

PROXY. Buen Punto

Alonso E. Caballero Quezada
 Editor y Miembro de RareGazZ Security Team, Security Wari Projects e informatizate

En un mundo donde las comunicaciones basadas en dispositivos electrónicos; ya se han convertido en una forma de vida; las comunicaciones fiables y rápidas son una necesidad vital.

Nosotros que día a día convivimos con computadoras, servidores, redes, routers, switches y demás. Es una necesidad el establecer un buen punto de inicio para una buena estructura organizacional, una vez establecida criterios como la topología de la red, por ejemplo.

Lo que pretendo en el siguiente escrito es exponer de manera directa y concisa el concepto de web proxy, el mecanismo de su funcionamiento y implantación de este a nivel de un empresa. No se tocan tópicos como la instalación y configuración. Los HOWTO's o Paper's relativos a ese tema son muy completos, y sería reiterativo el plasmar eso en el presente texto.

INTRODUCCION

En el ámbito de la seguridad informática; por lógica; es mucho mas fiable la vigilancia de un solo punto de comunicación, que la vigilancia de varios puntos de acceso. Claro que se puede dar a todas las estaciones de trabajo de una empresa IP's públicos. Pero son tantos puntos de entrada a nuestra red como IP's públicos se hayan asignado. Claro que se puede controlar con un buen firewall en cada PC, pero se parte de la premisa de que es recomendable el controlar y vigilar un solo punto de comunicación.

El caso mas típico es la de una intranet empresarial con clientes o estaciones de trabajo a los que se les permite acceso a otra red o internet.

La siguiente figura visualiza de mejor manera esta idea. :)

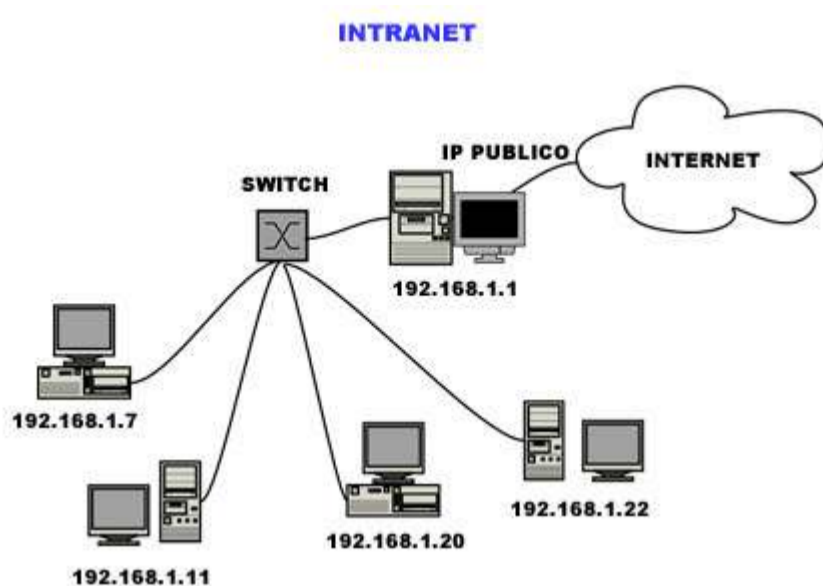


Figura 1

Si se desea dar acceso a internet; específicamente acceso Web; por premisa de seguridad. Los clientes de la intranet estarán asignados con IP's 'privados', llámese 192.168.1.0/24 u otro rango. Y solo será visible desde 'afuera' el IP publico asignado al proxy. Y las PC's de los usuarios se conectaran directamente a nuestro IP que actúa como gateway, si le hemos asignado la subred anterior, puede ser el IP, 192.168.1.1.

Pero mas allá de que los IP se estén 'acabando' o que IPv6 venga a solucionar el inconveniente con un mayor rango de IP, mayor seguridad, así como otras características; como mencione anteriormente, es preferible vigilar un solo punto de acceso.

Intuyo hasta este punto que ya se ha implementado un firewall o se hace a la par con la implantación del proxy. Lo que se detallara a continuación, esta basado en GNU/Linux y Software Libre.

Se asume que ya se ha hecho un 'enmascaramiento', y se hace uso de IP Tables. Es decir que los clientes con IP's privadas pueden hacer peticiones web al server e internet, y por ende las 'respuestas' ser redireccionadas a los clientes que originalmente hicieron la petición correspondiente. Ya que las peticiones que se realicen con "dichos" IP's no será enrutadas adecuadamente.

PROXY

Es aquí donde se tangibiliza el concepto de un servidor web Proxy. En el mundo Linux, esto se hace con el popular SQUID. Las siguientes características se coligan de la introducción anterior, y engloban el concepto de un proxy.

- Proporciona una capa extra de seguridad.
- Aísla a los usuarios de la intranet.
- Un Proxy actúa como un 'cache', es decir un almacenamiento dinámico de información con mayor acceso.
- Se realiza una vigilancia, control y acceso transparente para el usuario.

Entre las características para un administrador, puedo citar las siguientes:

- Podemos hacer usos de las características inherentes al SQUID para definir listas de control de acceso, tanto para usuarios, como para url's.
- Permite el control de acceso a diferentes sitios web. Podemos utilizar para este propósito al software GUARDIAN. (*)
- Permite reportes detallados del uso de internet, usuarios, ancho de banda, horas de acceso, etc. Se puede utilizar para este propósito a SQUINT o SARG.

[+] El concepto es simple, como lo muestra la siguiente imagen. Si la petición ya ha sido realizada por otro cliente y este se conserva en 'cache'; dicha petición NO saldrá a internet; con el consiguiente ahorro de ancho de banda y rápido acceso, ya que la información se obtendrá del 'cache' del servidor (PETICION1 + RESPUESTA2). Y consecuentemente si la petición es 'nueva', esta petición, si saldrá a la internet u otra red. (PETICION1+PETICION2+RESPUESTA2+RESPUESTA2)

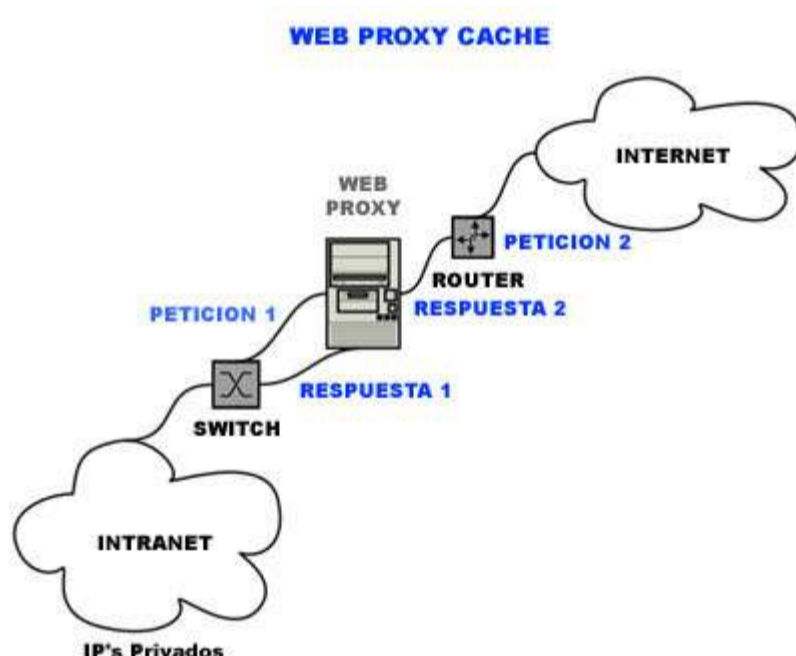


Figura 2

DETALLES

Los tres puntos antes mencionados (e, f, g) son de suma importancia para el encargado de administrar el servidor proxy, ya que el control y vigilancia de lo que los clientes hacen en internet no es cosa de Juego. Claro que esto debe estar bien definido en un reglamento interno de la empresa; de esta manera; si se presentarse algún inconveniente con el acceso a determinado contenido y la posterior acción por parte de la empresa, el usuario no podrá alegar el no conocimiento de los estatutos.

(+) Dada la naturaleza dinámica de internet, el controlar sitios por ciertos criterios como contenidos, se hace complicado. Un ejemplo simple es la censura de la palabra SEXO, ya que de encontrar esta palabra en la sitio web el software filtraría ese contenido; cuando en un simple formulario se puede encontrar esa palabra y que no tenga nada que ver con sitios para adultos.

La solución a esto es; como en el control de SPAM; NO solamente usar un criterio para filtrar contenido, sino la utilización de otros criterios. Es por ello que algunos Programas utilizan Bases de Datos que almacenan estos criterios de filtrados. Pero como dije, dada la naturaleza dinámica de internet, se puede minimizar pero no controlar en absoluto.

Una vez definidas las políticas de acceso a internet en la empresa, y con pleno conocimiento por parte de los usuarios de ella, el administrador será simplemente un vigilante del buen uso, mas no un controlador de contenido. Pero eso es en un caso ideal, ya que siempre por lo menos una vez se accesa a contenido denominado no 'permitido'.

Cabe acotar que en los dos puntos citados anteriormente, se hace uso de Software desarrollo externamente, no esta dentro de SQUID. Estos programas se basan en los logs del squid y analizando las peticiones realizadas al servidor.

IMPLANTACION DE SQUID

Dada la naturaleza de un servidor Web proxy; es decir, aquí se concentraran todas las peticiones web realizadas por las estaciones de trabajo; se debe de tener en consideración los siguientes criterios, respecto al Hardware:

- Tiempo de Búsqueda aleatoria del Dispositivo de almacenamiento.
- Cantidad de memoria del sistema.
- Poder de CPU.

El tiempo de búsqueda del HD, no solo se refiere al ello mismo, sino al hecho de la performance del sistema y de la capacidad de 'cache' del servidor. Todo esto dependerá de la cantidad de usuarios de la empresa, de la cantidad de peticiones que se realicen por hora o día, entre otros detalles.

Un ejemplo simple para clarificar la idea es el siguiente:

Supongamos que la transmisión máxima de download que nos proporcionada nuestro proveedor de acceso a internet es de 25 KB / seg al multiplicar esto por 3600 segundos (1 Horas), nos da un aproximado de 98.8 Megas / Hora. Y esto multiplicado por 24 Horas al día, nos da un aproximado de 2.1 Gigas por día. Esto, obviamente en el caso 'tope' y de un acceso continuo y constante de nuestro ancho de banda. Es decir que debemos tener un mínimo de almacenamiento para cache en disco de aproximadamente 2.1 Gigas.

Otro punto a tomar en consideración es la memoria del sistema, SQUID mantiene un índice de objetos en memoria y obviamente es mucho mas rápido el acceder a memoria RAM que a SWAP.

Sigamos con el ejemplo anterior; si cada objeto en disco ocupa 75 bytes y el promedio de los objetos en internet es de 13Kb, con 2.1 Gigas, almacenaremos alrededor de 150000 objetos. A 75 bytes de RAM por objeto, necesitamos aproximadamente 11 megas solamente para el índice de objetos de SQUID.

Respecto al poder de CPU, SQUID no es muy exigente en este aspecto. Mas Memoria y más Discos ayudan mucho más.

INSTALACION Y CONFIGURACION

No es el propósito; como lo mencione al principio del presente escrito; el explicar estos 2 acápite al detalle. Lo que si deseo comentar es que la opción de hacerlo por paquetes proporcionados por las diferentes distribuciones o por fuentes, depende mucho de la manera de trabajar del administrador del sistema.

Distribuciones como RedHat por ejemplo; proporcionan un relativamente; buen promedio de respuesta ante la detección de algún problema en los paquetes RPM.

El uso de fuentes permite un mayor control en la instalación y configuración de SQUID, recomendado para aquellos que nos gusta curiosear, o examinar el comportamiento del proxy ante ciertos eventos.

NOTAS FINALES

El Uso de un Proxy mas a favor de la seguridad de la intranet; dadas las características antes mencionadas; sino también en un punto a favor de la seguridad de la empresa.

Dadas las muchas características de configuración de SQUID y el hecho de ser Software Libre; hacen de SQUID un software de muy buen desarrollo, soporte y calidad.

Todo esto dicho, sin ningún apasionamiento. :)

BIBLIOGRAFIA

- Squid Web Proxy Cache / SQUID A User's Guide / <http://www.squid-cache.org>
- SecurityFocus / <http://www.securityfocus.com>
- DansGuardian / <http://dansguardian.org>
- SARG / <http://web.onda.com.br/orso/>
- SQUINT / <http://ledge.co.za/software/squint/>
- HOWTO Masquerading
- Mi experiencia.