MEGATUTORIAL Squid 5. Primera Parte.

Descripción

Este será el primer Megatutorial del sitio, debido a su gran extensión de contenido. Se intentará abarcar de una forma muy profunda y nunca antes vista en ningún sitio de Internet, la implementación y configuración de squid como proxy. **SQUID** tiene al menos **249** parámetros configurables. Su fichero de configuración altamente comentado, que normalmente está en **/etc/squid/squid.conf**, contiene más de **4,600** líneas de largo. Esto intimida incluso al más experimentado administrador de sistemas. Por lo que nos dimos **(@Franco sparrow_snet y un servidor)** a la tarea de hacer un tutorial lo más abarcador posible para llegar a entender a **SQUID.** Este sin duda será unos de los tutoriales más controversiales que escribiré y sin duda el más difícil. Como es lógico no todos poseemos las mismas características, ni la misma estructura en nuestras redes. Por lo que escribir un tutorial de configuración de squid es una tarea titánica y casi imposible. Con este **MEGATUTORIAL**, pretendo abarcar la mayoría de los aspectos básicos y de situaciones reales que pueden presentarse en una empresa cubana común. Se que hay otras instituciones que manejan un mayor volumen de usuarios y por ende deben tener una mayor protección. Pero básicamente tratare de explicarles, no a nivel **HOKAGE** sino de **CHUNNIN** (broma **OTAKU**) lo básico a tener en cuenta para lograr un squid totalmente funcional. Este tutorial se ira enriqueciendo a medida que ustedes opinen y posteen sus dudas. En el mismo pondré un caso hipotético de una empresa y tratare que sea lo más abarcador posible. Si hay condiciones que ustedes quieran agregar al caso que planteare, con gusto lo actualizare y le daré la explicación de cómo resolverlo.

A continuación les dejo el índice del Megatutorial. El mismo puede sufrir cambios y estará disponible en cada una de las partes.

ÍNDICE

Servidor Proxy Conceptos.

Que es SQUID y para que sirve?

Squid es una aplicacion de software libre bajo licencia **GLP**, disenado para ejecutarse en entornos tipo **UNIX**. Squid escucha las peticiones que hacen los usuarios de los objetos de Internet, se los entrega y se guarda una copia. A esa copia se le denomina cache. Por lo tanto, Squid es un proxy-cache para clientes Web que soporta FTP, gopher y HTTP. También puede ser configurado para otros tipos de proxy, como proxy inverso y transparente.

Algunas características:

- Almacena en RAM los metadatos y los objetos muy consultados.
- Guarda en cache las consultas DNS.

- Soporta consultas de DNS no bloqueantes.
- Soporta SSL.
- Desencriptación de HTTPS.
- Control de ancho de banda.
- Políticas de control de acceso.
- Permite reescrituras de consultas.
- Permite integración con dominios de Active Directory de Microsoft y Samba 4.

Entre muchas otras opciones.

Proxy y cache

El servicio que permite a los usuarios realizar indirectamente conexiones a Internet es conocido como servidor Proxy.

Un servidor Proxy se sitúa entre la estación cliente (el usuario) y el acceso a Internet (ADSL, cable, Frame Relay…). El cliente se conecta al servidor Proxy, solicita un recurso de Internet (una conexión, un fichero o cualquier otro recurso) y es el servidor Proxy el encargado de solicitar ese recurso a Internet para proporcionárselo al cliente. La traducción de la palabra inglesa “Proxy” viene a ser “por poderes”, es decir dejaremos que sea el servidor Proxy el que se conecte a Internet por nosotros.

En algunos casos es posible que el Proxy no se conecte a Internet para obtener el recurso solicitado, sino que lo obtenga de una cache. El término cache es utilizado en el ámbito informático para designar un conjunto de datos replicando a los originales, residentes en un almacenamiento remoto: Cuando se accede por primera vez a un dato, se hace una copia en el caché, los accesos siguientes se realizan a dicha copia, haciendo que el tiempo de acceso aparente al dato sea menor.

Web Proxy cache

Se dice que un servidor está actuando como Web Proxy cache cuando almacena en su disco duro las páginas Web descargadas de forma que, en próximas consultas, pueda acceder a ellas de forma muy rápida. De esta forma estamos optimizando el canal de acceso a Internet de la organización y mejoramos la sensación de navegación del usuario en momentos de ocupación importante de la línea.

Este tipo de Proxy se suele usar en alguno de estos entornos:

1. Cuando, por motivos de seguridad, no deseas permitir acceso libre a Internet a los usuarios, pero se desea proporcionarles acceso a la Web: se les proporciona a través del Proxy.

2. Cuando se desea optimizar el ancho de banda y acelerar la navegación para los usuarios. Por ejemplo, una oficina con muchos trabajadores que suelen visitar frecuentemente las mismas páginas.

Proxy inverso

Un Proxy inverso (o reverse proxy) es aquel que se sitúa cerca de uno o más servidores Web, de forma que es el Proxy quien recibe las peticiones y las reenvía a los servidores Web. Este tipo de Proxy se suele usar en algunos de estos entornos:

1. Para añadir seguridad a los servidores Web: en ningún momento se accede directamente a ellos sino al Proxy.

2. Para balancear la carga de los servidores: el servidor Proxy es el encargado de enviar las peticiones a aquellos servidores que estén más descargados.

3. Para descargar a los servidores Web de contenido estático como imágenes o documentos.

4. En caso de sitios Web seguros se puede dejar al Proxy que haga el encriptado de los datos y descargar así a los servidores Web.

Proxy transparente

Tal como hemos visto es posible usar un proxy para aplicar políticas de control de acceso a Internet. Normalmente esa configuración no es transparente: es necesario modificar el cliente para que use el Proxy al acceder a Internet, de forma que es posible que un usuario modifique esa configuración.

Una configuración de Proxy transparente hace que no sea necesaria modificación alguna en las máquinas clientes, eliminando el riesgo de que un usuario modifique dicha configuración a su antojo. El uso de un Proxy transparente combina un servidor Proxy con NAT, de forma que todas las conexiones son encaminadas a través del Proxy sin la intervención de la máquina cliente.

Datos para el ejemplo a desarrollar.

Los siguientes datos exponen las versiones de los paquetes y Sistemas Operativos en los que fueron probadas las configuraciones del presente tutorial.

Servidor Proxy:

- Os: Debian 10 (Buster)
- Versión de Squid: 5.0.2

ADDC (todos los probado en este tutorial):

- Debian 9 con Samba 4.10.6
- Windows Server 2008 R2
- Windows Server 2016

Ejemplo Practico:

En una empresa la cual se encuentra tras un proxy padre, con dominio dado se nos pidió implementar un proxy con las siguientes particularidades.

Condiciones:

- Existirá un grupo de usuarios con posibilidades de navegación en la red cubana **(.cu)**.
- Tendremos otro grupo que ademas de navegación nacional tendrá derecho de acceso a determinadas web’s de Internet, autorizadas por el director de la empresa. Navegación Nacional privilegiada.
- Un grupo con **TOTAL** acceso a Internet.
- Otro grupo con acceso limitado a Internet.
- Creación de una cache local para el acceso mas rápido.
- Condicionar y configurar un sistema de trazas y monitoreo en tiempo real.

Como seguridad tendremos:

- La navegación sera por horarios.
- La autentificación será obligatoria tanto para navegar nacional como en Internet.
- Solo se permitirá el acceso desde la red local.
- Se filtraran todos los puertos dejando solo los necesarios abiertos.
- Los usuarios con derecho a navegación de Internet estarán anclados por MAC e IP.
- Se priorizaran las conexiones de los servidores sobre las de navegación.
- Se filtrara el contenido por categorías.

Hasta aquí la introducción al Megatutorial en las próximas partes se explicaran cada uno de los capítulos del índice.

Categoría

1. Como se hace
2. Proxy
3. Software Libre

Fecha de creación
junio 2020
Autor
alexminator