PROXY AND IPTABLES FUN - TRANSPARENT PROXYING AND USERNAMES

As anyone who has read any of my previous articles knows, I like the *iptables* Linux firewall. A nice complementing server to this is the squid proxy server. In this article I am going to go through two things which make a network administrators life easier. Setting up transparent proxying, and setting up the proxy so that usage of it requires authorization.

Transparent Proxying
What this means is that you do not need to make any changes to any clients on your network, you do not have to worry about how your users are accessing the Internet, because all web traffic will be diverted to the proxy no matter what. To start with you will of course need an iptables firewall and a squid proxy server. I am assuming that these two machines will be two separate physical machines (I also recommend that the proxy server sits inside the internal LAN). To start with we setup the iptables firewall with the following rules..

```
##SETUP THESE VARIABLES##
PROXY=<the ip address of your proxy machine>
SOURCE=<your internal network addresses>
FWINT=<the ip address of your firewall's internal interface>
####
$IPT -t nat -A PREROUTING -s $PROXY -p tcp -m tcp --dport 80 -j ACCEPT
$IPT -t nat -A PREROUTING -s $SOURCE -p tcp --dport 80 -j DNAT --to-dest $PROXY:3128
$IPT -A FORWARD -s $SOURCE -d $PROXY -p tcp -m tcp --dport 3128 -j ACCEPT
$IPT -t nat -A POSTROUTING -s $SOURCE -d $PROXY -j SNAT --to-source $FWINT
```

What this does is..
- the first line allows all web access from the proxy
- the second line reroutes any external web traffic to the proxy and the proxy port
- the third line allows the rerouted traffic through
- the fourth line changes the source of the rerouted traffic to the firewall so that any responses can find their way back

Now all web traffic (port 80) will be rerouted through the proxy. Nifty. But we still need to make some changes to the squid server configuration before it works perfectly. Edit your *squid.conf* (by default in */etc/squid/squid.conf*) and make sure the following is set..

```
http_port 3128
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
http_access allow all
```

Now after a restart to ensure that your proxy is using the changed configuration file, all will be fine. Now would be the time when you setup *squidGuard* to further protect your network and bandwidth (see here). One thing you will notice when looking at the *access.log* file for squid, is that you will only ever see one IP address accessing the proxy, this is a result of the forwarding rules, and where the next tip comes into play for reporting on individual usage.

Proxy Usernames
One handly thing you can do with the squid proxy is set it up to require a username and password whenever someone wants to use it, you combine this with the above method of forcing everyone to use the proxy and you have a nice way of monitoring usage and stopping unwanted access. We will be setting up a very basic username and password system, there are more complicated setups, but this works fine as a proof of concept and for smaller companies.

First off, you will need to go to where you unextracted the squid source code, and proceed with the following steps

```
/<wherever_squid_source_is>/helpers/basic_auth/NCSA
```

```
make
make install
```

This will create the following executable, *ncsa_auth*. By default it sits in */usr/local/squid/libexec/ncsa_auth*, if you installed squid from rpm you will have to search for where this file is on your system. Once you have that done, use the *htpasswd* utility to create a password database with the usernames and passwords you want (I generally keep it in */etc/squid/passwd*)..

```
htpasswd /etc/squid/passwd <username>
```

Now you will need to edit your squid configuration file (*squid,conf*) to make use of these settings..

```
auth_param basic program /usr/local/squid/libexec/ncsa_auth /etc/squid/
passwd
auth_param basic children 5
auth_param basic realm Web Proxy
auth_param basic credentialsttl 2 hours
acl valid-people proxy_auth REQUIRED
http_access allow valid-people
http_access deny all
```

Now once you restart your squid services any new accesses to the web via the proxy will need a username and password. This is very useful for tracking individual usage of the web, and all squid reporting utilities can use this information to create user-based reports. Very nice.

Final Words
We covered off on two handy ways to use your firewall and your proxy, but remember that each of these servers can do a lot more than just this. So experiment, learn and have fun.