English • Deutsch • Español • Français • Italiano • ??? • Polski • Português • ??????? • Svenska • ???(????)? • ???(??)? •

Running a transparent proxy server on your network can be used for more advanced content filtering of web pages for environments such as a school or library (where in some locales, filtering is required by law) or as a way to protect children in the household.

This guide will help you enable a transparent proxy server on your network by having your WRT54G router forward all traffic to the proxy server automatically.

Contents

Desktop Setup

Squid versions older than 2.6

First install Squid on your Unix box. After that you have to set up Squid to do transparent proxying with these settings:

httpd_accel_host virtual

httpd_accel_port 80

httpd_accel_with_proxy on

httpd_accel_uses_host_header on

Squid versions 2.6 or newer

With Squid installed on your Unix/Linux box, set the following:

http_port 192.168.1.10:3128 transparent

substituting the IP address you're listening on, and the port you wish to use in the example, making sure they match the variables at the top of the router setup script below.

Important for Debian users!

The Squid3 (squid3_3.0.PRE5-5) package from Debian Etch isn't working with this kind of transparent proxy. Try using Squid3 from Debian Lenny or downgrade to Squid-2.6 in Etch.

Router Setup

You will need to use iptables to tell your router how to forward traffic. If you don't have a good grasp on iptables yet, someone has already done the work and written a shell script to do the work for you. Be sure to edit the variables at the top.

These script need to be saved to your firewall script. In the WEB UI navigate to Administration -> Commands and paste your edited script in the input box, then press the Save Firewall button.

Proxy Server on the LAN Subnet

This script can be found at: http://www.dd-wrt.com/phpBB2/viewtopic.php?t=62222

```
#!/bin/sh
PROXY_IP=192.168.1.10
PROXY_PORT=3128
LAN_IP=`nvram get lan_ipaddr`
LAN_NET=$LAN_IP/`nvram get lan_netmask`

iptables -t nat -A PREROUTING -i br0 -s $LAN_NET -d $LAN_NET -p tcp --dport 80 -j ACCEPT
 iptables -t nat -A PREROUTING -i br0 ! -s $PROXY_IP -p tcp --dport 80 -j DNAT --to $PROXY_IP:$PR
iptables -t nat -I POSTROUTING -o br0 -s $LAN_NET -d $PROXY_IP -p tcp -j SNAT --to $LAN_IP
iptables -I FORWARD -i br0 -o br0 -s $LAN_NET -d $PROXY_IP -p tcp --dport $PROXY_PORT -j ACCEPT
```

Change the PROXY_IP and PROXY_PORT variables to match your proxy server's IP address and TCP port.

If you need to allow a host to bypass the transparent proxy (such as a game system, or media receiver), then add this command which allows a specific IP to bypass the proxy. You can use it to add as many exceptions as you like. DirecTV receivers which have Video On Demand need to bypass the proxy.

```
iptables -t nat -I PREROUTING -i br0 -s [IPADDRESS] -j ACCEPT
```

Proxy Server on the LAN Subnet -- Alternative Solution

This solution described in the previous section redirects packets to the proxy server using Network Address Translation to modify the actual packets. The result is that packets arriving at the proxy have a source IP address of the router rather than the original client. As a result, it's not possible to see the IP address of the originating client in the proxy logs, nor is it possible to apply access rules in the proxy based on the originating client IP address.

The following alternative approach uses the mangle table to mark packets and route them to the proxy using a custom routes table, which only has one defaut route directly to the proxy box. This requires some additional

iptable configuration on your proxy server, but it also has the advantage of retaining the client IP address. This solution was adapated from information found at http://en.tldp.org/HOWTO/TransparentProxy-6.html.

```
#!/bin/sh
PROXY_IP=192.168.1.10

iptables -t mangle -A PREROUTING -p tcp --dport 80 -s $PROXY_IP -j ACCEPT
iptables -t mangle -A PREROUTING -p tcp --dport 80 -j MARK --set-mark 3
ip rule add fwmark 3 table 2
ip route add default via $PROXY_IP dev br0 table 2
```

Change the PROXY_IP variable to match your proxy server's IP address.

If you need to allow a host to bypass the transparent proxy (such as a game system, or media receiver), then add this command which allows a specific IP to bypass the proxy. You can use it to add as many exceptions as you like. DirecTV receivers which have Video On Demand need to bypass the proxy.

```
iptables -t mangle -A PREROUTING -p tcp --dport 80 -s [IPADDRESS] -j ACCEPT
```

The changes above will route packets to your the IP Address of your poxy server, but since the packets were unmodified, they will still arrive at the proxy on port 80. You will still need to redirect the packets to the correct proxy port as they arrive. Add the following rule to the iptable on your proxy machine (note, extra steps will be needed on your proxy box to make this change persistent, but they are not covered here).

```
iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 80 -j REDIRECT --to-port [PROXY_PORT]
```

Replace PROXY_PORT with the correct port for your proxy, which would be 3128 from the previous example.

Proxy Server on Different Network and Using Chillispot

Scripts above are used when the Proxy Server is on same network, who needs proxy transparent with dd-wrt Chillispot enabled in most case (mine too), the Proxy Server is on different Network. I have changed the script Option 1 above to this needs. Edit the bolded variables to match your configuration.

```
#!/bin/sh
CHILLI_IP=192.168.182.1
CHILLI_NET=$CHILLI_IP/24
PROXY_IP=192.168.1.10
PROXY_PORT=3128
LAN_NET=192.168.1.0/24

iptables -t nat -A PREROUTING -i tun0 -s $CHILLI_NET -d $LAN_NET -p tcp --dport 80 -j ACCEPT
iptables -t nat -A PREROUTING -i tun0 -s $CHILLI_NET -p tcp --dport 80 -j DNAT --to $PROXY_IP:$P
iptables -t nat -A POSTROUTING -o br0 -s $PROXY_IP -p tcp -d $CHILLI_NET -j SNAT --to $CHILLI_IP
iptables -I FORWARD -i tun0 -o br0 -s $CHILLI_NET -d $PROXY_IP -p tcp --dport $PROXY_PORT -j ACC
```

Reverse proxy

Squid can also be used as a "reverse proxy" or "web accelerator" if the computer(s) behind it are web servers running database-intensive applications such as wiki, blog or forum hosting.

For Squid 2.4 and earlier, this is referred to as "accelerate single host" mode; for version 2.6 the commands in squid.cfg look like:

```
# Squid normally listens to port 3128, remove this:
# http_port 3128
#
# Instead, change so that squid listens to port 80, substituting your external (WAN) static addre
http_port 999.999.999.999:80 vhost defaultsite=example.org
# Then have all the requests forwarded to your actual web server (LAN address, change to match yo
cache_peer 192.168.1.2 parent 80 0 no-query originserver
```

Squid obtains a speed improvement by storing copies of rendered web pages to the file system and serving the stored copies to users instead of having the actual web server repeatedly regenerate dynamic content. As such, it is suited primarily for use on devices with adequate hard disk storage and may not be suited to small servers with limited storage space.

As the "reverse proxy" Squid configuration is used by large wiki sites such as Wikipedia, MediaWiki.org and Wikipedia's meta wiki do offer some information on the use of Squid in this manner.