Administrador de Proxy basado en Web

GUNNAR WOLF

Octubre, 1999

Abstract

Da una interfaz Web a una de las operaciones más comunes del mantenimiento diario de un proxy: La restricción o control de acceso sobre el uso del proxy.

Contents

1 Cuál es la misión de WPM en este mundo

Hay muchas - y muy buenas - implementaciones de proxies y firewalls para las plataformas Linux y UNIX en general. Sin embargo, el manejarlos siempre ha involucrado ir a la línea de comando para escribir algunos comandos de sintaxis muy obscura, o en el mejor de los casos modificar un archivo de configuración que está perdido en alguna parte de la jerarquía de directorios del servidor. Para todos estos cambios es necesario, además, ser el superusuario (root), siendo imposible permitir que usuarios menos privilegiados hagan estas modificaciones.

Una situación tal vez demasiado común de los centros de cómputo, específicamente de las escuelas, es el tener una gran cantidad de computadoras con una salida demasiado limitada a Internet, típicamente de 64 Kbps. El desarrollo del programa fue inspirado por esta situación, aunque seguramente podrá resolver otras muchas y muy variadas. Para mi explicación, me basaré en las situaciones que más comúnmente veríamos en una escuela.

Primero que nada, expondré brevemente lo que la Dirección espera de mí, el administrador de sistemas.

En todo momento, todos los laboratorios deben estar disponibles para el grupo que quiera utilizarlos. La salida a Internet debe ser tan rápida como sea posible. Un maestro debe tener la posibilidad de bloquear la salida a Internet a su grupo, ya sea a todos juntos (para concentrar la atención del grupo completo en lo que él está enseñando), o a un sólo alumno problemático - manteniendo, tal vez, la posibilidad de utilizar Internet desde su computadora para apoyarse en su enseñanza.

Además, es deseable que haya diferentes niveles de acceso: Tal vez sólo el administrador de la red deba poder desactivar todas las restricciones. Tal vez un maestro deba poder contolar únicamente una dirección específica en cada operación, y no todo un laboratorio. Tal vez sólo una persona deba tener la capacidad de agregar o remover usuarios. Y quién sabe qué otras tantas políticas sea importante que sigamos.

Como administrador o como director, me interesa ver rápidamente y de manera clara qué laboratorios o computadoras tienen acceso o restricciones de uso.

Y viendo un poco hacia el futuro, hacia las opciones que aún no han sido implementadas en el programa, tal vez el sistema deba saber por sí sólo a qué hora activar o desactivar una restricción en cierto rango de computadoras, facilitando la administración del sistema entero.

Todo esto debe realizarse, obviamente, por medio de una interfaz sencilla. Esto, por dos razones: Primero, no queremos que los maestros, no especializados en computación, sufran aprendiendo comandos con difícil sintaxis ni complicados procedimientos(y, por si fuera poco, no queremos darle la contraseña de root a todos ellos), y segundo, para presumir un poco a nuestros amigos de lo fácil que es administrar nuestro sistema :-)

Con estos requisitos en mente, me dí a la tarea de escribir este programa, con la clara idea de liberarlo bajo la licencia GPL para que pueda ser aprovechado por la mayor cantidad de usuarios posible. El saber que este código sería leído y utilizado por personas en todo el mundo me llevó a escribirlo completamente en inglés, para no limitar los usuarios beneficiados a únicamente aquellos que hablan español.

2 Cómo está implementado

Elegí Perl como el lenguaje sobre el cual escribir WPM, principalmente, por la facilidad que tiene para manejar la interacción con el usuario por Web, y por la libertad y facilidad de programación que brinda al no ser un lenguaje que obligue a declarar y tipificar variables ni cuidar el manejo de memoria. Cierto, el código en C es mucho más eficiente que el código en Perl, pero para el tamaño de programas que forman a WPM, creo que podemos prescindir de ésta velocidad sin mayor problema, y gozar de las ventajas tan grandes que nos da este lenguaje. El no tener que preocuparnos por ataques al stack, además, nos permitirá dormir más tranquilos.

WPM no maneja propiamente al proxy, sino que maneja un firewall en la computadora que contiene al proxy, evitando que esta escuche las peticiones de las computadoras que estén bloqueadas en determinado momento.

En este momento, WPM requiere Linux 2.2 para funcionar, ya que requiere interactuar con ipchains, aunque no debe ser difícil agregarle soporte para cualquier otra arquitectura.

WPM consta de dos partes principales a nivel estructural: Los CGIs y el demonio. Los CGIs se encargan de toda la interacción con el usuario, el despliegue del estado, la administración de usuarios y la interacción con el demonio, corriendo como usuario no privilegiado (usualmente, nobody). El demonio, por su lado, se encarga de ejecutar todos los comandos del firewall y de informar al CGI que lo invoca del estado actual.

Debe quedar claro que WPM todavía está considerado Beta. En este momento aún tiene varios defectos por corregir - el principal de ellos puede estar en el lado del demonio: No acepta aún más de una conexión simultánea. Normalmente, esto no debe representar ningún problema, pero (obviamente) tengo programado corregirlo tan pronto entienda bien como hacer un fork() con un socket que está siendo utilizado.

3 Cómo funciona

Llegamos ya a la parte divertida, con muestras de pantallas y demás cosas bonitas.

Debemos levantar el demonio antes de utilizar el programa, para lo cual, entrando como root al directorio de WPM y escribiendo:

wpmd -c wpmd.conf

Para entrar al programa, debemos utilizar un navegador y apuntarlo a la dirección deseada (en mi caso, http://localhost/wpm.html se me hizo un buen nombre). Nos recibe la pantalla 1(ver al final del artículo).

WPM trae una cuenta preconfigurada con la cual podemos entrar al sistema, dar de alta nuevas cuentas y, por supuesto, posteriormente deshabilitar esta cuenta, pues no queremos que nadie entre sin nuestra autorización. El login es wpm y la contraseña es (sorpresivamente) también wpm. Enviamos los datos y nos recibe la pantalla 2.

No detallaré demasiado respecto a la pantalla de cambio de contraseña (3), pues su funcionamiento es obvio.

El manejo de cuentas también es relativamente sencillo (pantalla 4). Podemos cambiar el nombre de cada una de las cuentas así como su nivel de acceso. Claro, si tuviéramos una cuenta menos privilegiada (con 0 como el nivel de mayor privilegio y 4 el de menor), no podríamos modificar ninguna cuenta con mayor privilegio, ni ascender a ninguna cuenta mas allá del nivel de la propia. Además, para borrar una cuenta es necesario tener nivel cero.

La parte medular del programa está en las pantallas 5 y 6. La pantalla 5 nos muestra cómo se vería nuestra red la primera vez que utilicemos el programa, con todos los segmientos en color verde, lo que nos indica que todos ellos están posibilitados para salir a Internet. La pantalla 6 nos los muestra después de algo de uso: El segmento 1 aparece en rojo, lo que nos indica que todas las computadoras que lo componen tienen negada la salida a Internet. El segmento 3 aparece en amarillo, lo que significa que algunas de sus computadoras tienen permiso de salir, mientras que otras no.

En esta última pantalla podemos realizar diferentes acciones: Oprimiendo los botones que aparecen al lado de cada segmento, podemos permitir o negar la salida al segmento completo. Podemos permitir o negar la salida a una dirección IP individual de nuestra red, y podemos levantar todas las restricciones y, mediante un solo click, permitir la salida a todas las computadoras.

4 Qué sigue

El programa ya puede ser utilizado, prueba de lo cual es que ya está siendo utilizado (por lo menos) en México, Singapur, Brasil y Australia. Sin embargo, aún faltan muchas cosas.

Por un lado, estoy trabajando para agregar una interfaz gráfica a la configuración del demonio (puerto, red, localización de los archivos de configuración, etc.) y de los segmentos de la red, que actualmente están en dos archivos de texto plano con formato relativamente sencillo de entender - pero si estoy haciendo una herramienta de configuración y mantenimiento por Web, lo menos que puedo hacer es permitir la configuración de la misma por Web.

Por otro lado, hay varias adiciones pendientes que darán mayor funcionalidad al programa. Las principales que se me han ocurrido son:

- Cambios automatizados por horario: Alguna manera de insertar o remover comandos del crontab para que las acciones que programemos puedan efectuarse automáticamente de modo diario, semanal o mensual (dudo que tenga alguna utilidad hacerlo de modo horario o anual, pero también sería posible).
- Diferenciación por puerto: Actualmente, tenemos una solución de todo o nada, que sirve para un proxy. Sin embargo, para poder realmente utilizar WPM para manejar un firewall, debe poder manejar diferentes puertos de entrada y salida para cada computadora. Por otro lado, al bloquear de la manera en que lo hace ahora, una computadora que esté bloqueada sólo puede ser liberada desde una estación que esté abierta. Sería deseable que sólo fuera bloqueado el puerto del proxy, para que desde cualquier computadora, bloqueada o no, el administrador pudiera entrar al programa.
- Soporte a diferentes configuraciones de red: En este momento, WPM sirve únicamente con redes clase C o menores (máscara de red de 24 bits, 255.255.255.0, o más). Eso normalmente no es un problema, ya que es poco común ver instalaciones con más de 254 nodos, pero ciertamente es una limitante. He pensado en un par de soluciones, pero ninguna me satisface por completo. Dentro del programa sugiero un “hack” para permitir clases B, pero no lo he probado.
- Lo que ustedes sugieran. Siendo este un proyecto 100% GPL, si bien yo inicié el desarrollo y escribí prácticamente todo el código, pueden estar seguros de que lo que me manden será incluído.

5 Contacto

Por si desean dar conmigo, ya sea por algo relacionado con el programa o no, pueden localizarme en la dirección `gwolf@campus.iztacala.unam.mx`. Espero que para cuando se lleve a cabo el congreso, la penosa huelga por la que atraviesa la Universidad Nacional Autónoma de México haya ya finalizado. De cualquier modo, en caso de que la dirección de correo falle, mi dirección temporal es `gwolf@chmd.edu.mx`.

La página Web del programa, en la que podrán encontrar la última versión de éste así como un poco más de explicación (como si todo el rollo que les aventé aquí no fuera suficiente) es `http://www.chmd.edu.mx/~gwolf/wpm`.

6 Pantallas

NOTA - Por consideraciones de espacio (LyX, el procesador de documentos con el que escribí este texto) requiere que las imágenes insertadas sean PostScript, y mi dominio de LaTeXno es tan amplio como yo quisiera, decidí enviar las pantallas por separado, en archivos con formato .JPG, que es aproximadamente 50 veces más compacto que el PostScript. Las pantallas las pueden encontrar como pantalla1.jpg - pantalla6.jpg

(si los organizadores del congreso deciden incluir las pantallas aquí... Adelante, ahí sí tendrían toda la razón. Tomen únicamente en cuenta que enviar 20MB desde México va en contra de la etiqueta de la red, por lo que mientras se pueda evitar...)