REVISTA DIGITAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
TELEM@TICA
Revista Telem@tica. Vol. 11. No. 2, mayo-agosto, 2012, p. 72-84 ISSN 1729-3804

TECNOLOGÍAS ACTUALES PARA LA GESTIÓN DE CONFIGURACIÓN Y CONTABILIDAD DEL SERVICIO DE ACCESO A INTERNET

Mercedes González González[1], Alain Abel Garófalo Hernández[2]

[1]Departamento de Telecomunicaciones y Telemática, CUJAE. Ing. mercedes.gg@tesla.cujae.edu.cu

[2]Departamento de Telecomunicaciones y Telemática, CUJAE, Dr. C. Tec alain@tesla.cujae.edu.cu

RESUMEN / *ABSTRACT*

En este artículo se presentan un conjunto de herramientas comerciales y de código abierto para la gestión de configuración y contabilidad en tiempo real del servicio de acceso a Internet a través de servidores proxy. De estas herramientas se explican los componentes o módulos de gestión que las integran y que hacen posible la aplicación de las políticas de la organización en aras de obtener altos índices de productividad laboral y disminuir los costos por el uso de Internet. El objetivo principal de este artículo es presentarle al lector las principales funcionalidades de cada herramienta de forma que le ayude a decidir cuál de ellas se ajusta más a sus necesidades y recursos disponibles.

Palabras claves: gestión de configuración y contabilidad, Internet, módulos de gestión, servidores proxy.

UP-TO-DATE INTERNET ACCESS SERVICE CONFIGURATION & ACCOUNTING MANAGEMENT TOOLS

This article presents a group of commercial and open-source network management tools which perform the configuration and real time billing of the Internet access service through proxy servers. These tools' main features and management modules are in charge of applying business policies, reducing Internet usage costs and improving employees' productivity, so they are explained in detail. This article's main objective is to show the reader these tools´ most important features, so he or she would be more qualified and well-informed to decide which of these tools better meets his or her needs and available resources.

Key words: configuration and billing management, Internet, management modules, proxy servers.

INTRODUCCIÓN

Actualmente, el acceso a Internet se está convirtiendo en una herramienta de trabajo irremplazable para lograr avances en proyectos de investigación y dar cumplimiento a los objetivos organizacionales trazados. Sin embargo, la conectividad ilimitada a Internet pude atentar en contra del rendimiento de los empleados, pues cuando se trata de redes, "rápido" e "ilimitado" no siempre optimizan productividad. En Internet abundan los virus y spyware, los cuales pueden amenazar considerablemente la seguridad y productividad de la organización. Solo basta que un virus logre burlar las barreras de seguridad impuestas, para que corrompa e incluso destruya toda la información almacenada en las computadoras de la entidad, lo que implicaría un tiempo de recuperación de días e incluso semanas. Los spyware roban rutinariamente información sensible, como suelen ser contraseñas y documentos privados. Estos disminuyen radicalmente el rendimiento de las computadoras y hacen aparecer constantemente molestas ventanas que distraen a los usuarios y les toman tiempo al tener que cerrarlas.

Desafortunadamente, Internet se ha convertido en una fuente irresistible de entretenimiento para los empleados durante las horas de trabajo. Actualmente, la mayoría de estos, en cualquier parte del mundo, emplean de 10 minutos a 1 hora navegando por sitios no relacionados con sus responsabilidades dentro de la organización. Entre las principales fuentes de distracción se encuentran: juegos y hacer compras en tiendas en línea, visitar sitios de chat y mensajería instantánea, reservar tickets, leer periódicos, descargar música, juegos e incluso películas. Además, si en la organización se utiliza el servicio de VoIP (Voz sobre IP) para ahorrar dinero en llamadas de larga distancia, es vital que ningún empleado pueda utilizar el ancho de banda completo de la conexión a Internet. De lo contrario las llamadas no podrían realizarse, y pudieran perderse clientes debido a una llamada perdida o a que la calidad de la conversación sea pobre.

El mal uso de Internet no solo repercute en una disminución de la productividad y en una pérdida cuantiosa de capital, sino que crea huecos de seguridad en las redes y las hace sumamente susceptible a ataques externos. Por tal motivo el control en el acceso a Internet es esencial para cada organización, especialmente a la luz de los actuales incrementos de los requerimientos regulatorios. Con este fin han surgidos numerosas herramientas de gestión de redes. En este artículo se pone a disposición de los lectores un análisis de cuatro herramientas de gestión, dos de ellas comerciales: UserGate Proxy & Firewall y Microsoft Forefront TMG 2010/ ISA Server 2004/2006 incluyendo a su módulo Bandwith Splitter, y otras dos de código abierto: SAMS (Squid Accounting Management System) y SICC-IP (Sistema Integrado de Configuración y Contabilidad).

USERGATE PROXY & FIREWALL

UserGate Proxy & Firewall es una solución de gestión compuesta para servidores proxy y firewall, que permite compartir el acceso a Internet entre los empleados de una organización; proteger la red local contra las actividades y software malicioso, tales como ataques de hackers, virus, gusanos y troyanos; realizar cálculos de tráfico; producir reportes y estadísticas acerca del consumo de los usuarios; controlar el acceso a Internet por parte del personal autorizado a partir del filtrado por URL; gestionar el ancho de banda a partir de la imposición de límites de velocidad en el acceso y asignación de cuotas de navegación, y contabilizar en tiempo real el consumo de cada cuenta haciendo uso de un flexible y potente sistema de facturación[1, 2].

El servidor DHCP integrado a UserGate automatiza el proceso de asignación de direcciones IP dentro de la red local y actualiza el mapa dinámico de direcciones cada vez que un dispositivo se conecta o desconecta de la red LAN basándose en las políticas y restricciones definidas por los administradores. Si la máquina en la que está instalado UserGate está conectada a dos o más redes locales, el servidor UserGate puede emplearse como un router para enrutar los paquetes IP entre estas redes LAN. UserGate pude ser utilizado para acceder a ciertos recursos internos desde el exterior de la red, tales como servidores web, FTP, VPN o de correo electrónico. Para hacer esto posible, todas las solicitudes hechas a un puerto y dirección IP externa en una máquina local donde UserGate está corriendo son redireccionadas hacia un servidor interno de acuerdo con la política aplicada. El servidor UserGate dedicado puede accederse remotamente desde cualquier computadora en la red LAN o en Internet donde se haya instalado la Consola de Administración de UserGate[3].

UserGate incluye una serie de servidores proxy para protocolos de la capa de aplicación, tales como HTTP, FTP, SOCKS, POP3, SMTP, SIP y H323. Todos los servidores proxy pueden trabajar en modo transparente, eliminando la necesidad de especificar la dirección IP y el puerto del proxy en las aplicaciones residentes en los ordenadores de los usuarios. Además UserGate incorpora una web cache, lo que acelera las solicitudes del servicio a partir de recuperar el contenido salvado en el almacenamiento local (cache) producto de solicitudes anteriores. Esto incrementa el rendimiento del canal y optimiza el uso del ancho de banda[4].

Los usuarios de UserGate son cuentas a las que se les concede o deniega el acceso a Internet, se les aplican las reglas de tráfico y se les contabiliza el consumo con el fin de generar estadísticas. Un usuario se define a partir de un parámetro específico como una dirección IP o MAC, combinación de usuario/contraseña, una cuenta de Active Directory, entre otros. La compatibilidad con Active Directory permite utilizar información de usuario almacenada de forma centralizada y de esta manera asegurarse de que todos los cambios se reflejen automáticamente en UserGate. Para simplificar la gestión del tráfico, los usuarios pueden combinarse en grupos mediante el uso de la opción “Grupos” de UserGate.

El módulo de filtrado por URL “Entensys” surge debido a la alianza tecnológica entre UserGate Proxy & Firewall y BrightCloud, y está diseñado para permitir el control administrativo sobre las descargas de Internet y restringir el acceso a sitios web potencialmente peligrosos. La base de datos de BrightCloud utilizada en el módulo de filtrado por URL Entensys, constituye una de las más grandes y precisas de la industria con más de 470 millones de URLs divididas en 70 categorías y cubre tanto los sitios más visitados como los sitios que forman la “Long Tail”. “Long Tail” representa los sitios web menos populares y que por tanto son visitados con menor frecuencia que los 20 millones de sitios web más importantes. Los administradores pueden optar por restringir el acceso a ciertos sitios web o categorías en general o seleccionar para cada usuario o grupo de usuarios, qué categorías o sitios web de la base de datos de BrightCloud estarán bloqueados[5].

UserGate tiene un módulo de filtrado de aplicaciones integrado que permite la gestión de aplicaciones y el establecimiento de restricciones en su uso según distintos criterios. Su finalidad es doble: permitir a los administradores restringir el uso personal de aplicaciones basadas en Internet como mensajería instantánea, programas de chat (IRC) o conferencias web, y proteger a la red local de las amenazas externas de Internet. El firewall de aplicaciones de UserGate trabaja sobre la base de reglas definidas por el administrador, las cuales son aplicadas a un usuario o grupo de usuarios [6].

UserGate permite establecer límites en la velocidad de conexión, asignar cuotas de tráfico o definir la cantidad de tiempo que cada usuario podrá estar conectado a Internet. Una forma de establecer un límite de velocidad en UserGate es mediante la creación de una regla de velocidad en el módulo de Política de Tráfico, y luego elegir la regla en las propiedades de un determinado usuario o grupo de usuarios. Además, se pueden especificar parámetros opcionales que definen cómo y cuándo se va a aplicar la regla. Otra forma de restringir la velocidad de la conexión es creando una regla en el Gestor de Ancho de Banda, la cual fija el límite de velocidad para un adaptador específico de red, dirección IP fuente y destino, protocolo y puerto. Este módulo de UserGate, no solo les permite a los administradores configurar los límites de ancho de banda, sino que brinda la posibilidad de establecer las prioridades en el procesamiento de las solicitudes sobre la base de las políticas de la organización [7].

UserGate permite establecer cuotas diarias, semanales o mensuales para el consumo de tráfico. El acceso del usuario a Internet puede ser bloqueado o el plan de facturación cambiado al llegar al límite. Existe una opción que permite especificar los protocolos que serán bloqueados en estos casos y que, por tanto, le confiere mayor flexibilidad al sistema. Por ejemplo, un usuario puede seguir utilizando el correo electrónico (POP3 y SMTP) después de que su límite en el tráfico HTTP haya sido alcanzado. Las limitaciones de velocidad y las cuotas de tráfico pueden complementarse entre sí, permitiendo aplicar un cierto límite de velocidad al alcanzar un determinado consumo. Además de los límites de velocidad y de tráfico, un administrador puede especificar cuánto tiempo le es permitido a un usuario permanecer en línea en dependencia de la hora o día de la semana.

El módulo de Estadísticas de UserGate posee una poderosa capacidad de filtrado lo que permite obtener reportes a partir de parámetros específicos, los cuales pueden ser: rango de fechas, usuario o grupo de usuarios, categoría de sitio web, costo, tamaño de cache o protocolo, entre otros, en cualquier combinación. Por tanto se pueden obtener estadísticas detalladas para cada usuario o grupo, revisar el consumo del tráfico, sitios web visitados, etcétera. De igual manera, en la página de Estadísticas de la Consola de Administración se puede ver el consumo de tráfico por usuario o grupo de usuarios para un período de tiempo específico. Desde esa página, también se puede activar o desactivar una cuenta de usuario o grupo en particular, así como añadirle fondos a su saldo en caso de que se utilice el Sistema de Facturación de UserGate para supervisar y controlar los gastos de tráfico[8, 9].

El Sistema de Facturación de UserGate ejecuta de manera automática los cálculos del consumo de cada usuario basándose en el tiempo y/o volumen de tráfico. A cada usuario se le asigna una tarifa para que el Sistema de Facturación pueda iniciar la recolección de estadísticas. En una tarifa se especifica la tasa de conversión por megabyte de tráfico de entrada y/o salida, así como el costo por hora para un plan de acceso a Internet cronometrado. Este sistema soporta diferentes tarifas para cada usuario o grupo, las cuales cambian de manera dinámica al cumplirse determinadas condiciones. Esto se hace mediante la creación de reglas de tráfico en la Consola de Administración de UserGate. Los ejemplos incluyen el cambio a una tarifa diferente dependiendo de la hora del día (una tarifa para el día, y otra para la noche), día de la semana, dirección del sitio web visitado, o al llegar a un máximo de gasto o límite de descarga. Los administradores pueden añadir fondos a una cuenta de usuario y además establecer que la conexión para un usuario en particular se cancele automáticamente cuando su saldo cae por debajo de una cierta cantidad [10].

Existen dos motores de antivirus integrados en UserGate encargados de chequear todo el tráfico entrante (correo electrónico, FTP, HTTP). Se puede optar por incluir uno o incluso dos de ellos en la instalación de UserGate. Se recomienda el uso de Kaspersky y Panda, los cuales se complementan entre sí y disminuyen el riesgo de una amenaza no detectada. Además de la protección contra malware (virus, gusanos y troyanos), UserGate incorpora un firewall avanzado el cual proporciona inspección profunda de paquetes con el fin de proteger a la red local contra posibles intrusiones de hackers y otros tipos más sofisticados de intrusiones basadas en protocolos. Esto lo logra a partir de bloquear el tráfico por determinados puertos y limitar el uso de ciertas aplicaciones [11].

UserGate permite trabajar con múltiples Proveedores de Servicio de Internet. Esto trae consigo dos beneficios: los usuarios serán automáticamente conmutados hacia una conexión secundaria si la primaria falla y los administradores podrán habilitar distintos proveedores para diferentes grupos de usuarios.

UserGate incluye soporte para conexiones VPN y telefonía IP. Soporta los protocolos SIP y H.323 y por tanto puede utilizarse como una puerta de entrada de VoIP para softphones y teléfonos IP dedicados.

FOREFRONT THREAT MANAGEMENT GATEWAY 2010 (TMG)

Forefront Threat Management Gateway 2010 (TMG) fue construido sobre la base de Microsoft ISA Server 2006 y puede comportarse como un router, un gateway de Internet, un servidor de red privada virtual (VPN), un servidor de traducción de direcciones (NAT) y un servidor proxy, contando con una consola de administración la cual ofrece gestión de políticas local y remota para servidores y facilitando la autenticación y aplicación de políticas a partir de su integración con el Directorio Activo de Windows[12].

Forefront TMG es desplegado en la red como un gateway unificado que inspecciona el tráfico a nivel de la capa de red, aplicación y contenido con el propósito de garantizar una seguridad exhaustiva y liberar al firewall de la organización de funciones que sobrecargan intensivamente al procesador, tales como la inspección de paquetes para detectar malware. El servidor Forefront TMG 2010 proporciona múltiples tecnologías de inspección. Además del firewall a nivel de red y aplicación, cuenta con un poderoso sistema de prevención de intrusos (IPS) que proporciona protección ante las vulnerabilidades basadas en el navegador e incluye soporte para el filtrado por URL y para la detección y eliminación de malware en el tráfico web y de correo electrónico.

Este se conecta al Servicio de Protección Web de Forefront TMG para llevar a cabo el filtrado por URL y las actualizaciones anti-malware. El Servicio de Protección Web de Forefront TMG (incluido en la Suite de Protección de Forefront) distribuye actualizaciones anti-malware y proporciona conexión en tiempo real a tecnologías de filtrado URL basadas en la nube que pueden ser utilizadas para monitorear o restringir el uso de la web por parte de los empleados. Todo ello permite erradicar vulnerabilidades de seguridad y restringir el acceso de los usuarios a sitios web maliciosos o inapropiados, es decir, que pertenezcan a una categoría de contenido que viole políticas de seguridad definidas por la organización [12, 13].

Forefront TMG lleva a cabo la inspección del tráfico HTTPs, es decir, inspecciona el tráfico web de usuario que fluye a través de sesiones encriptadas con el protocolo SSL (Secure Sockets Layer), lo que no solo permite proteger a la organización de los riesgos de seguridad inherentes a los túneles SSL, tales

como virus y otros contenidos maliciosos que pueden infiltrarse en la organización sin ser detectados, sino que se le puede restringir a los usuarios el acceso a sitios aprobados [13].

Con el fin de mejorar el rendimiento de la red, Forefront TMG comprime el tráfico web para elevar la velocidad de la comunicación y cuenta con una memoria cache web en la que se almacena el contenido web regularmente accedido con el objetivo de reducir el tráfico por la red y proporcionar un acceso más rápido a las páginas web más frecuentemente visitadas. De igual manera se programan las descargas de dichas páginas con el fin de actualizarlas en períodos de tiempo en los que el tráfico en la red es estadísticamente bajo. Forefront TMG igualmente pude almacenar en cache datos recibidos a través del Servicio de Transferencia de Fondo Inteligente, como es el caso de actualizaciones de software publicadas en el sitio web de Microsoft Update[13].

Bandwith Splitter es un programa o extensión para Microsoft Forefront TMG 2010 & ISA Server que le añade a esta solución componentes encargados de permitir un uso compartido más racional del ancho de banda de la conexión a Internet existente a partir de distribuirlo entre los usuarios y servidores de acuerdo a reglas prefijadas.

Bandwith Splitter proporciona excelentes habilidades de monitoreo en tiempo real que le permite a los administradores controlar eficazmente el uso del tráfico, distribuye de manera racional el canal de ancho de banda de Internet a partir de la aplicación de reglas predefinidas por el administrador, reduce los costos de Internet al limitar el tráfico no prioritario tales como los intercambios peer-to-peer y las grandes descargas, garantiza rapidez en la conexión de los usuarios importantes pues les reserva mayor ancho de banda y prioriza sus tráficos, lo que repercute en el incremento de eficiencia y productividad, permite que los usuarios puedan consultar el estado de su cuota de tráfico a través de una interfaz web y proporciona reportes sobre el consumo del ancho de banda que permite tomar decisiones estratégicas[14].

Se pueden crear dos tipos de reglas en Bandwidth Splitter: reglas velocidad de tráfico y reglas de cuota de tráfico. El primer tipo de regla controla cuales usuarios pueden acceder a cuales recursos, a cual velocidad y en cual momento, es decir, estructura y conforma el tráfico de red limitando así el ancho de banda de la conexión a Internet utilizada por los usuarios y hosts o grupos de usuarios y hosts. El segundo tipo de regla establece la cuota de tráfico la cual refleja el consumo máximo permitido de tráfico de Internet (en megabytes) autorizado por día, semana, mes o sin límites de tiempo para usuarios individuales y hosts o grupos de usuarios y hosts[15].

Esta herramienta brinda mucha flexibilidad pues se puede programar para que un usuario particular o grupo de usuarios estén limitados a una velocidad de tráfico durante un período de tiempo determinado y que posteriormente este límite de velocidad de tráfico cambie a otro valor durante otro período de tiempo. Se puede incluso configurar límites de velocidad y cuotas de tráfico diferentes en dependencia de si se trata de tráfico de salida o de entrada. Otra opción muy útil es permitir a los usuarios o hosts acumular el remanente de la asignación de ancho de banda o cuota no consumido y sumarlo con la asignación para el nuevo período de tiempo. De igual manera se pueden excluir del proceso de facturación las visitas a ciertos sitios web o suspender la facturación por determinados períodos de tiempo, o todo lo contrario, bloquear el acceso a determinados sitios o durante períodos de tiempo específicos. Igualmente se puede seleccionar la opción de no contabilizar el tráfico almacenado en memoria cache [15].

Las ráfagas HTTP permiten que a un determinado usuario o grupo de usuarios se le asigne un ancho de banda superior al establecido en la regla de velocidad de tráfico que le es aplicada mientras descarga contenido de ciertos tipos de sitios web, de manera que este usuario o grupo de usuarios que han estado inactivos por un determinado período de tiempo puede trabajar a una velocidad superior. El administrador es el encargado de determinar la duración de las ráfagas HTTP y de los períodos de inactividad, así como de los tipos de contenidos para los que se utilizarán las ráfagas HTTP [16].

Bandwith Splitter permite limitar el número de conexiones concurrentes autorizadas para un usuario o host. Si las reglas se han aplicado a un conjunto de usuarios o direcciones IP, se puede escoger entre asignar el ancho de banda o cuota individualmente para cada usuario o dirección IP o si compartir el ancho de banda o cuota entre todos. Finalmente, se puede aplicar la regla de velocidad de tráfico solo cuando se ha consumido la cuota de tráfico, lo que implica disminuir la velocidad de la conexión del usuario en vez de denegarle totalmente el acceso a Internet [15].

Cabe también mencionar que Bandwidth Splitter cuenta con un componente encargado de la generación de reportes que contienen información detallada acerca del uso del ancho de banda por cada usuario, cliente IP, regla de cuota o de conformación del tráfico y con los gráficos que muestren el comportamiento dinámico del uso del ancho de banda[15, 16].

SQUID ACCOUNTING MANAGEMENT SYSTEM SAMS

Squid Account Management System (SAMS) es una herramienta de código abierto que permite gestionar el acceso de los usuarios al servidor proxy Squid. Cuenta con tres modos de autorización: autorización NTML, autorización NCSA y a través de direcciones ip. La inmensa mayoría de las tareas de configuración en SAMS son realizadas a través de su interfaz web y los parámetros de configuración son almacenados en la base de datos del sistema, la cual es gestionada por un servidor MySQL[17].

Para facilitar las tareas de gestión, SAMS permite que los usuarios se agrupen en grupos. Cada usuario pertenece a una de las siguientes cuatro categorías: administradores, auditores, usuarios privilegiados, usuarios de red. Los administradores son aquellos con los permisos necesarios para configurar y gestionar nuevas cuentas de usuarios, los auditores son los responsables de controlar todo el tráfico y no están autorizados a gestionar el sistema, los usuarios privilegiados son aquellos que reciben permisos de acceso extendidos sobre la interfaz web con el fin de que puedan controlar el tráfico del resto de los usuarios que pertenecen a su grupo, y por último, los usuarios de red se les confiere acceso a la interfaz web con el propósito de que puedan controlar su propio tráfico[17].

SAMS permite crear listas para prohibir el acceso de los usuarios a determinados recursos de Internet. Estas listas de control de acceso contiene direcciones de dominios, así como URL de sitios web prohibidos, escritas de acuerdo a la reglas PCRE.

La configuración de las cuentas de usuarios en SAMS se realiza a partir de plantillas. Estas plantillas son asignadas a los usuarios y permiten definir un conjunto de parámetros de configuración tales como las listas de control de acceso que serán aplicadas durante la navegación, la cantidad de tráfico límite o cuota de tráfico que el usuario puede consumir y el período de tiempo por el cual esta cuota estará disponible antes de que se reinicialice, el tiempo máximo autorizado para estar en línea en caso de que se trate de un plan de acceso a Internet cronometrado, el modo de autenticación para el usuario (NTML,

NCSA, dirección ip) y la velocidad máxima permitida para el acceso a Internet. SAMS le inhabilita a los usuarios el acceso al servidor proxy Squid cuando han excedido su cuota de tráfico asignada.

Esta herramienta genera reportes detallados del tráfico de usuario. Estos reportes reflejan el tráfico de entrada, así como los sitios web visitados tanto por usuarios individuales, grupos de usuarios o por todos los usuarios del sistema [17].

SISTEMA INTEGRADO DE CONFIGURACIÓN Y CONTABILIDAD SICC-IP

El Sistema Integrado de Configuración y Contabilidad es un sistema de gestión de código abierto que surgió con el objetivo de controlar el uso del ancho de banda en la conexión a Internet de la red del Instituto Superior Politécnico José Antonio Echeverría. Constituye una plataforma de gestión de contabilidad que integra las tareas de configuración y otorgamiento de los servicios con la facturación, notificación y control de cuotas, presentando un diseño modular que facilita la adición de nuevos requerimientos de gestión [18].

Desde el punto de vista contable, los usuarios en el SICC-IP se agrupan por centros de costo, para el manejo de los cuales se definen administradores de centros de costo y administradores de contabilidad. Estos últimos tienen acceso a toda la información concerniente a la contabilidad del sistema. Los administradores de centros de costo solo acceden a la información relacionada con sus centros de costo. Desde el punto de vista de la configuración, los usuarios se agrupan por unidades administrativas siguiendo una estructura arbórea, las cuales son gestionadas por administradores de unidades y administradores de configuración. Estos últimos tienen acceso a toda la información relativa a la configuración del sistema mientras que los administradores de unidades solo acceden a la información relacionada con sus unidades [18].

Para el uso de un determinado servicio, los usuarios tienen asignada una cuota, la cual está expresada en unidades monetarias y en base a esas unidades se registra el consumo en las tablas correspondiente a cada servicio. La “unidad monetaria” no es más que una unidad de medida que indica el impacto que tiene en la red el uso de los recursos o los servicios por parte de los usuarios y expresa el costo por el consumo del servicio. Para poder diferenciar, de acuerdo a las características del servicio, el impacto del comportamiento del usuario sobre la red en términos de “unidades monetarias”, se aplican diferentes tarifas en diferentes momentos de tiempo o tipos de solicitud de servicio [18].

Actualmente el SICC-IP gestiona servicios tales como el acceso a Internet, el correo electrónico y el acceso telefónico, pero como bien está expuesto en las metas trazadas a la hora de su diseño, se pueden incorporar con pocos esfuerzos aplicaciones de contabilidad y/o configuración a medida que surjan nuevos servicios, así como aplicaciones web que les permitan a los usuarios y administradores relacionarse con el sistema.

Entre los módulos del SICC-IP de obligatoria instalación se encuentran la SICCDB, la LibSICC y el SICC-ADMIN.

La SICCDB es la base de datos principal del sistema donde se almacena el repositorio de políticas del SICC-IP. Contiene un conjunto de tablas que reflejan la información necesaria para gestionar los servicios, así como procedimientos almacenados y disparadores que garantizan el cumplimiento de las políticas de acceso al servicio. Se gestiona mediante un servidor PostgreSQL.

La LibSICC es un paquete de módulos que sirven de interfaz entre el programador y la base de datos y por tanto facilitan el desarrollo de aplicaciones de gestión para el SICC-IP. Requiere Python versión 2.3 o superior.

SICC-ADMIN o, como también se le conoce, "Módulo de gestión de la información básica de soporte" se ocupa de la gestión de la información imprescindible para las funciones e incorporación de servicios al SICC-IP. Este módulo presenta una interfaz de gestión web que les permite a los administradores del SICC-IP crear, modificar y eliminar las cuentas de usuario y de administración con sus roles y ámbitos, las clasificaciones en las que se agrupan los distintos usuarios, los centros de costos que financian los servicios asignados a los mismos y las unidades organizativas utilizadas para mantener la estructura de la organización [19]. La última versión de esta aplicación web está montada en Django, un framework Python, y la información que ella gestiona se almacena en la base de datos del sistema.

La arquitectura del subsistema de configuración para la gestión del servicio de acceso a Internet a través de cache proxy cumple con las especificaciones de los sistemas de gestión de red basada en políticas (PBNM). Entre los componentes de este subsistema se encuentran el Administrador de Políticas (AP), el Repositorio de Políticas (RP) o Base de Datos Principal del sistema (SICCDB) y el componente con funcionalidad de Punto de Decisión de Políticas Local (LPDP) y funcionalidades de Punto de Ejecución de Políticas (PEP/LPDP)[18].

La interfaz web del Administrador de Políticas del subsistema de configuración para el servicio de acceso a Internet a través de cache proxy es también conocida como SICC-PROXY y permite el acceso de administradores y usuarios a los que se les han asignado dicho servicio.

Esta interfaz web les confiere a los administradores del SICC-IP la autorización requerida para definir, modificar y borrar las políticas del servicio de acceso a Internet en aquellas áreas funcionales de las cuales sean responsables y para los usuarios que se encuentren bajo su jurisdicción. Los administradores con permisos de configuración son los responsables de definir para cada cuenta, parámetros tales como la cuota para el consumo del servicio, si este está activo o no, si se desactivará o no ante sobrepaso de la cuota, el período de tiempo por el cual la cuenta será válida, el centro de costo que financiará al servicio, el nombre de la cuenta y su contraseña y la plantilla de configuración asociada al mismo. Esta plantilla de configuración define los protocolos, conexiones y direcciones ip que pueden utilizarse para navegar, así como el servidor proxy que atenderá las solicitudes y el horario en que está autorizada la navegación. Los administradores encargados de la configuración serán los encargados de crear, modificar, eliminar y asignar dichas plantillas. Por su parte los administradores con permisos de contabilidad están autorizados a crear, modificar, eliminar y asignar una plantilla de contabilidad a cada cuenta del servicio. Esta plantilla especifica el horario en que será aplicada y los valores de las variables para el cálculo de los cargos por el consumo del servicio asignado a cada usuario o grupo de usuarios, es decir, define cómo se efectuará la conversión de megabytes a unidades monetarias [19].

Los usuarios pueden acceder a SICC-PROXY con el fin de modificar sus contraseñas, el estado del servicio, es decir, si está activo o no, así como el rango de direcciones IP y los horarios autorizados para la navegación.

Las políticas del servicio son almacenadas en la base de datos del sistema (SICCDB) y consultadas por los módulos encargados de tomar y ejecutar decisiones con respecto a las solicitudes realizadas por parte de los usuarios (LPDP/PEP).

El PEP/LPDP se encuentra corriendo en el servidor proxy Squid que proporciona el servicio de acceso a Internet, siendo esta una de las implementaciones más robustas de cache proxy. El Squid permite la incorporación de software externo para la toma de decisiones respecto a las solicitudes de los usuarios, lo cual se aprovechó para el desarrollo del PEP/LPDP quien de un lado se comunica con el Squid y del otro accede al repositorio de políticas (SICCDB) con el apoyo de la LibSICC[18].

Cada cuenta de usuario creada en SICC-ADMIN tiene asociada una clasificación. Estas clasificaciones de usuario tienen como objetivo agrupar aquellos que presentan características afines. El SICC-IP cuenta con un módulo encargado de traducir dichas clasificaciones a grupos del Dansguardian. Este último es un software de filtrado de contenidos encargado de controlar el acceso a sitios web, es decir, para cada grupo del Dansguardian se aplican uno o varios filtros que restringen el acceso de los usuarios a los recursos de Internet.

De igual manera el SICC-IP cuenta con un módulo denominado SICCSRC, el cual no es más que un subsistema responsable de generar reportes acerca del consumo de los servicios por parte de los usuarios y que construye dichos reportes mediante la interacción con los módulos de contabilidad de cada servicio. Lo que hace que este componente sea extensible a nuevos servicios con relativo poco esfuerzo.

Conclusiones

Las herramientas de gestión son una pieza clave e indispensable para lograr un uso racional y eficiente de la red y sus servicios, y de esta forma garantizar el incremento de la productividad laboral y la disminución de los costos.

Los módulos de filtrado de contenido, de facturación en tiempo real y de generación de reporte y estadísticas acerca del tráfico de usuario están presentes en todas las herramientas comerciales presentadas y constituyen los principales agentes de control de acceso. El SICC-IP, no cuenta con un módulo especializado en filtrado de contenido, sino que para ello utiliza el Dansguardian. No obstante posee un módulo para la generación de reportes sobre el consumo de tráfico por parte de los usuarios y cuenta con un poderoso sistema de facturación que contabiliza en tiempo real el consumo de los usuarios en unidades monetarias, siendo este un mecanismo de cobro más justo en comparación al empleado por la mayoría de este tipo herramientas, incluyendo las presentadas en este artículo, quienes facturan a los usuarios en megabytes o tiempo permanecido en línea.

Las herramientas comerciales no solo cuentan con estas funcionalidades, sino que incluyen muchas otras como es el soporte para conexiones VPN, telefonía IP y múltiples ISP, incluyen módulos de antivirus y anti-spam y pueden comportarse como un router, un firewall de capa de aplicación y capa de red, un servidor DHCP o un servidor proxy. Su principal desventaja radica en que requieren para su instalación y funcionamiento óptimo, de recursos de hardware costos, y se caracterizan por presentar altos precios los cuales se incrementan a medida que crece el número de usuarios. Por tal motivo se recomienda la utilización de herramientas de software libre, que aunque no sean tan completas como las comerciales, cuentan con los componentes requeridos para gestionar los recursos, son extensibles mediante desarrollos propios y están respaldadas por una comunidad de desarrolladores activa y en constante crecimiento.

Referencias Bibliográficas

1. Entensys Corporation, User Gate Proxy & Firewall Administration Manual. 2010. p. 1-44.

2. Entensys Corporation. User Gate Proxy & Firewall Overview. 2010 [cited Febrero 3, 2012]; Available from: http://www.entensys.com/products/usergate/.

3. Entensys Corporation. User Gate Proxy & Firewall Network Administration. 2010 [cited Febrero 3, 2012]; Available from: http://www.entensys.com/products/usergate/network_administration.php.

4. Entensys Corporation. User Gate Proxy & Firewall Proxy Service. 2010 [cited Febrero 3, 2012]; Available from: http://www.entensys.com/products/usergate/proxy_service.php.

5. Entensys Corporation. User Gate Proxy & Firewall Categorized URL Filtering. 2010 [cited Febrero 3, 2012]; Available from: http://www.entensys.com/products/usergate/url_filtering.php.

6. Entensys Corporation. User Gate Proxy & Firewall Application firewall. 2010 [cited Febrero 3, 2012]; Available from: http://www.entensys.com/products/usergate/application_firewall.php.

7. Entensys Corporation. User Gate Proxy & Firewall Speed limitations and traffic cuotas. 2010 [cited Febrero 3, 2012]; Available from: http://www.entensys.com/products/usergate/speed_limitations.php.

8. Entensys Corporation. User Gate Proxy & Firewall Internet traffic monitoring and reporting. 2010 [cited Febrero 3, 2012]; Available from: http://www.entensys.com/products/usergate/traffic_monitoring.php.

9. Entensys Corporation. User Gate Proxy & Firewall Web statistics client. 2010 [cited Febrero 3, 2012]; Available from: http://www.entensys.com/products/usergate/web_statistics.php.

10. Entensys Corporation. User Gate Proxy & Firewall Billing system. 2010 [cited Febrero 3, 2012]; Available from: http://www.entensys.com/products/usergate/billing.php.

11. Entensys Corporation. User Gate Proxy & Firewall Internet Security. 2012 [cited Febrero 3, 2012]; Available from: http://www.entensys.com/products/usergate/internet_security.php.

12. Microsoft. Microsoft Forefront Threat Management Gateway (TMG) 2010 Overview. 2012 [cited Septiembre 3, 2012]; Available from: http://www.microsoft.com/en-us/server-cloud/forefront/threat-management-gateway-overview.aspx.

13. Microsoft. Microsoft Forefront Threat Management Gateway (TMG) 2010 Features. 2012 [cited Septiembre 3, 2012]; Available from: http://www.microsoft.com/en-us/server-cloud/forefront/threat-management-gateway-features.aspx.

14. BNTC Software. Bandwidth Splitter for Microsoft ISA Server & Forefront TMG Overview. 2012 [cited Septiembre 4, 2012]; Available from: http://www.bsplitter.com/.

15. Shinder, D. Product Review: BNTC Software's Bandwidth Splitter. 2010 Octubre 2, 2010 [cited Septiembre 4, 2012]; Available from: http://www.isaserver.org/tutorials/Product-Review-BNTC-Softwares-Bandwidth-Splitter.html.

16. BNTC Software. Bandwidth Splitter for Microsoft ISA Server & Forefront TMG Features. 2012 [cited Septiembre 4, 2012]; Available from: http://www.bsplitter.com/features.aspx.

17. SAMS Team. SAMS (SQUID Account Management System) 2012 [cited; Available from: http://sams.perm.ru/index.php?option=com_content&task=view&id=28&Itemid=1.

18. Garófalo Hernández, A.A., Método y Sistema para la Gestión de Contabilidad y Configuración en redes IP, in Departamento de Telecomunicaciones y Telemática. 2005, Instituto Superior Politécnico José Antonio Echeverría: La Habana. p. 141.

19. Gonzalez Gonzalez, M., Nueva versión de los componentes para la gestión de la información básica de soporte y del servicio de acceso a Internet del SICC-IP, in Departamento de Telecomunicaciones y Telemática. 2012, Instituto Superior Politécnico José Antonio Echeverría: La Habana. p. 163.