se permite parte de ellos. El fichero '/etc/e2guardian/lists/usuarios/bannedsslsitelist va a contener una lista de sitios https (Protocolo seguro de transferencia de hipertexto) prohibidos, '/etc/e2guardian/lists/usuarios/greysslsitelist' lista de sitios https bloqueados pero que permite parte de ellos. En el fichero '/etc/e2guardian/lists/usuarios/exceptionsitelist 'se encuentra una serie de sitios permitidos, '/etc/e2guardian/lists/usuarios/bannedurllist 'va a contener una lista de url *Uniform Resource Locator* **(**Localizador Uniforme de Recursos**)** bloqueadas, '/etc/e2guardian/lists/usuarios/greyurllist 'contiene una lista de url bloqueadas, pero que permite parte de ellas. El fichero '/etc/e2guardian/lists/usuarios/exceptionsurllist 'contiene una lista de url que se van a permitir. '/etc/e2guardian/lists/usuarios/exceptionregexurllist 'tiene una lista de expresiones regulares que se van a permitir, '/etc/e2guardian/lists/usuarios/bannedregexurllist 'posee una lista de expresiones regulares a bloquear.

En el fichero /etc/e2guardian/e2guardianf2.conf se definió que el nombre de grupo es los usuarios va a pertenecer al modo de grupo 1 que son los que se filtran porque también existen el 0 donde va a denegar todo usuario que no se encuentre en la red y el 2 los que no se van a filtrar. Ver Anexo 6

```
  GNU nano 2.3.1                    File: /etc/e2guardian/e2guardianf2.conf

# ssllegacylogic = off

# Content filtering files location
#exceptioniplist = '/etc/e2guardian/lists/usuarios/exceptioniplist'
bannedphraselist = '/etc/e2guardian/lists/usuarios/bannedphraselist'
weightedphraselist = '/etc/e2guardian/lists/usuarios/weightedphraselist'
exceptionphraselist = '/etc/e2guardian/lists/usuarios/exceptionphraselist'
bannedsitelist = '/etc/e2guardian/lists/usuarios/bannedsitelist'
greysitelist = '/etc/e2guardian/lists/usuarios/greysitelist'
bannedsslsitelist = '/etc/e2guardian/lists/usuarios/bannedsslsitelist'
greysslsitelist = '/etc/e2guardian/lists/usuarios/greysslsitelist'
exceptionsitelist = '/etc/e2guardian/lists/usuarios/exceptionsitelist'
bannedurllist = '/etc/e2guardian/lists/usuarios/bannedurllist'
greyurllist = '/etc/e2guardian/lists/usuarios/greyurllist'
exceptionurllist = '/etc/e2guardian/lists/usuarios/exceptionurllist'
exceptionregexpurllist = '/etc/e2guardian/lists/usuarios/exceptionregexpurllist'
bannedregexpurllist = '/etc/e2guardian/lists/usuarios/bannedregexpurllist'
picsfile = '/etc/e2guardian/lists/usuarios/pics'
contentregexplist = '/etc/e2guardian/lists/usuarios/contentregexplist'
urlregexplist = '/etc/e2guardian/lists/usuarios/urlregexplist'
refererexceptionsitelist = '/etc/e2guardian/lists/usuarios/refererexceptionsitelist'
refererexceptionurllist = '/etc/e2guardian/lists/usuarios/refererexceptionurllist'
embededreferersitelist = '/etc/e2guardian/lists/usuarios/embededreferersitelist'
embededrefererurllist = '/etc/e2guardian/lists/usuarios/embededrefererurllist'
urlredirectregexplist = '/etc/e2guardian/lists/usuarios/urlredirectregexplist'

# local versions of lists (where LOCAL_LISTS enabled)
# enablelocallists = on/off
#localbannedsitelist = '/etc/e2guardian/lists/usuarios/localbannedsitelist'
#localgreysitelist = '/etc/e2guardian/lists/usuarios/localgreysitelist'
#localexceptionsitelist = '/etc/e2guardian/lists/usuarios/localexceptionsitelist'
#localbannedurllist = '/etc/e2guardian/lists/usuarios/localbannedurllist'
#localgreyurllist = '/etc/e2guardian/lists/usuarios/localgreyurllist'
#localexceptionurllist = '/etc/e2guardian/lists/usuarios/localexceptionurllist'
#localbannedsslsitelist = '/etc/e2guardian/lists/usuarios/localbannedsslsitelist'
#localgreysslsitelist = '/etc/e2guardian/lists/usuarios/localgreysslsitelist'

^G Get Help      ^O WriteOut      ^R Read File     ^Y Prev Page     ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify       ^W Where Is      ^V Next Page     ^U UnCut Text    ^T To Spell
```

Figura 5: Fichero de configuración del filtro de usuarios

En el fichero de configuración /etc/e2guardian/list/usuarios/bannedsitelist cada fichero apunta a una carpeta que se encuentra en blacklist(listas negras) donde se encuentran todos los dominios en lista negra o sea bloqueados. Se encuentran organizados por chat, ropa, teléfonos, culinaria, ropa, droga, gobierno, juegos etc. Esto permite bloquear todos esos dominios prohibidos a los usuarios. Se puede agregar cualquier dominio que se quiera bloquear.

```
  GNU nano 2.3.1                    File: /etc/e2guardian/lists/usuarios/bannedsitelist

#.Include</etc/e2guardian/lists/blacklists/beerliquorinfo/domains>
#.Include</etc/e2guardian/lists/blacklists/beerliquorsale/domains>
#.Include</etc/e2guardian/lists/blacklists/chat/domains>
#.Include</etc/e2guardian/lists/blacklists/childcare/domains>
#.Include</etc/e2guardian/lists/blacklists/clothing/domains>
#.Include</etc/e2guardian/lists/blacklists/culinary/domains>
#.Include</etc/e2guardian/lists/blacklists/dialers/domains>
#.Include</etc/e2guardian/lists/blacklists/drugs/domains>
#.Include</etc/e2guardian/lists/blacklists/entertainment/domains>
#.Include</etc/e2guardian/lists/blacklists/forums/domains>
#.Include</etc/e2guardian/lists/blacklists/frencheducation/domains>
.Include</etc/e2guardian/lists/blacklists/games/domains>
.Include</etc/e2guardian/lists/blacklists/gambling/domains>
#.Include</etc/e2guardian/lists/blacklists/government/domains>
.Include</etc/e2guardian/lists/blacklists/hacking/domains>
#.Include</etc/e2guardian/lists/blacklists/homerepair/domains>
#.Include</etc/e2guardian/lists/blacklists/hygiene/domains>
#.Include</etc/e2guardian/lists/blacklists/jewelry/domains>
#.Include</etc/e2guardian/lists/blacklists/jobsearch/domains>
#.Include</etc/e2guardian/lists/blacklists/kidstimewasting/domains>
.Include</etc/e2guardian/lists/blacklists/mail/domains>
.Include</etc/e2guardian/lists/blacklists/malware/domains>
.Include</etc/e2guardian/lists/blacklists/mixed_adult/domains>
#.Include</etc/e2guardian/lists/blacklists/news/domains>
#.Include</etc/e2guardian/lists/blacklists/onlineauctions/domains>
.Include</etc/e2guardian/lists/blacklists/onlinegames/domains>
#.Include</etc/e2guardian/lists/blacklists/onlinepayment/domains>
#.Include</etc/e2guardian/lists/blacklists/personalfinance/domains>
#.Include</etc/e2guardian/lists/blacklists/pets/domains>
.Include</etc/e2guardian/lists/blacklists/phishing/domains>
.Include</etc/e2guardian/lists/blacklists/porn/domains>
```

Figura 6: Fichero de sitios denegados

3.4 Configuración del Sarg

Se configura el fichero usr/local/etc/sarg.conf, se utilizó el comando acces_log, el mismo permite darle una dirección de archivo al Sarg de donde se encuentran los logs del squid y con este otro comando output_dir se los envía a la carpeta donde el sarg almacena los logs.

Se utilizó el comando rsync, se utiliza para sincronizar archivos, pero en este caso los logs del Squid con los del Sarg, se puso en una sentencia crontab que es un ejecutador automático donde se copian los logs diarios del Squid al Sarg o sea todos los días de la semana..

*00 0 * * * root rsync /var/log/squid/access.log root@10.120.2.5:/home/admin/*

Donde el primer número minutos, horas, día del mes y día de la semana.

En el Anexo 1 se observa como el Sarg muestra una información detallada de cada usuario, el tiempo que estuvieron conectados, el tamaño total de las descargas que realizaron, el por ciento de bytes descargados con respecto al total, el tiempo que estuvo conectado, el por ciento en caché, esto ofrece una medida de cuan cargada estuvo la red porque al ser mayor el por ciento menos tráfico, porque busca la página en caché y no en Internet. Te brinda un total general de todo y un promedio.

En el Anexo 3 se muestran los sitios más visitados (*top site*) en él los intentos de conexión que se hicieron, los bytes descargados del sitio, la cantidad de usuarios que accedieron, en la parte superior existen vínculos que muestran una relación de sitios con usuarios, las descargas que se hicieron, los accesos que se denegaron y las autenticaciones que fallaron.

También se puede observar la información de los sitios que accedió cada usuario, los intentos de conexiones que estableció por sitio, cantidad de megas que descargó, porciento respecto a los restantes usuarios, el tiempo que estuvo en ese sitio. Ver Anexo 4. Se observa también un reporte de la cuota que ha usado por días cada usuario en un período de tiempo Anexo 5.

3.5 Configuración del Squish

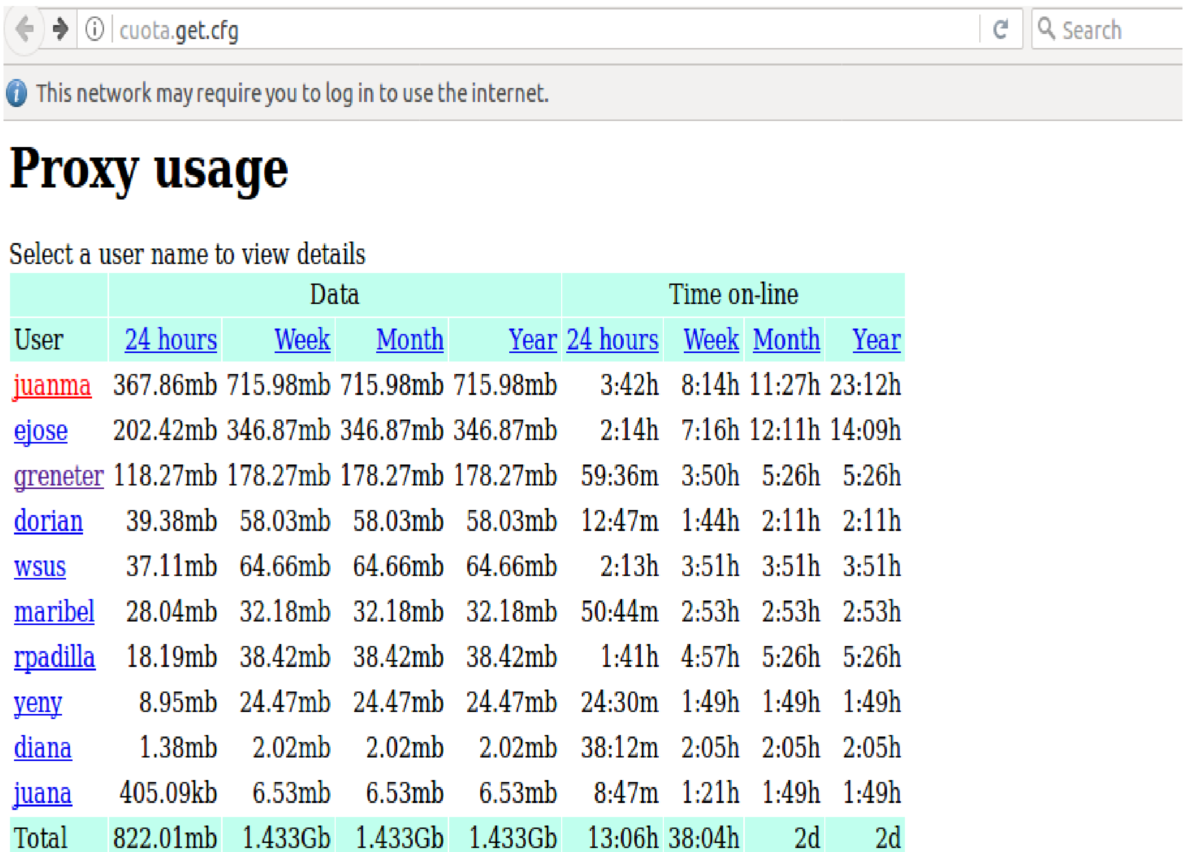
En el archivo de configuración /etc/squid/squish.conf se puede observar en la figura 7 la cuota designada para cada usuario que fue por semana, pero puede ser por días, semanas o meses, en este caso fue de 10Gb semanales ya que al ser pocos usuarios no afecta la red, de haber más servicios se puede poner una cuota menor. Aunque la cuota sea alta no se debe poner indefinida porque se necesita de un control sobre la cuota. En el caso del wsus se le triplica la cuota porque él va a descargar las actualizaciones del antivirus Kaspersky y las actualizaciones del wsus. Además, los usuarios que excedan la cuota los coloca en un fichero que se llama squished y a través de una ACL que se le pone al Squid es que el bloquea los usuarios que van apareciendo en ese fichero.

```
  GNU nano 2.3.1                            File: /etc/squid/squish.conf

# This file contains data formatted as follows:
#
# Blank lines and hashed stuff is for comments
# user  amount/period
#       bandwidth: 999[kmG]b  / period: day, week, month
#       time: 999[smh]        / period: day, week, month
#
# Whitelist entries - they can have as much as they like
#192\.168\.99\.44              25h/day
#192\.168\.97\.43              25h/day
# Poor guy:
#andrewm                2h/day  4Mb/day    10Mb/week
# Catchall -- people and IP's not matched by the above rules
#.*              4h/day  20Mb/day   20h/week     100Mb/week

juanma     200Mb/week
greneter   10Gb/week
maribel    10Gb/week
ejose      10Gb/week
rpadilla   10Gb/week
yeny       10Gb/week
martica    10Gb/week
dayami     10Gb/week
juana      10Gb/week
diana      10Gb/week
betsy      10Gb/week
dorian     10Gb/week
wsus       30Gb/week
```

Figura 7: Configuración del fichero para la asignación de la cuota para cada usuario

Se agregó una ACL diciendo cual es el dominio donde el Squish en este caso es proxy-jm.get.cfg y en el fichero /etc/squid/squished se van a encontrar los usuarios que han sido bloqueados, luego deniega y se le asigna la página del squished para cuando bloquee usuarios. Ver anexo 12

En la figura 8 se puede observar la página cuota.get.cfg en ella se muestra como los usuarios que han excedido la cuota se marcan en rojo, en este caso fue el usuario Juanma, además un registro de los usuarios en un día, una semana, un mes y además el tiempo en conexión respectivamente. En el anexo 1 se puede ver una foto detallada de los horarios y el ancho de banda que estuvo bajando el usuario Juanma que está subrayado.



Proxy usage

Select a user name to view details

	Data				Time on-line			
User	24 hours	Week	Month	Year	24 hours	Week	Month	Year
juanma	367.86mb	715.98mb	715.98mb	715.98mb	3:42h	8:14h	11:27h	23:12h
ejose	202.42mb	346.87mb	346.87mb	346.87mb	2:14h	7:16h	12:11h	14:09h
greneter	118.27mb	178.27mb	178.27mb	178.27mb	59:36m	3:50h	5:26h	5:26h
dorian	39.38mb	58.03mb	58.03mb	58.03mb	12:47m	1:44h	2:11h	2:11h
wsus	37.11mb	64.66mb	64.66mb	64.66mb	2:13h	3:51h	3:51h	3:51h
maribel	28.04mb	32.18mb	32.18mb	32.18mb	50:44m	2:53h	2:53h	2:53h
rpadilla	18.19mb	38.42mb	38.42mb	38.42mb	1:41h	4:57h	5:26h	5:26h
yeny	8.95mb	24.47mb	24.47mb	24.47mb	24:30m	1:49h	1:49h	1:49h
diana	1.38mb	2.02mb	2.02mb	2.02mb	38:12m	2:05h	2:05h	2:05h
juana	405.09kb	6.53mb	6.53mb	6.53mb	8:47m	1:21h	1:49h	1:49h
Total	822.01mb	1.433Gb	1.433Gb	1.433Gb	13:06h	38:04h	2d	2d

Figura 8: Registro de la cuota de los usuarios

3.6 Conclusiones parciales

Se implementó el sistema de navegación segura a raíz del estudio realizado anteriormente con óptimos resultados. Dando como fruto un sistema auxiliado de programas específicos para el control de la red de datos del GET de Cienfuegos.

Conclusiones Generales.

Se identificaron programas y protocolos existentes para un sistema proxy de navegación segura en el GET de Cienfuegos. A partir de una comparación de programas se seleccionaron los que más se adecuaban al GET siendo en este sentido el Squid como servidor proxy, el E2guardian como filtro web, el Squish para el control de cuota, el método de autenticación NTLM. Se caracterizó la red de datos del GET de Cienfuegos sonde se utiliza *Fast Ethernet* o *Ethernet* de alta velocidad. Se diseñó la implementación con los programas adecuados y se implementó adecuadamente, así como pruebas de funcionamiento que amparan una validación óptima.

Referencias Bibliográficas

[1]. «:: Seguridad Informática ::.» [En línea]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/ServAutenticacion.php. [Accedido: 23-may-2017].

[2] «Instalación de un Servidor Proxy». [En línea]. Disponible en: http://html.rincondelvago.com/instalacion-de-un-servidor-proxy.html. [Accedido: 27-feb-2017].

[3] «TESINA: IMPORTANCIA DEL PROXY PARA LA REDES INTERNAS DE UNA EMPRESA - Blog de ESTADISTICAS». [En línea]. Disponible en: http://estadisticas.blogspot.es/1400087429/tesina-importancia-del-proxy-para-la-redes-internas-de-una-empresa/. [Accedido: 28-feb-2017].

[4] «Qué es un proxy». [En línea]. Disponible en: http://es.ccm.net/faq/2755-que-es-un-proxy. [Accedido: 23-may-2017].

[5] «Squid: servidor proxy-caché | Observatorio Tecnológico». [En línea]. Disponible en: http://recursostic.educacion.es/observatorio/web/es/software/servidores/589-elvira-mifsud. [Accedido: 28-feb-2017].

[6] «Calamar Proxy Alternativa». [En línea]. Disponible en: http://letras-diferentes.info/computadoras/calamar-proxy-alternativa.php. [Accedido: 15-mar-2017].

[7] «A filtering HTTP proxy — WebCleaner». [En línea]. Disponible en: http://webcleaner.sourceforge.net/. [Accedido: 28-mar-2017].

[8] «Aspectos Básicos de la Seguridad en Aplicaciones Web | Documentos - CSI -». [En línea]. Disponible en: http://www.seguridad.unam.mx/documento/?id=17. [Accedido: 28-feb-2017].

[9] «DansGuardian - EcuRed». [En línea]. Disponible en: https://www.ecured.cu/DansGuardian. [Accedido: 28-feb-2017].

[10] «e2guardian-3.4.0.3-1.mga6.x86_64 RPM». [En línea]. Disponible en: http://rpmfind.net/linux/RPM/mageia/cauldron/x86_64/media/core/release/e2guardian-3.4.0.3-1.mga6.x86_64.html. [Accedido: 28-feb-2017].

[11] «Controla el uso de Internet en tu red con NxFilter - NeoTeo». [En línea]. Disponible en: http://www.neoteo.com/controla-el-uso-de-internet-en-tu-red-con-nxfilter/. [Accedido: 27-mar-2017].

[12] «SARG - Squid Analysis Report Generator (Internet software tool) | AcronymFinder». [En línea]. Disponible en: http://www.acronymfinder.com/Squid-Analysis-Report-Generator-(Internet-software-tool)-(SARG).html. [Accedido: 02-mar-2017].

[13] «LightSquid Home Site : Home». [En línea]. Disponible en: http://lightsquid.sourceforge.net/. [Accedido: 23-may-2017].

[14] «Kerberos». [En línea]. Disponible en: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-kerberos.html. [Accedido: 06-mar-2017].

[15] «The NTLM Authentication Protocol and Security Support Provider». [En línea]. Disponible en: http://davenport.sourceforge.net/ntlm.html. [Accedido: 11-mar-2017].

[16] «Digest - EcuRed». [En línea]. Disponible en: https://www.ecured.cu/Digest. [Accedido: 07-mar-2017].

[17] «LDAP - EcuRed». [En línea]. Disponible en: https://www.ecured.cu/LDAP. [Accedido: 09-mar-2017].

Bibliografía

[1] «.:: Seguridad Informática ::.» [En línea]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/ServAutenticacion.php. [Accedido: 23-may-2017].

[2] «Alternativas gratuitas y libres a los programas - LinuxParty», 15-mar-2017. [En línea]. Disponible en: http://www.linux-party.com/index.php/60-software/9419-alternativas-gratuitas-y-libres-a-los-programas. [Accedido: 15-mar-2017].

[3] «Análisis y estadísticas de SQUID con SquidAnalyzer en Debian – Leninmhs», 15-mar-2017. [En línea]. Disponible en: https://leninmhs.wordpress.com/2015/03/28/squidanalyzer-debian-squid-stats/. [Accedido: 15-mar-2017].

[4] «Antivirus para proxy Squid basado el motor antivirus ClamAV. – Software Libre Juventud», 27-feb-2017. [En línea]. Disponible en: https://softwarelibrejuventud.wordpress.com/2016/08/21/antivirus-para-proxy-squid-basado-el-motor-antivirus-clamav/#more-3636. [Accedido: 27-feb-2017].

[5] «Aspectos Básicos de la Seguridad en Aplicaciones Web | Documentos - CSI -», 28-feb-2017. [En línea]. Disponible en: http://www.seguridad.unam.mx/documento/?id=17. [Accedido: 28-feb-2017].

[6] «Calamar Proxy Alternativa», 15-mar-2017. [En línea]. Disponible en: http://letras-diferentes.info/computadoras/calamar-proxy-alternativa.php. [Accedido: 15-mar-2017].

[7] «Comparing Windows Kerberos and NTLM Authentication Protocols | Security content from Windows IT Pro», 06-mar-2017. [En línea]. Disponible en: http://windowsitpro.com/security/comparing-windows-kerberos-and-ntlm-authentication-protocols. [Accedido: 06-mar-2017].

[8] «Configuración de Squid: Opciones básicas. - Alcance Libre», 24-feb-2017. [En línea]. Disponible en: http://www.alcancelibre.org/staticpages/index.php/19-0-como-squid-general. [Accedido: 24-feb-2017].

[9] «Configuración de Squid: Opciones básicas. - Alcance Libre», 24-feb-2017. [En línea]. Disponible en: http://www.alcancelibre.org/staticpages/index.php/19-0-

como-squid-general. [Accedido: 24-feb-2017].

[10] «¿Cuál es la importancia de un Servidor Proxy», 28-feb-2017. [En línea]. Disponible en: http://www.ordenador.online/Redes/Redes-Internet/%C2%BFCu%C3%A1l-es-la-importancia-de-un-Servidor-Proxy-.html. [Accedido: 28-feb-2017].

[11] «DansGuardian --> Alternativas e Apps similares», 15-mar-2017. [En línea]. Disponible en: http://alternativapara.com.br/dansguardian. [Accedido: 15-mar-2017].

[12] «Dansguardian - EcuRed», 28-feb-2017. [En línea]. Disponible en: https://www.ecured.cu/DansGuardian. [Accedido: 28-feb-2017].

[13] «Digest - EcuRed», 07-mar-2017. [En línea]. Disponible en: https://www.ecured.cu/Digest. [Accedido: 07-mar-2017].

[14] «e2guardian-3.4.0.3-1.mga6.x86_64 RPM», 28-feb-2017. [En línea]. Disponible en: http://rpmfind.net/linux/RPM/mageia/cauldron/x86_64/media/core/release/e2guardian-3.4.0.3-1.mga6.x86_64.html. [Accedido: 28-feb-2017].

[15] «Filter Content on Your Home Network with E2guardian | Linux.com | The source for Linux information», 28-feb-2017. [En línea]. Disponible en: https://www.linux.com/learn/filter-content-your-home-network-e2guardian. [Accedido: 28-feb-2017].

[16] «Free Proxy Finder Software - Descarga (gratuita) de la versión para Windows», 27-feb-2017. [En línea]. Disponible en: http://es.freedownloadmanager.org/Windows-PC/Free-Proxy-Finder-Software-GRATIS.html. [Accedido: 27-feb-2017].

[17] «Free-SA statistic analyzer tool | Linux Server Admin and Benchmark Tools | Opensource Software Directory». [En línea]. Disponible en: http://www.gnutoolbox.com/freesa-statistic-analyzer-tool/. [Accedido: 23-may-2017].

[18] «Generando Reportes de Acceso al Proxy Squid con SARG – Nettix Perú», 02-mar-2017. [En línea]. Disponible en: http://www.nettix.com.pe/documentacion/administracion/generando-reportes-

de-acceso-al-proxy-squid-con-sarg. [Accedido: 02-mar-2017].

[19] Center for History and New Media, «Guía rápida». [En línea]. Disponible en: http://zotero.org/support/quick_start_guide.

[20] «Historia del servidor proxy | Informática y Telecomunicaciones | Xuletas, chuletas para exámenes, apuntes y trabajos», 27-feb-2017. [En línea]. Disponible en: https://www.xuletas.es/ficha/historia-servidor-proxy/. [Accedido: 27-feb-2017].

[21] «Instalación de un Servidor Proxy», 27-feb-2017. [En línea]. Disponible en: http://html.rincondelvago.com/instalacion-de-un-servidor-proxy.html. [Accedido: 27-feb-2017].

[22] «Instalación y Configuración de un Servidor Proxy en Linux Ubuntu», 24-feb-2017. [En línea]. Disponible en: https://es.slideshare.net/marceloaalcivar/instalacin-y-configuracin-de-un-servidor-proxy-en-linux-ubuntu. [Accedido: 24-feb-2017].

[23] «Instalar un servidor proxy HTTP (Squid)», 24-feb-2017. [En línea]. Disponible en: http://es.ccm.net/faq/613-instalar-un-servidor-proxy-http-squid. [Accedido: 24-feb-2017].

[24] «Kerberos», 06-mar-2017. [En línea]. Disponible en: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-kerberos.html. [Accedido: 06-mar-2017].

[25] «LDAP - EcuRed», 09-mar-2017. [En línea]. Disponible en: https://www.ecured.cu/LDAP. [Accedido: 09-mar-2017].

[26] «LightSquid Home Site : Home». [En línea]. Disponible en: http://lightsquid.sourceforge.net/. [Accedido: 23-may-2017].

[27] «Migración a software libre: romper paradigmas virtuales - Cuba en Noticias», 27-feb-2017. [En línea]. Disponible en: http://www.cubahora.cu/ciencia-y-tecnologia/migracion-a-software-libre-romper-paradigmas-virtuales. [Accedido: 27-feb-2017].

[28] «Navegación web - EcuRed», 16-feb-2017. [En línea]. Disponible en: https://www.ecured.cu/Navegaci%C3%B3n_web. [Accedido: 16-feb-2017].

[29] «Proxy Caches», 02-mar-2017. [En línea]. Disponible en: http://www.web-caching.com/proxy-caches.html. [Accedido: 02-mar-2017].

[30] «Proxy en linux | Guía completa para desarrollar un servidor proxy», 24-feb-2017. [En línea]. Disponible en: https://proxyenlinux.wordpress.com/. [Accedido: 24-feb-2017].

[31] «Proxy squid | Redes Linux», 24-feb-2017. [En línea]. Disponible en: http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/proxy_squid.html. [Accedido: 24-feb-2017].

[32] «Qué es un proxy», 16-feb-2017. [En línea]. Disponible en: http://es.ccm.net/faq/2755-que-es-un-proxy. [Accedido: 16-feb-2017].

[33] «Qué es un proxy». [En línea]. Disponible en: http://es.ccm.net/faq/2755-que-es-un-proxy. [Accedido: 23-may-2017].

[34] «¿Qué es un Proxy? | Características y Ventajas de un Proxy». [En línea]. Disponible en: https://okhosting.com/blog/que-es-un-proxy/. [Accedido: 23-may-2017].

[35] «SARG - Squid Analysis Report Generator and Internet Bandwidth Monitoring Tool», 09-mar-2017. [En línea]. Disponible en: http://www.tecmint.com/sarg-squid-analysis-report-generator-and-internet-bandwidth-monitoring-tool/. [Accedido: 09-mar-2017].

[36] «SARG - Squid Analysis Report Generator (Internet software tool) | AcronymFinder», 02-mar-2017. [En línea]. Disponible en: http://www.acronymfinder.com/Squid-Analysis-Report-Generator-(Internet-software-tool)-(SARG).html. [Accedido: 02-mar-2017].

[37] «SARG - Squid Analysis Report Generator [wiki.ipfire.org]», 09-mar-2017. [En línea]. Disponible en: http://wiki.ipfire.org/en/addons/sarg/start. [Accedido: 09-mar-2017].

[38] «Servicio proxy-caché», 24-feb-2017. [En línea]. Disponible en: http://portal.uned.es/portal/page?_pageid=93,36656481&_dad=portal&_schema=PORTAL. [Accedido: 24-feb-2017].

[39] «Servidores Proxy cache – Optimizando la red - Security Art Work», 24-feb-2017. [En línea]. Disponible en: https://www.securityartwork.es/2010/03/03/servidores-proxy-cache-%E2%80%93-optimizando-la-red/. [Accedido: 24-feb-2017].

[40] «Servidor proxy de navegación - YMANT», 16-feb-2017. [En línea]. Disponible en: http://www.ymant.com/proxy-de-navegacion/. [Accedido: 16-feb-2017].

[41] «Servidor Proxy: Squid proxy.», 27-feb-2017. [En línea]. Disponible en: http://recursos.cepindalo.es/mod/book/view.php?id=596&chapterid=222. [Accedido: 27-feb-2017].

[42] «Squid+DansGuardian (DG)+Squish | Linux and kitchen», 02-mar-2017. [En línea]. Disponible en: http://en.linuxkitchen.com/2013/12/31/squiddansguardian-dgsquish/. [Accedido: 02-mar-2017].

[43] «Squid: servidor proxy-caché | Observatorio Tecnológico», 28-feb-2017. [En línea]. Disponible en: http://recursostic.educacion.es/observatorio/web/es/software/servidores/589-elvira-mifsud. [Accedido: 28-feb-2017].

[44] «Squid: servidor proxy-caché | Observatorio Tecnológico», 28-feb-2017. [En línea]. Disponible en: http://recursostic.educacion.es/observatorio/web/es/software/servidores/589-elvira-mifsud. [Accedido: 28-feb-2017].

[45] «squish bandwidth quotas for squid cache», 02-mar-2017. [En línea]. Disponible en: http://www.mcgill.org.za/software/squish/. [Accedido: 02-mar-2017].

[46] «Tecnologías de la información y la comunicación: Conectividad (redes locales, red. Internet)», 27-feb-2017. [En línea]. Disponible en: http://tics-perez2.blogspot.com/2008/10/conectividad-redes-locales-red-internet.html. [Accedido: 27-feb-2017].

[47] «TESINA: IMPORTANCIA DEL PROXY PARA LA REDES INTERNAS DE UNA EMPRESA - Blog de ESTADISTICAS», 28-feb-2017. [En línea]. Disponible en: http://estadisticas.blogspot.es/1400087429/tesina-importancia-del-proxy-para-la-redes-internas-de-una-empresa/. [Accedido: 28-feb-2017].

[48] «The NTLM Authentication Protocol and Security Support Provider», 06-mar-2017. [En línea]. Disponible en: http://davenport.sourceforge.net/ntlm.html. [Accedido: 06-mar-2017].

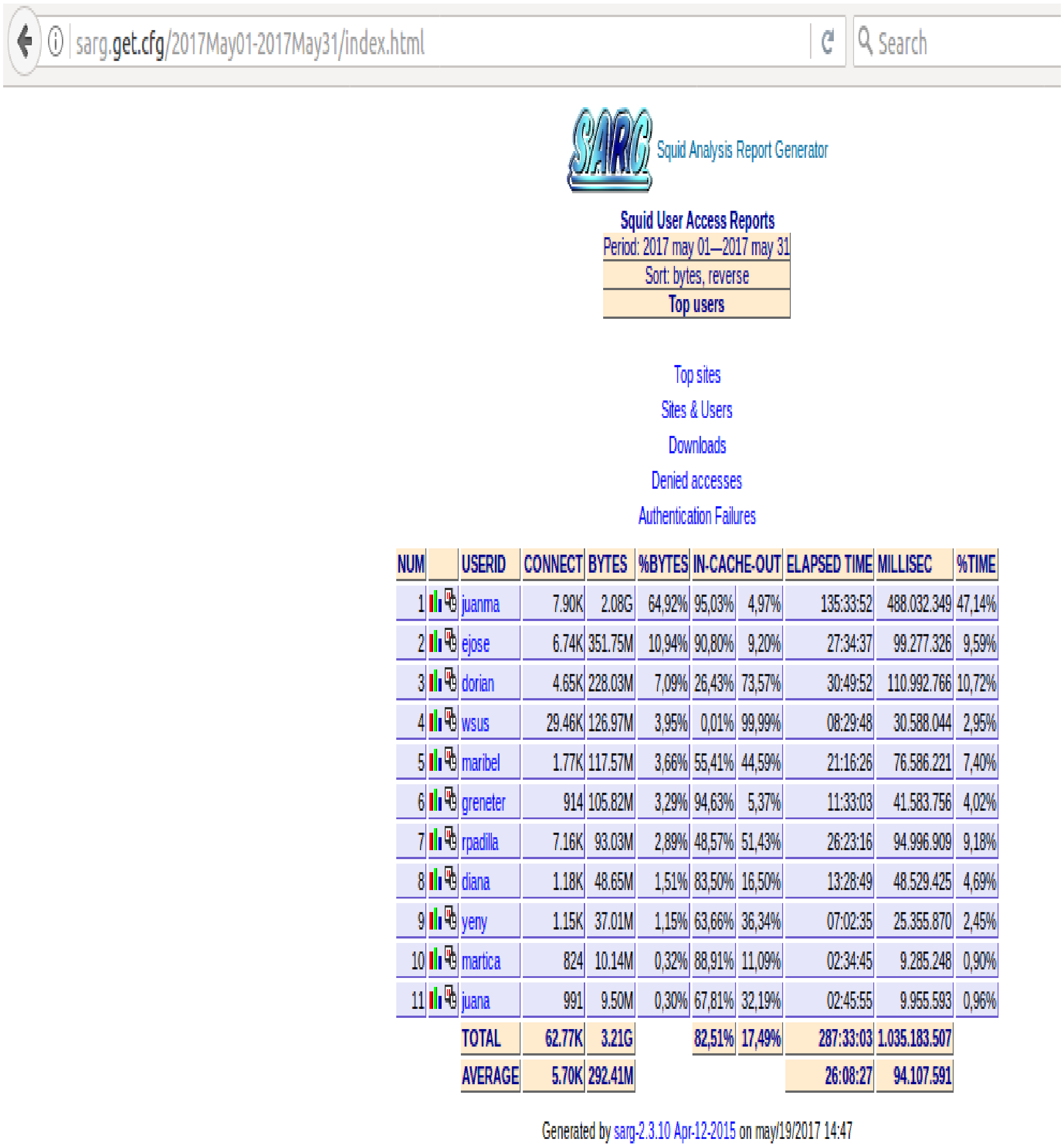
[49] «What is NTLM? Webopedia Definition», 06-mar-2017. [En línea]. Disponible en: http://www.webopedia.com/TERM/N/NTLM.html. [Accedido: 06-mar-2017].

Glosario de términos

- TCP/IP: Son las siglas de Protocolo de Control de Transmisión/Protocolo de Internet (en inglés *Transmission Control Protocol/Internet Protocol*).
- AVI: Intercalado de Audio y Video
- DNS: El Sistema de Nombres de Dominio (DNS, *Domain Name System*) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.
- WCCP**:** Es un protocolo definido por Cisco que se emplea para definir la manera de redirigir el tráfico IP desde un router a un proxy-caché.
- GZIP**:** es una abreviatura de GNU ZIP, un software libre GNU que reemplaza al programa *Compress* de UNIX el cual comprime archivos.

Anexos

Anexo1: Información detallada por usuarios



sarg.get.cfg/2017May01-2017May31/index.html

Search

SARG Squid Analysis Report Generator

Squid User Access Reports

Period: 2017 may 01—2017 may 31

Sort: bytes, reverse

Top users

Top sites

Sites & Users

Downloads

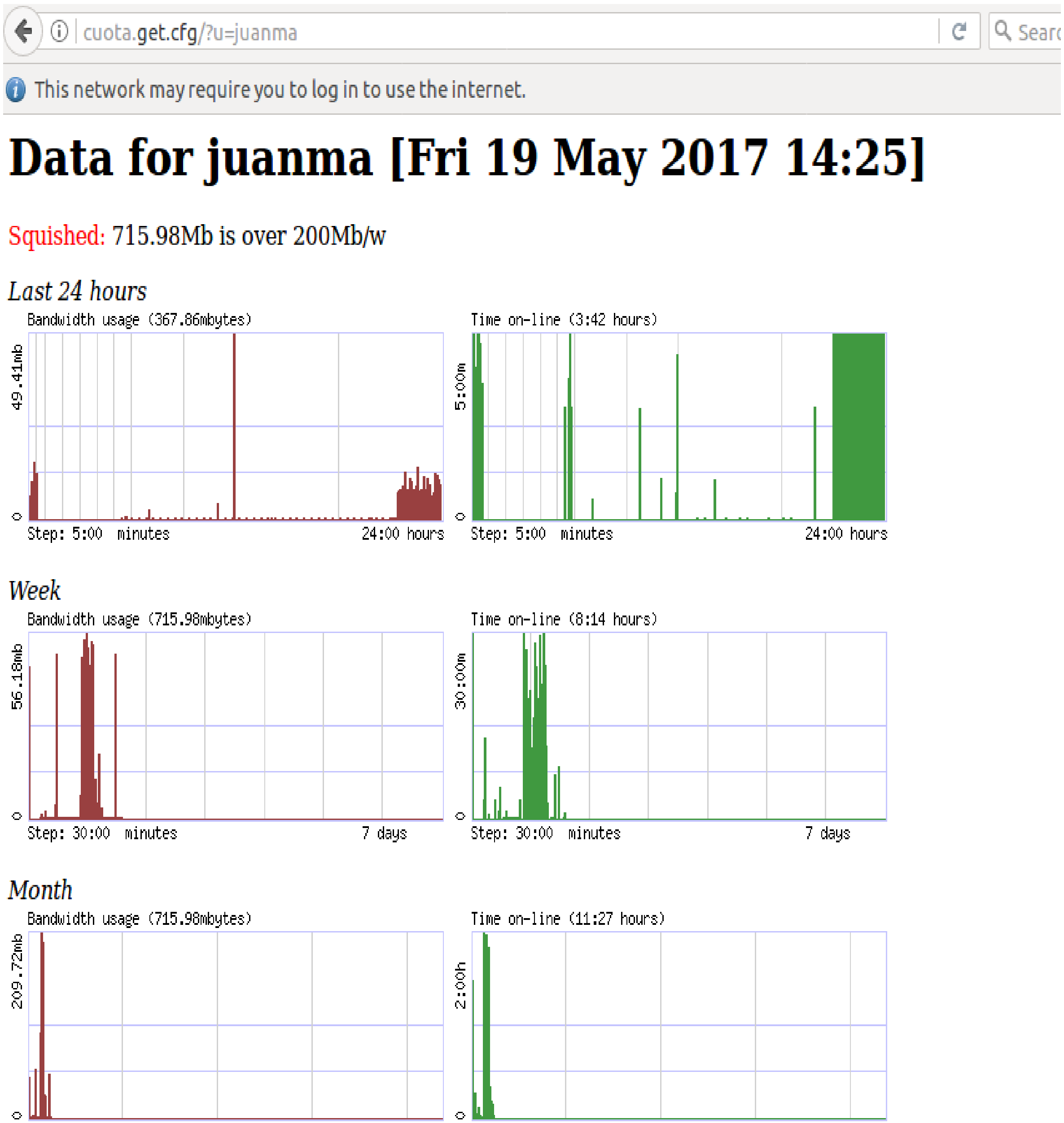
Denied accesses

Authentication Failures

NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
1		juanma	7.90K	2.08G	64,92%	95,03%	4,97%	135:33:52	488.032.349	47,14%
2		ejose	6.74K	351.75M	10,94%	90,80%	9,20%	27:34:37	99.277.326	9,59%
3		dorian	4.65K	228.03M	7,09%	26,43%	73,57%	30:49:52	110.992.766	10,72%
4		wsus	29.46K	126.97M	3,95%	0,01%	99,99%	08:29:48	30.588.044	2,95%
5		maribel	1.77K	117.57M	3,66%	55,41%	44,59%	21:16:26	76.586.221	7,40%
6		greneter	914	105.82M	3,29%	94,63%	5,37%	11:33:03	41.583.756	4,02%
7		rpadilla	7.16K	93.03M	2,89%	48,57%	51,43%	26:23:16	94.996.909	9,18%
8		diana	1.18K	48.65M	1,51%	83,50%	16,50%	13:28:49	48.529.425	4,69%
9		yeny	1.15K	37.01M	1,15%	63,66%	36,34%	07:02:35	25.355.870	2,45%
10		martica	824	10.14M	0,32%	88,91%	11,09%	02:34:45	9.285.248	0,90%
11		juana	991	9.50M	0,30%	67,81%	32,19%	02:45:55	9.955.593	0,96%
		TOTAL	**62.77K**	**3.21G**		**82,51%**	**17,49%**	**287:33:03**	**1.035.183.507**	
		AVERAGE	**5.70K**	**292.41M**				**26:08:27**	**94.107.591**	

Generated by sarg-2.3.10 Apr-12-2015 on may/19/2017 14:47

Anexo 2: Reporte del ancho de banda realizado por el usuario Juanma



Anexo 3: Reporte de los 100 sitios más visitados

sarg.get.cfg/2017May01-2017May31/topsites.html

Search

Squid Analysis Report Generator

Squid User Access Reports

Period: 2017 may 01—2017 may 31

Top 100 sites

NUM	ACCESSED SITE	CONNECT	BYTES	TIME	USERS
1	cifras.beisbolcubano.cu	4.64K	2.72M	3:14:47	1
2	cuota.get.cfg	1.31K	506.49K	0	2
3	dnl-19.geo.kaspersky.com	820	20.06M	0:05:42	1
4	detectportal.firefox.com	806	525.66K	0:04:15	5
5	media.cubadebate.cu	739	15.11M	0:10:22	6
6	encrypted-tbn0.gstatic.com:443	665	25.24M	1:08:21	8
7	dnl-06.geo.kaspersky.com	644	15.28M	0:06:04	1
8	dnl-04.geo.kaspersky.com	610	9.54M	0:08:00	1
9	as02.epimg.net	609	1.52M	0:05:48	1
10	dnl-07.geo.kaspersky.com	600	15.48M	0:07:47	1
11	a.espncdn.com	582	17.40M	0:15:36	1
12	i.ytimg.com:443	575	19.02M	12:36:06	9
13	images.spot.im:443	519	3.37M	1:47:20	1
14	www.google.com.cu:443	496	26.96M	11:04:32	9
15	62.128.100.217:443	481	0	0:09:54	1
16	dnl-09.geo.kaspersky.com	479	15.13M	0:05:14	1
17	62.128.100.163:443	477	0	0:08:34	1
18	www.sediv.net	475	31.18M	0:26:23	1
19	62.128.100.161:443	468	0	0:08:44	1
20	38.113.165.110:443	467	0	0:11:30	1
21	38.113.165.77:443	467	0	0:08:47	1
22	62.128.100.49:443	467	0	0:07:49	1
23	62.128.100.55:443	466	0	0:08:41	1
24	62.128.100.43:443	465	0	0:10:16	1
25	81.19.104.45:443	463	0	0:09:22	1
26	81.19.104.39:443	459	0	0:09:06	1
27	81.19.104.42:443	459	0	0:08:18	1
28	180.87.4.151:443	458	0	0:08:11	1
29	dnl-17.geo.kaspersky.com	456	12.75M	0:04:18	1
30	62.128.100.221:443	455	0	0:09:47	1
31	www.smscubano.com	454	3.87M	0:08:18	1
32	62.128.100.47:443	454	0	0:10:06	1

Anexo 4: Reporte de sitios visitados de un usuario específico

sarg.get.cfg/2017May01-2017May31/juanma/juanma.html

Search

Squid Analysis Report Generator

Squid User Access Reports

Period: 2017 may 01—2017 may 31

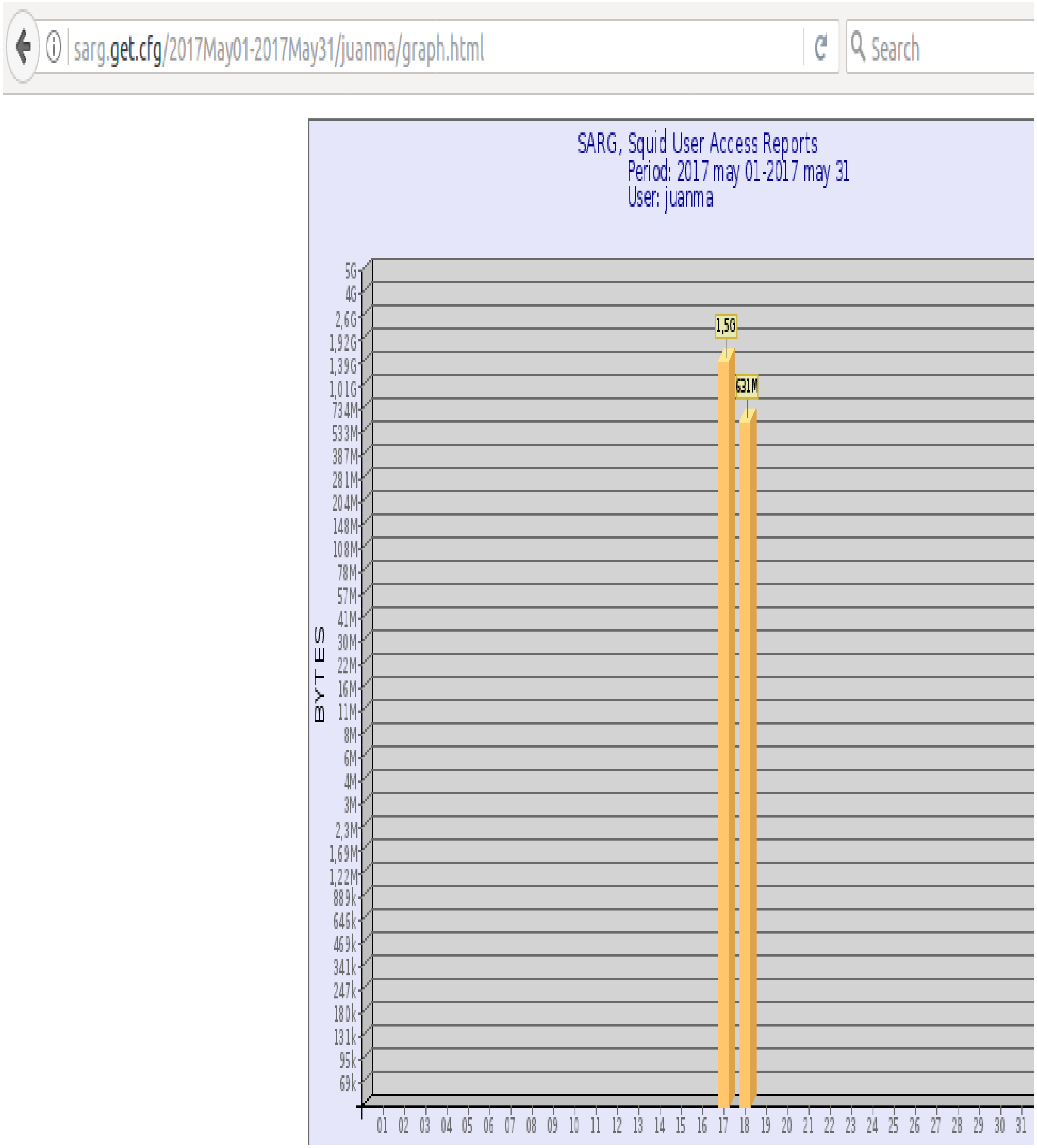
User: juanma

Sort: bytes, reverse

User report

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
r1---sn-xuxjn5-i58e.googlevideo.com:443	424	683.77M	32,75%	100,00%	0,00%	05:50:17	21.017.504	4,31%
r2---sn-xuxjn5-i58e.googlevideo.com:443	275	411.44M	19,71%	100,00%	0,00%	03:52:08	13.928.769	2,85%
r3---sn-xuxjn5-i58e.googlevideo.com:443	273	377.19M	18,06%	100,00%	0,00%	03:50:15	13.815.704	2,83%
r4---sn-xuxjn5-i58e.googlevideo.com:443	194	243.19M	11,65%	100,00%	0,00%	02:34:33	9.273.091	1,90%
r4---sn-vgqsrnee.googlevideo.com:443	33	76.40M	3,66%	100,00%	0,00%	00:55:25	3.325.219	0,68%
s3.amazonaws.com:443	3	49.51M	2,37%	100,00%	0,00%	00:04:00	240.376	0,05%
de.archive.ubuntu.com	60	21.28M	1,02%	0,00%	100,00%	00:04:59	299.203	0,06%
www.youtube.com:443	199	20.41M	0,98%	100,00%	0,00%	12:49:24	46.164.935	9,46%
br.archive.ubuntu.com	65	16.91M	0,81%	7,98%	92,02%	00:06:13	373.169	0,08%
r7---sn-5uaeznlz.googlevideo.com:443	3	12.97M	0,62%	100,00%	0,00%	00:05:14	314.458	0,06%
open.cachefly.net	30	11.45M	0,55%	0,00%	100,00%	00:05:27	327.850	0,07%
i.ytimg.com:443	501	10.94M	0,52%	100,00%	0,00%	09:06:41	32.801.946	6,72%
d.wintouch.cc	4	8.61M	0,41%	0,00%	100,00%	00:07:45	465.345	0,10%
ftp.jaist.ac.jp	2	8.49M	0,41%	0,00%	100,00%	00:01:55	115.776	0,02%
download.openvz.org:443	4	7.35M	0,35%	100,00%	0,00%	00:07:04	424.152	0,09%
security.ubuntu.com	73	6.66M	0,32%	28,60%	71,40%	00:03:02	182.335	0,04%
ftp.gwdg.de	4	6.46M	0,31%	0,00%	100,00%	00:07:05	425.081	0,09%
cdn.rt.com:443	48	5.97M	0,29%	100,00%	0,00%	00:52:00	3.120.456	0,64%
www.google.com.cu:443	199	5.83M	0,28%	100,00%	0,00%	03:05:49	11.149.187	2,28%
esp.rt.com:443	98	5.38M	0,26%	100,00%	0,00%	01:00:27	3.627.270	0,74%
mirror.vtti.vt.edu	4	5.21M	0,25%	0,00%	100,00%	00:00:58	58.726	0,01%
yt3.ggpht.com:443	199	5.08M	0,24%	100,00%	0,00%	04:28:35	16.115.800	3,30%

Anexo 5: Reporte de cuota consumida por un usuario en un período de tiempo.



Anexo 6: Archivo de configuración del e2guardian

```
  GNU nano 2.3.1                    File: /etc/e2guardian/e2guardianf2.conf

# e2guardian filter group config file for version 3.4.0.3


# Filter group mode
# This option determines whether members of this group have their web access
# unfiltered, filtered, or banned.
#
# 0 = banned
# 1 = filtered
# 2 = unfiltered (exception)
#
# Only filter groups with a mode of 1 need to define phrase, URL, site, extension,
# mimetype and PICS lists; in other modes, these options are ignored to conserve
# memory.
#
# Defaults to 0 if unspecified.
# Unauthenticated users are treated as being in the first filter group.
groupmode = 1

# Filter group name
# Used to fill in the -FILTERGROUP- placeholder in the HTML template file, and to
# name the group in the access logs
# Defaults to empty string
#groupname = ''
groupname = 'usuarios'

# Enable legacy (DG) ssl logic
#
# Note that the logic for handling SSL is changed. In DG when either blanket block (or SSL blanket block)
# was active then an SSL site would not be blocked if site name matched either exceptionsitelist or greysitelist.
# In e2guardian with blanket block (or SSL blanket block) active an SSL site will only be allowed if it matches
# exceptionsitelist or greysslsitelist. This ensures that only trusted sites can be accessed via SSL.
# The greysslsitelist is used in order to allow a site to drop through so that it's domain can be mangled via urlregexplist,
# e.g. To use the Google mechanism for prevention of https Google search, or to allow an SSL site whilst blocking the corresponding http: sit$
#
# Default off (logic as above)
                                        [ Read 483 lines ]
^G Get Help      ^O WriteOut      ^R Read File     ^Y Prev Page     ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify       ^W Where Is      ^V Next Page     ^U UnCut Text    ^T To Spell
```

Anexo 7: Guía general de configuración

Update repositories and upgrade packages

Next weâ€™ll update the repository list and then apply any updates so weâ€™re kept secure.

```
>#apt-get update
>#apt-get upgrade
```

Install our packages!

Now onto the install itself! The following command will install everything we need: Samba, Squid, DansGuardian, Webmin and a few dependencies on the side. It asks for the debian install CD to be inserted part way in, and depending on the speed of your internet connection could take several minutes.

```
>#apt-get install dnsmasq webmin squid dansguardian samba
winbind krb5-user libcompress-zlib-perl resolvconf ntp ntpdate
```

It will ask to specify your workgroup/domain you want the server to be in, enter your domain in caps like this: EXAMPLE and not like this EXAMPLE.LOCAL

Configure Kerberos

Next a small bit of configration to take care of:

```
>#dpkg-reconfigure krb5-config
```

It will ask for:

    Default Kerberos version 5 realm: EXAMPLEDOMAIN.LOCAL
    Add locations of default Kerberos servers to
/etc/krb5.conf? No

Anexo 8: Guía general de configuración

Configure NTP with your domain

Networks run better when all the machines have the same time, so weâ€™ll change us from getting Network Time Protcotol updates from Debians servers to just using our domain controller.

Add server domaincontroller.exampledomain.local iburst to /etc/ntp.conf below
pool.ntp.org maps to about 1000 low-stratum NTP servers. Your server will
pick a different set every time it starts up. Please consider joining the
pool:
server 0.debian.pool.ntp.org iburst
server 1.debian.pool.ntp.org iburst
server 2.debian.pool.ntp.org iburst
server 3.debian.pool.ntp.org iburst
and comment out the four Debian time server entries.

Configure Samba

Make a backup copy of /etc/samba/smb.conf before we start to edit it.
>#nano /etc/samba/smb.conf
Under the section labeled â€œAuthenticationâ€ add security = ads below the line which reads # security = user

Anexo 9: Guía general de configuración

immediatly below the line ; domain logons = yes

Under the â€oMiscâ€ section, find the following two lines:
; idmap uid = 10000-20000
; idmap gid = 10000-20000
and uncomment them (remove the â€˜;â€™ from the begining of each line.)

At this point add the following three lines, just above the next section marked â€oShare Definitionsâ€
winbind trusted domains only = yes
realm = EXAMPLEDOMAIN.LOCAL
winbind cache time = 3600

******************************Adicional a esto
Edit /etc/samba/smb.conf and fill in the Windows AD Server information (workgroup, password server, and realm) under the [global] section. In this example, bright is used as workgroup, bcm.bright.local is used as password server, and BRIGHT.LOCAL is used as an Active Directory realm. The rest of the parameters should be kept the same.

Anexo 10: Guía general de configuración

```
[global]
   workgroup = bright
   password server = bcm.bright.local
   realm = BRIGHT.LOCAL
   encrypt passwords = yes
   winbind enum groups = yes
   winbind enum users = yes
   winbind use default domain = yes
   security = ADS
   debuglevel = 2
   wins support = no
   idmap uid = 10000-20000
   idmap gid = 10000-20000
   template shell = /bin/false
   winbind offline logon = false
```

y comentar workgroup = WORGROUP
****

All done for smb.conf, so save and exit.

Prepare to join the domain

Restart samba, winbind and synchronize the time with the domain controller.

```
net time set -S domaincontroller
/etc/init.d/winbind stop
/etc/init.d/samba restart
/etc/init.d/winbind start
```

Join the domain

First reboot: this may not be needed but it seems to help.
Join the machine to the domain:
>#kinit Administrator   El comando kinit es un script de inicialización de Kerberos que hace referencia a la cuenta de administrador de Active Directory y al dominio Kerberos. Como Active Directory requiere tickets Kerberos, kinit obtiene y almacena en caché un ticket de concesión de tickets Kerberos para la autenticación cliente / servidor.

Anexo 11: Guía general de configuración

```
>#net ads join -U Administrator
Dado que la máquina window1 se encontró automáticamente en el
dominio Kerberos correspondiente (el comando kinit tuvo
éxito), el comando net se conecta al servidor Active Directory
utilizando su cuenta de administrador y contraseña requeridas.
Esto crea la cuenta de máquina adecuada en Active Directory y
otorga permisos al servidor miembro del dominio Samba para
unirse al dominio.
Youâ€™ll be asked for the password of the domain user you
specify at the end of the command, once for each command. You
should get:
root@proxy:~# kinit Administrator
Password for Administrator@EXAMPLEDOMAIN.LOCAL:
root@sbproxy:~# net ads join -U Administrator
Enter Administrator's password:
Using short domain name -- EXAMPLEDOMAIN
Joined 'PROXY' to realm 'exampledomain.local'

As this sometimes gives a positive result without actually
doing whatâ€™s required, the following is an essential check:
wbinfo -t
This should give: checking the trust secret for domain
EXAMPLEDOMAIN via RPC calls succeeded. If this step fails, you
canâ€™t procede. Rebooting a few times and starting from the
begining of â€˜Join the domainâ€™ should fix it.

Final checks on having the domain auth working, try these to
commands, the first of which should all the users in the
domain (which does mean it can take some time!) and the second
of which should list all the groups on the domain.
wbinfo -u
wbinfo -g
```

Anexo 12: Guía general de configuración

Configure Squid

Make a backup copy of /etc/squid/squid.conf before we start to edit it.

Add the following three lines below the block of #auth_param that are there, leave them incase you want to change something in the future.

```
auth_param ntlm program /usr/bin/ntlm_auth --helper-
protocol=squid-2.5-ntlmssp
auth_param basic program /usr/bin/ntlm_auth --helper-
protocol=squid-2.5-ntlmssp
auth_param basic realm exampledomain
```

Add:

```
acl ntlm_auth proxy_auth REQUIRED
http_access allow ntlm_auth
```

above:

```
# Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager
# Only allow purge requests from localhost
http_access allow purge localhost
http_access deny purge
# Deny requests to unknown ports
http_access deny !Safe_ports
# Deny CONNECT to other than SSL ports
http_access deny CONNECT !SSL_ports
```

Anexo 13: Guía general de configuración

```
Configure Squid

Make a backup copy of /etc/squid/squid.conf before we start to
edit it.

Add the following three lines below the block of #auth_param
that are there, leave them incase you want to change something
in the future.
auth_param ntlm program /usr/bin/ntlm_auth --helper-
protocol=squid-2.5-ntlmssp
auth_param basic program /usr/bin/ntlm_auth --helper-
protocol=squid-2.5-ntlmssp
auth_param basic realm exampledomain

Add:
acl ntlm_auth proxy_auth REQUIRED
http_access allow ntlm_auth
above:
# Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager
# Only allow purge requests from localhost
http_access allow purge localhost
http_access deny purge
# Deny requests to unknown ports
http_access deny !Safe_ports
# Deny CONNECT to other than SSL ports
http_access deny CONNECT !SSL_ports
```

Anexo 12: Configuración del Squish

```
### added by squish (begin)
# acl's for squish - autodetected, sometimes
acl SQUISHLOC dst proxy-jm.get.cfg
acl SQUISHED1 proxy_auth -i "/etc/squid/squished"
# acl SQUISHED2 ident "/etc/squid/squished"
#### NO IP ####acl SQUISHED3 src "/etc/squid/squished"
# Error info that says you're squished
#### WEB ABAJO ####deny_info http://proy-jm.get.cfg/squish/?
squishe
deny_info http://cuota.get.cfg/?squished& SQUISHED1
# deny_info http://proy-jm.ucf.edu.cu/squish/?squished& SQUISHED2
#### NO IP ####deny_info http://proy-jm.get.cfg/squish/?squished&
S
# HTTP access controls for squish
#http_access allow SQUISHLOC
#http_access allow ntlm_auth !SQUISHED1
http_access deny SQUISHED1
# http_access deny SQUISHED2
#### NO IP ####http_access deny SQUISHED3
### added by squish (end)
```