

Redireccionar a otro servidor utilizando una sola IP con mod_proxy

Integrantes:

Guido Clavijo

Juan José Benitez

Oscar Wallingre

Julio Wallingre

Copyright (c) 2009, Guido Clavijo, Juan José Benitez, Oscar Wallingre, Julio Wallingre

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Contenido

1 Introducción

1.1 Un caso real

1.2 Posible solución del problema

2 El Proxy

2.1 Funcionamiento

2.2 Instalación

3 Configuración

3.1 Archivos de configuración de Mod_proxy

3.2 Archivos de configuración de Apache 2

3.3 Otras directivas importantes

4 Conclusiones

4.1 Ventajas

4.2 Desventajas

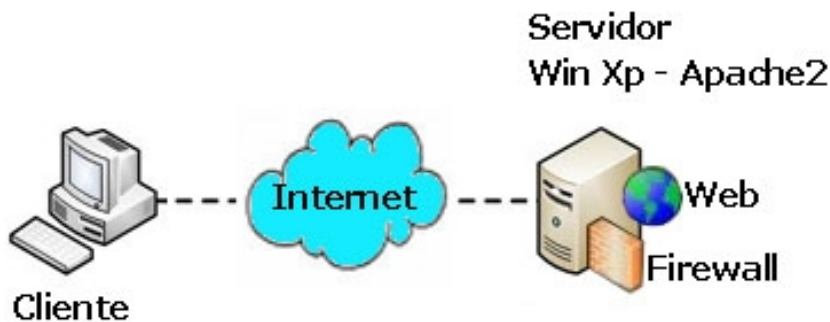
4.3 Experiencias.

1. Introducción:

1.1 Un caso real

Se desea migrar un servidor con Windows XP y Apache2 el cual tiene todo los sitios instalados y funcionando con PHP 4.2 y MySQL 4.1 a uno Linux Debian 5, con Apache2, PHP5 y MySQL5.

Configuración actual:

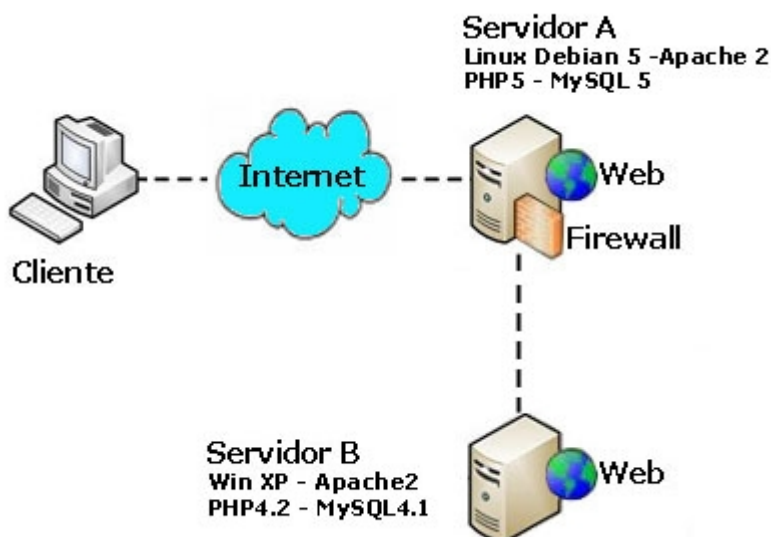


1.2 Posible solución del problema

Para que la transición sea lo menos problemática posible, se decidió instalar un segundo servidor el cual este escuchando a Internet con LINUX Debian 5, Apache2, PHP5 y MySQL5 instalado. Este servidor va a ser el encargado de redireccionar los sitios web que el cliente peticiona desde Internet, al segundo servidor si este mismo no los posee. De esta manera se podrá ir migrando los sitios uno a uno hasta poder descartar el servidor con WinXP.

Las restricciones son: Solo se dispone de una IP y por problemas de seguridad se quiere dar salida únicamente al puerto 80.

Configuración a actualizar:



2 El Proxy

2.1 Funcionamiento:

Que es y para que sirve?

Un proxy es un programa o dispositivo que realiza una tarea de acceso a Internet en lugar de otra computadora. Un proxy es un punto intermedio entre una computadora conectada a Internet y el servidor que está accediendo. Cuando navegamos a través de un proxy, nosotros en realidad no estamos accediendo directamente al servidor, sino que realizamos una solicitud sobre el proxy y es éste quien se conecta con el servidor que queremos acceder y nos devuelve el resultado de la solicitud.

Cuando nos conectamos con un proxy, el servidor al que accedemos en realidad recibe la solicitud del proxy, en vez de recibirla directamente desde nuestra computadora. Puede haber sistemas proxy que interceptan diversos servicios de Internet. Lo más habitual es el proxy web, que sirve para interceptar las conexiones con la web y puede ser útil para incrementar la seguridad, rapidez de navegación o anonimato. Este suele tener lo que denominamos una caché, con una copia de las páginas web que se van visitando. Entonces, si varias personas que acceden a Internet a través del mismo proxy acceden al primer sitio web, el proxy la primera vez accede físicamente al servidor destino, solicita la página y la guarda en la caché, además de enviarla al usuario que la ha solicitado. En sucesivos accesos a la misma información por distintos usuarios, el proxy sólo comprueba si la página solicitada se encuentra en la caché y no ha sido modificada desde la última solicitud. En ese caso, en lugar de solicitar de nuevo la página al servidor, envía al usuario la copia que tiene en la caché. Esto mejora el rendimiento o velocidad de la conexión a Internet de los equipos que están detrás del proxy.

Proxy Inverso

Un **Proxy inverso** es un servidor que funciona de afuera hacia dentro de nuestra red LAN. Todo el tráfico entrante de Internet y con el destino de alguna computadora de nuestra LAN pasa a través del servidor proxy. Hay varias razones para instalar un "reverse proxy":

- Seguridad: el servidor proxy es una capa adicional de defensa y por lo tanto protege los servidores web.
- Cifrado / Aceleración SSL: cuando se crea un sitio web seguro, habitualmente el cifrado SSL no lo hace el mismo servidor web, sino que es realizado por el "reverse proxy", el cual está equipado con un hardware de aceleración SSL (Security Sockets Layer).
- **Distribución de Carga: el "reverse proxy" puede distribuir la carga entre varios servidores web. En ese caso, el "reverse proxy" puede necesitar reescribir las URL de cada página web (traducción de la URL externa a la URL interna correspondiente, según en qué servidor se encuentre la información solicitada).**
- Caché de contenido estático: Un "reverse proxy" puede descargar los servidores web almacenando contenido estático como imágenes u otro contenido gráfico.

fuelle wikipedia

2.2 Como se instala?

Mod_proxy :

Para esta tarea utilizaremos un módulo para Apache que actuará como enlace entre Servidor A en Linux y Servidor B en WinXP, llamado **Mod_Proxy**.

Primero desde Apache 2 se ha de habilitar el modulo de proxy, en Debian por ejemplo seria:

```
a2enmod proxy proxy_http
```

Una vez activado el modulo Proxy con el comando **a2enmod Proxy Proxy_http**, Linux Debian crea un enlace simbólico desde la carpeta mods-enabled a la carpeta mods-available donde se encuentran los archivos **Proxy.conf** , **Proxy.load** y **Proxy_http.load**.

Ya solo falta reiniciar el Apache y disfrutar de la nueva configuración con el siguiente comando:

```
Invoke-rc.d apache2 restart
```

3 Configuración:

Apache puede ser configurado para trabajar tanto en modo *Forward Proxy* o *Reverse Proxy*.

Ejemplos:

Forward Proxy

```
ProxyRequests On  
ProxyVia On
```

```
<Proxy *>  
Order deny,allow  
Deny from all  
Allow from internal.example.com  
</Proxy>
```

Reverse Proxy

```
ProxyRequests Off
```

```
<Proxy *>  
Order deny,allow  
Allow from all  
</Proxy>
```

```
ProxyPass /foo http://foo.example.com/bar  
ProxyPassReverse /foo http://foo.example.com/bar
```

3.1. Configuración del archivo proxy.conf :

Una vez activado el modulo Proxy es hora de configurar el archivo por defecto **Proxy.conf**.

```
<IfModule mod_proxy.c>
    #turning ProxyRequests on and allowing proxying from all may allow
    #spammers to use your proxy to send email.

    ProxyRequests Off

    <Proxy *>
        AddDefaultCharset off
        Order deny,allow
        Deny from all
        #Allow from .example.com
    </Proxy>

    # Enable/disable the handling of HTTP/1.1 "Via:" headers.
    # ("Full" adds the server version; "Block" removes all outgoing Via:
headers)
    # Set to one of: Off | On | Full | Block

    ProxyVia On
</IfModule>
```

Veamos un poco las directivas usadas para esta configuración:

ProxyRequests: No ajuste "**ProxyRequests On**". El ajuste ProxyRequests convierte a su servidor proxy en abierto. Hay robots de exploración de la web de proxies abiertos. Cuando encuentran un Proxy abierto podrían ser capaces de enviar correo spam a través de su proxy. Su legítimo tráfico será inundado, y encontrará su servidor bloqueado.

AddDefaultCharset: Esta directiva especifica un valor por defecto para el parámetro del conjunto de caracteres que se añade añade si solo si el tipo de contenido de una respuesta es text/plain o text/html. EL valor pecificado en esta directiva no prevalecerá si cualquier otro conjunto de caracteres es especificado en el cuerpo del documento por medio de una etiqueta META, aunque a menudo, el comportamiento exacto está determinado por la configuración del cliente. Si se especifica AddDefaultCharset Off, se desactiva esta funcionalidad. AddDefaultCharset On activa el uso del conjunto de caracteres por defecto interno de Apache, iso-8859-1. Cualquier otro valor se asume que es el charset a usar, que será uno los [registrados por la IANA](#) como tipos MIME. Por ejemplo:

```
AddDefaultCharset utf-8
```

AddDefaultCharset debe ser usada solo cuando todos los recursos de texto a los que se aplican se saben que usan un determiando conjunto de caracteres (character encoding) y no es conveniente etiquetar los documentos individualmente. Un ejemplo es su uso en recursos que contienen contenido generado, como CGIs antiguos, que puede ser vulnerables a ataques debidos a que se incluye en el resultado datos suministrados por el usuario. Tenga en cuenta, sin embargo, que una mejor solución es simplemente modificar (o borrar) esos scripts, porque especificar un conjunto de caracteres por defecto no protege a los usuarios que tengan activada en su navegador la opción "auto-detect character encoding".

Order :La directiva Order directive controla el orden en que se evalúan las directivas Allow y Deny:

Order Deny,Allow

Primero se evalúa Deny. Se permite acceso a cualquier host que primero no esté indicado en Deny o que sí lo esté en Allow. **El acceso se garantiza por defecto.**

Order Allow,Deny

Primero se evalúa Allow. Se deniega acceso a cualquier host que primero no esté indicado en Allow o que sí lo esté en Deny. **El acceso se deniega por defecto.**

Los valores se separan por comas y sin espacios.

En el siguiente ejemplo, todos los hosts del dominio misitio.org tienen acceso pero ningún otro.

Order Deny,Allow

Deny from all

Allow from misitio.org

En el siguiente ejemplo todos los hosts del dominio misitio.org tienen acceso salvo los host que estén en el subdominio piratillas.ies-bezmiliana.org. El resto de hosts que no están en el dominio ies-bezmiliana.org tampoco tendrían acceso.

Order Allow,Deny

Allow from misitio.org

Deny from piratas.misitio.org

Por otro lado, si cambiamos Order en el anterior ejemplo y lo ponemos como Deny,Allow, todos los hosts tendrían acceso. Esto sucede porque Allow se evalúa en segundo lugar y permitiría acceso a piratas.misitio.org y el acceso por defecto es aceptar.

La presencia de una directiva Order puede afectar al acceso a una parte del servidor incluso en ausencia de directivas Allow y Deny por los efectos de los valores predeterminados. Por ejemplo:

```
<Directory /www>  
  Order Allow,Deny  
</Directory>
```

denegaría todo el acceso al directorio /www ya que el estado por defecto sería Deny.

ProxyVia: Activa/desactiva el manejo de los encabezados HTTP/1.1 "Via:"

ProxyPass: La directiva de configuración fundamentales para establecer un proxy inverso es ProxyPass. Lo utilizamos para poder establecer normas para cada uno de los servidores de aplicaciones.

3.2. En la configuración del virtualhost de apache:

```
NameVirtualHost *  
  
<VirtualHost *>
```

```
ServerAdmin webmaster@correo.mio
ServerName elproxiado.midominio.com
ProxyPass / http://10.0.0.2/
ProxyPassReverse / http://10.0.0.2/
ErrorLog logs/elproxiado-error_log
CustomLog logs/elproxiado-access_log common
</VirtualHost>
```

Aqui asumimos que la ip interna del otro servidor es 10.0.0.2 .

Notese que en ProxyPass lo primero que aparece es una diagonal "/" esto es porque podemos decirle a Apache que a partir de cual directorio queremos nosotros que inserte el otro sitio web.

Por Ej: Digamos que el server es http://misitio.com.ar y quiero meter dentro de mi sitio a todo el sitio de misitio2.

Simple:

```
<VirtualHost *>
  ServerAdmin misitio2@ciudad.com.ar
  ServerName misitio.com.ar
  ProxyPass /misitio2 http://www.misitio.com.ar
  ProxyPassReverse /misitio2 http://www.misitio.com.ar
</VirtualHost>
```

Asi, si alguien accede http://misitio.com.ar/misitio2 estará en realidad accediendo el sitio web de misitio2. Igualmente podemos insertar un subdominio de otro sitio, y asi podemos tener las referencias "en vivo" dentro de mi site.

3.3 Otras directivas importantes

ProxyMaxForwards

La directiva ProxyMaxForwards especifica el número máximo de solicitudes que pueden pasar a través del proxy, si no hay cabecera Max-Forwards suministrado con la solicitud. Esto puede ser configurado para evitar bucles infinitos proxy, o un ataque DOS.

Ejemplo: **ProxyMaxForwards 15**

ProxyBlock

La directiva ProxyBlock especifica una lista de palabras hosts o dominios, separados por espacios. HTTP, HTTPS y FTP documento pide a los sitios cuyos nombres contengan las palabras combinadas, los hosts o dominios quedan bloqueados por el servidor proxy.

Ejemplo: **ProxyBlock joes-garage.com some-host.co.uk rocky.wotsamattau.edu**

BalancerMember Directive

Esta directiva añade un miembro a un grupo de balanceo de carga. Se podría utilizar dentro de un contenedor <Proxy balancer://...> y puede tomar cualquiera de los pares de valor clave a disposición de la directiva ProxyPass.

NoProxy Directive

Esta directiva sólo es útil para los servidores proxy de Apache en las intranets. La directiva especifica NoProxy una lista de subredes, direcciones IP, hosts y / o dominios, separados por espacios. Una petición a un host que coincide con uno o más de estos se sirve siempre directamente, sin reenvío a la configuración del servidor proxy ProxyRemote (s).

Ejemplo:

```
ProxyRemote * http://firewall.example.com:81  
NoProxy .example.com 192.168.112.0/21
```

4. Conclusiones y Experiencias

Tiene desventajas? Claro. Si hago proxy inverso de un servidor externo al servidor donde corro el proxy inverso, estaré consumiendo mi ancho de banda para bajar lo que el usuario pida, y luego lo volveré a consumir entregandole al usuario lo que pidió. Por eso no es recomendable hacer Proxy inverso de servidores ajenos a mi.

Esta tecnología está bién para el caso de tener todo un grupo de servidores web enmascarados por una sola ip externa, por ejemplo. o hacer proxy inverso de algún servidor interno que responde a velocidad de LAN (típicamente 100 megabits).

Es extremadamente útil cuando tienes un servidor apache y llega un servidor IIS y tu no quieres perder tu página en apache, y pues solamente "haces proxy" al servidor IIS mediante un subdominio o un directorio de tu site.

Para poder probar el mod_proxy se configuro un servidor con las características descritas ya que no se podian hacer las pruebas en el servidor que está on line.

La primera prueba no funciono, después de varios intentos nos dimos cuenta que el Firewall de Windows XP estaba activado y no permitía ingresar por el puerto 80, por tal motivo se configuro de la siguiente manera:

