ISSN: 1692-7257 - Volumen 1 – Número 33 - 2019
Revista Colombiana de Tecnologías de Avanzada

Recibido: 10 de marzo de 2018
Aceptado: 16 de julio de 2018

# IMPLEMENTACIÓN DE UN SISTEMA PROXY DE NAVEGACION SEGURA EN EL GET DE CIENFUEGOS

IMPLEMENTATION OF A PROXY SYSTEM OF SAFE NAVIGATION IN THE GET OF CIENFUEGOS

Ing. Juan Manuel Castellanos Hernández[*], Ing. Frank Manuel López Pérez-Borroto[2**]

[*] Ministerio de Turismo, Cienfuegos Cuba.
juanma@get.cfg.tur.cu.
[**] Programa de informática. Universidad de Cienfuegos.
Carretera de Rodas Km 4, Cienfuegos, Cuba.

**Resumen:** El objetivo fue implementar un sistema de proxy gratuito basado en software libre para el logro de mayor seguridad y control en el Grupo de Electrónica para el Turismo de Cienfuegos (GET). Esta entidad utiliza un proxy Kerio para el control de la red, programa limitado por la compra de licencias. Se identificaron softwares y protocolos existentes para un sistema proxy de navegación segura. Se caracterizó la red de datos del GET de Cienfuegos. Se compararon los softwares existentes para el sistema. Se propuso el Squid como servidor proxy por su fortaleza y seguridad, el E2guardian como filtro web por su potencial, el Squish para el control de cuota por ser el único programa de software libre. Además, se escogieron los métodos de autenticación NTLM por ser el método más seguro entre los tres niveles de autenticación del Squid, Se implementó en una Pc corei3 con el Promox versión 4.4.

**Palabras clave:** software libre, redes, seguridad

**Abstract:** The objective was to implement a free proxy system based on free software to achieve greater security and control in the Group of Electronics for Tourism of Cienfuegos (GET). This entity uses a Kerio proxy to control the network, a program limited by the purchase of licenses. Existing software and protocols were identified for a secure navigation proxy system. The GET data network of Cienfuegos was characterized. The existing software for the system was compared. Squid was proposed as a proxy server for its strength and security, the E2guardian as a web filter for its potential, the Squish for quota control for being the only free software program. In addition, the NTLM authentication methods were chosen as the most secure among the three levels of authentication of the Squid. It was implemented in a Pc corei3 with Promox version 4.4.

**Keywords:** free software, networks, security

## 1. 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. Para mantener la seguridad de cualquier entorno de software se deben tener en cuenta diferentes conceptos como 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 y cuándo fueron enviados y recibidos también sean correctos**.** Además, es necesario otros procesos como autorización, privacidad: disponibilidad e integridad:

En el mundo actual se hace cada vez más común el uso de un servidor proxy (Informática, 2017), un servidor que hace de 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.

Un proxy permite conectar 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 web, descargar un fichero mp3, etc), es realmente el proxy quien realiza la comunicación y a continuación envía el resultado al equipo que solicitó dicha información (Alvernia & Rico (2017) (DEC Márquez, TV Pérez. 2018).

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 web, que previamente ha sido almacenada en la caché, la respuesta y el tiempo de visualización es más rápido (Hight-Tech, 2017).

## 2. METODOLOGIA

**Identificación de softwares y protocolos adecuados para una mayor seguridad y control del sistema proxy en el GET de Cienfuegos**

Se realizó un análisis del estado del arte con bibliografía actualizada buscando alternativa a Keiro con software libres.

**Selección de herramientas a utilizar en el sistema.**

**Se analizaron diferentes sistemas de Proxy como***:* Squid (SQUID, 2008), Tinyproxy (Calamar, 2017), WebCleaner (WebCleaner, 2017) comparados con Kerio (Kerio Control, 2012) que 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 pueden encontrar: inspección profunda de paquetes, inspección de protocolo Servidor de protocolo de Configuración Dinámica de Host (DHCP, *Dynamic Host Configuration Protocol*) y posee un filtrado de dirección física (MAC, *Media Access Control*) y otros soportes (Kerio, 2012)

Se revisaron las ventajas de diferentes software para el filtrar contenidos de la web como ya que lo que usualmente se recomienda es ver al filtrado como un proceso de inspección y no tratar de corregir los datos, es mejor forzar a los usuarios a jugar con las reglas válidas (UNAM, 2016). Se analizaron DansGuardian (DansGuardian, 2017), E2guardian (E2guardian, 2017) Nxfilter (Fernández, 2014), SquidGuard software que se puede instalar en debe instalarse en un equipo Unix o Linux, como un equipo servidor. El filtrado del software se extiende a todos los equipos de una organización, incluidos los equipos Windows y Macintosh.

**Análisis de Software para el control de las cuotas de usuarios.** Se analizaron el Squish: Un software bajo Licencia General Pública (GPL) que ofrece el código fuente y es libre de costo alguno, nos permite un mayor control de los usuarios de forma tal que podemos 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.

**Se analizaron diferentes Software para el análisis de logs como:** SARG (SARG, 2017) y Free-Sa (LightSquid, 2017).

**Análisis de Protocolos para la seguridad en la autentificación** Se revisaron los Kerberoscon diferentes funciones: Autenticación, Integridad de datos, nivel de Privacidad de datos y las diferentes arquitecturas de los Kerberos como El KDC (Red Hat Enterprise, 2017), el NTLM (NTLM, 2017), Digest (Digest, 2017)y el LDAP [ LDAP, 2017]

**Diseño de un sistema proxy de navegación segura.**

A partir de la caracterización de la ret de GET Cienfuegos y las ventajas de los softwares analizados se diseñó un sistema proxy de navegación segura.

**Validación el sistema proxy de navegación segura**

Se validó el sistema utilizando los servicios en una Pc corei3 con el Promox versión 4.4, en conexión con el proxi del MINTUR en la Habana.

.

## 3. RESULTADOS

**Identificación de softwares y protocolos adecuados para una mayor seguridad y control del sistema proxy en el GET de Cienfuegos.**

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 para 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 están 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 ADSL 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 en Cienfuegos (Figura 1)

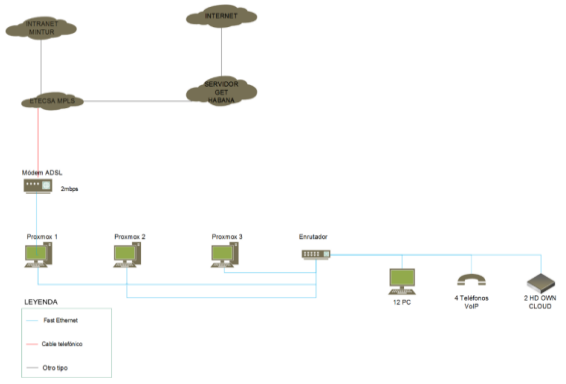



Figura 1: Caracterización de la red de GET de Cienfuegos

Comparación entre los proxys de navegación.

Taba 1: Ventajas y desventajas del Kerio

| Ventajas: | Desventajas |
|---|---|
| Inspección profunda de paquetes<br>Inspección de protocolos<br>Inspección del estado de los paquetes<br>Servidor DHCP<br>Reenvío de DNS<br>Asignación de Traducción de Direcciones de Red (NAT,*Network Address Translation*)<br>Filtrado de MAC<br>Detección de intrusos<br>Red de invitado con portal cautivo<br>Asistente de configuración de reglas de tráfico<br>Reglas basadas en tiempo<br>Inspección Hypertext Transfer Protocol Secure (IHTPS)<br>Capacidad de excepción de la regla<br>Límites de conexión<br>Múltiples direcciones IP en una única interfaz de red<br>DNS dinámico<br>Tabla de enrutamiento personalizable<br>Proxy inverso<br>IPv4 simultáneo y soporte IPv6<br>Traducción de prefijo de red IPv6<br>La división de túnel u opción de túnel forzada<br>Túneles de sitio a sitio múltiples/simultáneas<br>Posee una red privada virtual (Virtual Private Network ,VPN) de cliente a sitio y de sitio a sitio<br>Conexión opcional persistente<br>Múltiples conexiones VPN almacenadas<br>Fuerte encriptación SSL<br>Soporta *VPN*<br>Soporta *NAT*<br>Enrutamiento automático o personalizado<br>Módulo de reportes estadísticos de Kerio Control<br>Informes detallados de uso: Sitios web, protocolos y ancho de banda<br>Reportes individuales por usuario, grupos, o toda la red<br>Reportes automatizados de correos diario/semanal/mensual<br>Sitios más visitados y clasificación de usuarios por categoría web<br>Reporte de tráfico por hora por usuario<br>Palabras clave de búsqueda en Google<br>Informe de filtrado web de Kerio Control<br>Registro externo para syslog<br>Monitoreo SNMP (El Protocolo Simple de Administración de Red)<br>Gráficas de tráfico<br>Tablero de administración<br>Clasificación de tráfico (multimedia, mensajería, transferencia de archivos grandes) | Se necesita del pago de una licencia para su utilización por ser un software de carácter privativo. Si la compañía del fabricante del software desaparece, la posibilidad de tener versiones mejoradas de dicho software y de corregir errores es nula. |

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.

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.

Sigue los protocolos ICP, protocolo para la consulta (HTCP, *Hyper Text Caching Protocol,*), Protocolo de selección de enrutamiento de cache (CARP, *Cache Array Routing Protocol*) y caché digests.

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.

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.

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, mostrará el que ya se encuentra en el caché en lugar de volver a descargarlo desde Internet.

Permite activar el protocolo SNMP (Protocolo Simple de Administración de Red), este proporciona un método simple de administración de red, que permite supervisar, analizar y comunicar información de estado entre una gran variedad de máquinas.

Está compuesto también por el programa servidor DNS, que se encarga de la búsqueda de nombres de dominio.

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 software 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 software.

Modo anónimo: Permite especificar los encabezados HTTP individuales que se deben permitir y que deben bloquearse.

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.

**Comparación entre filtros de contenido web**
Ventajas y desventajas del Kerio

| Ventajas: | Desventajas |
|---|---|
| Limita el acceso según la dirección URL.<br>Deniega el acceso sobre la base de ocurrencia de palabras prohibidas.<br>Limita el acceso a ciertos servidores FTP.<br>Limita basado en los nombres de archivo. | Posee un filtrado web muy pobre porque se necesita insertar manualmente todos sitios prohibidos por lo que dificulta mucho el trabajo cuando existen softwares para esta función que evitan esta extensa tarea y mejoran el trabajo. |

**Ventajas del E2Guardian**
Incorporado en el sistema de complemento del escáner de contenido que incluye escaneado AV.
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 (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* para detectar *URL* en *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).

**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

**Ventajas de los recopiladores de logs**

**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.

**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.

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.

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

**Desventajas**

**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.

**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.

**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.

Se compararon los softwares existentes para el sistema siendo los mejores en este sentido el Squid como servidor proxy por su amplia bibliografía además de su fortaleza y seguridad en la red, siendo además unos de los proxys más usados a nivel mundial, el E2guardian como filtro web por su potencial en el filtrado que lo hacen mejor que cualquier otro software en esta función siendo este una versión avanzada del DansGuardian, el Squish para el control de cuota por sus característica especial de ser el único programa de software libre

**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, una computadora adicional con el Sarg instalado para el control de los logs del Squid todo se puede apreciar en la Figura 2.

A través del estudio realizado en el GET de Cienfuegos se decidió implementar en la empresa es el Squid por sus características que lo amparan como son software libre, además permite integrarse con otros programas y posee una extensa bibliografía, así como el software 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 software 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 usó el Kerberos por su seguridad en la autenticidad.

**Configuración del Squid:** 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,, acl work time MTWHF 08:00-14:00, acl work time 00:00-06:00, acl mwork time MTWHF 08:00-14:00*

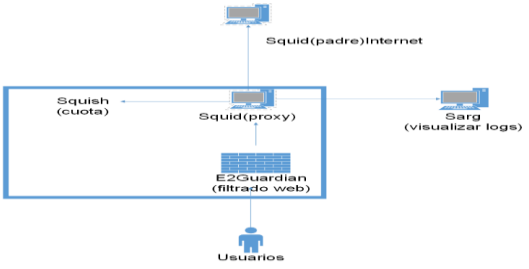



Figura 2: Diseño de la propuesta de sistema proxy a implementar

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 las IP nacionales porque estas si puedes 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 falla. 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 indica que al mismo lugar el máximo de conexiones es 5 para evitar que la red colapse. 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.Luego 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 el 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.

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 (Figura 3).


Figura 3: Fichero de configuración de filtros por usuario

Se configuraron 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, donde cada filtro posee un fichero diferente, en la figura 5 se puede apreciar la configuración del filtro del grupo de los usuarios.

En el fichero de configuración /etc/e2guardian/list/usuarios/bannedsitelist indica que a 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. Estos se encuentran organizados por chat, ropa, teléfonos, culinaria, ropa, droga, gobierno, juegos etc. Esto permite permite bloquear todos esos dominios prohibidos a los usuarios. Se puede agregar cualquier dominio que se quiera bloquear.

**Configuración del Sarg:** Se configura el fichero usr/local/etc/sarg.conf, se utilizó el comando acces_log, el mismo te 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.

**Configuración del Squish:** En el archivo de configuración /etc/squid/squish.conf (Figura 4) se puede observar 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. 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.

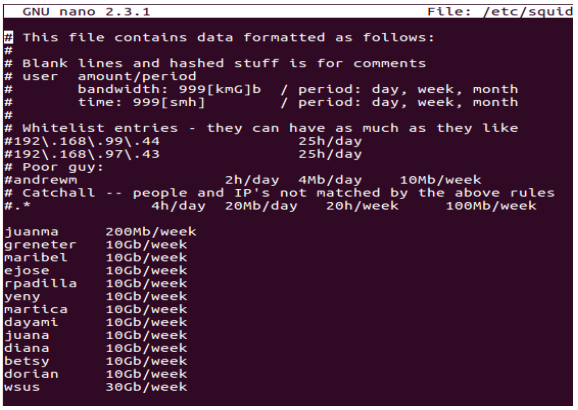
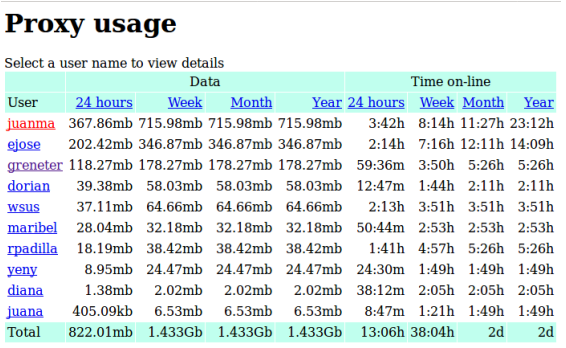



Figura 4: Configuración del fichero squish.conf

Además, se agregó una ACL diciendo cual es el dominio donde tenemos 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. En la figura 5 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.



**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 5: Registro de la cuota de los usuarios

Se implementó el sistema de navegación segura a raíz del estudio realizado anteriormente resultando un sistema auxiliado de programas específicos para el control de la red del GET de Cienfuegos con la seguridad señalada por Rico et al., (2011). Se crearon dos máquinas virtuales una con el Squid y otra con el Sarg complementándose entre ellas.

## 4. CONCLUSIONES

Se identificaron softwares y protocolos existentes para un sistema proxy de navegación segura en el GET de Cienfuegos. Se caracterizó la red de datos del GET de Cienfuegos. Se compararon los softwares existentes para el sistema siendo los mejores en este sentido el Squid como servidor proxy por su amplia bibliografía además de su fortaleza y seguridad en la red, siendo además unos de los proxys más usados a nivel mundial, el E2guardian como filtro web por su potencial en el filtrado que lo hacen mejor que cualquier otro software en esta función siendo este una versión avanzada del DansGuardian, el Squish para el control de cuota por sus característica especial de ser el único programa de software libre. Además, se escogieron los métodos de autenticación NTLM por ser el método más seguro entre los tres niveles de autenticación del Squid, Se diseñó la implementación con los softwares adecuados y se implementó utilizando los servicios en una Pc corei3 con el Promox versión 4.4 siendo la versión más actualizada hasta el momento.

## REFERENCIAS

S. A. A. Acevedo, D. R. Bautista. (2017). Análisis de una red en un entorno IPV6: una mirada desde las intrusiones de red y el modelo TCP/IP. REVISTA COLOMBIANA DE TECNOLOGÍAS DE AVANZADA, ISSN: 1692-7257. 1(29).

Alvernia Acevedo, S., & Rico Bautista, D. (2017). Análisis de una red en un entorno IPV6: una mirada desde las intrusiones de red y el modelo TCP/IP. REVISTA COLOMBIANA DE TECNOLOGÍAS DE AVANZADA, 1(29).

Calamar. (2016). Calamar Proxy Alternativa. [En línea]. Disponible en: http://letras-diferentes.info/computadoras/calamar-proxy-alternativa.php.

DansGuardian (2017) «DansGuardian - EcuRed». [En línea]. Disponible en: https://www.ecured.cu/DansGuardian

DEC Márquez, TV Pérez. (2018), Integración De Seguridad Y Gestión De Servicios En El Gobierno De Las Tecnologías De La Información Revista Colombiana de Tecnologías de Avanzada ISSN: 1692-7257.

Digest (2017). «Digest - EcuRed». [En línea]. Disponible en: https://www.ecured.cu/Digest.

E2guardian.(2017).e2guardian-3.4.0.3-1.mga 6.x86_64 RPM. [En línea]. Disponible en: http://www.rpmfind.info/linux/RPM/mageia/cauldron/x86_64/media/core/release/e2guardian-4.1.5-1.mga7.x86_64.html

Fernández E. (2014). «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/.

Hight-Tech (2017) «Qué es un proxy». [En línea]. Disponible en: http://es.ccm.net/faq/2755-que-es-un-proxy.

Informática. (2017). «Instalación de un Servidor Proxy». s/a. [En línea]. Disponible en: http://html.rincondelvago.com/instalacion-de-un-servidor-proxy.html.

Kerio Control. (2012) [En línea]. Disponible en: file:///C:/Users/asus/Downloads/kerio-control-stepbystep-en-7.4.0-5027-p1.pdf.

LDAP (2017). «LDAP - EcuRed». [En línea]. Disponible en: https://www.ecured.cu/LDAP.

LightSquid (2017). «LightSquid Home Site : Home». [En línea]. Disponible en: http://lightsquid.sourceforge.net/.

NTLM (2003). «The NTLM Authentication Protocol and Security Support Provider». [En línea]. Disponible en: http://davenport.sourceforge.net/ntlm.html.

Rico, D. W., Edwin, Q. H., & Carvajal Mora, H. R. (2011). Redes y tecnologías de banda ancha. Tecnologías de acceso de banda ancha. Revista Tecnologías de Avanzada, 1(17), 113–120.

Red Hat Enterprise (2017). «Kerberos». [En línea]. Disponible en: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-kerberos.html.

SARG (2017) «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.

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

UNAM. (2016). «Aspectos Básicos de la Seguridad en Aplicaciones Web | Documentos - CSI -». [En línea]. Disponible en: http://www.seguridad.unam.mx/documento/?id=17.

WebCleaner (2017). «A filtering HTTP proxy — WebCleaner». [En línea]. Disponible en: http://webcleaner.sourceforge.net/.