

Slow DNS requests?

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2006-03/msg00371.html>

- *From:* Jim R <flaflashr@xxxxxxxxxxxx>
 - *Date:* Tue, 14 Mar 2006 00:05:14 -0500
-

I need some help with my outbound requests, which seem much slower than I think they should. I'm really uncertain of where to look, so I will tell you what I think might contribute to the problem. I think that the delay is in resolving the DNS requests.

First a bit of background.

I am running Suse 9.1 on a dual-boot machine in a personal home network. The problem is apparent on Linux, but not on WinXp on the same machine. Here is the topology best as I can map it using clumsy ASCII

```
Charter.net 3 Mbps
|
V
Linksys BEFSR41
||||
||| ---> Linksys WAP54G
|||
||> n/c
||
||> Dell 400SC Suse 9.1/WinXP
|
> guest
```

Machines connected via the WAP54G run fine.

Guest machines connected via CAT5 to the BEFSR41 run fine.

When running WinXP on the Dell connected via CAT5 to the BEFSR41 runs fine.

Here's the problem. Running the Dell connected via the same CAT5 to the BEFSR41 seem very slow in resolving the host name. As soon as the host name is resolved, performance seems to improve dramatically for that connection. Subsequent net connection requests are slowed again.

The "slowness" is anything from a few seconds to a dozen seconds or more. This is apparent when requesting a Web page via a browser (Firefox or Mozilla). Or by pinging a URL style page (e.g., ping www.yahoo.com). Or requesting downloads from a remote POP. etc.

In the BEFSR41, I am running DHCP. The Charter.net DNS entered into the setup there are 241.151.8.210, 241.151.8.211 and 66.189.130.5. I do not remember where I got those, but it must have been from Charter.net when I set the system up over a year ago. When I search the Charter.net support site now, it does not talk about DNS addresses. It almost seems to go a long way to avoid the subject.

Slow DNS requests?

In Suse, I use Yast to enter the DNS setup page. These values seem to be stored in the file `/etc/resolv.conf`. It offers one set of entries for "Name Servers" and a different set for "Domain Search". Under Name Servers, I have entered the same IPs as shown above in the BEFSR41. Under Domain Search, I have entered `charter.net` for lack of something more clever.

All of that may be a red herring. Hopefully you can point me in the right direction. I have made a few tweaks in the entries on Suse, and it had both positive and negative effects on the search, but none seem to make it as fast as I think is correct.

Another area is my iptables blocking file. I run a small http server, and as soon as I started it several months ago, the hackers tried to break in. From the logs, I can see the IPs of the attacking clients. I read a bit about iptables, and figured that I could block these clients out by dropping their IP address. I have about 50 entries in the table so far. Here is the rest of my iptable, which is the default. Perhaps this is causing my problem -- I hope that you can direct me.

```
# syntax
#from the sample script
#!/bin/sh

IPTABLES=/usr/sbin/iptables

case "$1" in
start)
echo -n "Starting IP Firewall and NAT..."
echo "1" > /proc/sys/net/ipv4/ip_forward
echo "1" > /proc/sys/net/ipv4/tcp_syncookies

# Clear old rules
$IPTABLES -X
$IPTABLES -F
$IPTABLES -Z

# INPUT Rules - Add to this section the ports you wish to explicitly allow connections on
# Below are some common services that are commonly used
# Comment out the lines to disable access to these services
# The port numbers for other services you may wish to allow can be found in the /etc/services file

$IPTABLES -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT #Allows
connections you start

$IPTABLES -A INPUT -i eth0 -p tcp --dport 21 -j ACCEPT #Allow FTP Connections
$IPTABLES -A INPUT -i eth0 -p udp --dport 21 -j ACCEPT

$IPTABLES -A INPUT -i eth0 -p tcp --dport 22 -j ACCEPT #SSH Connections

$IPTABLES -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT #HTTP Connections

$IPTABLES -A INPUT -i eth0 -p tcp --dport 443 -j ACCEPT #SSL Connections

$IPTABLES -A INPUT -i eth0 -p tcp --dport 137 -j ACCEPT #SAMBA related ports
$IPTABLES -A INPUT -i eth0 -p tcp --dport 138 -j ACCEPT
```

Slow DNS requests?

Slow DNS requests?

```
$IPTABLES -A INPUT -i eth0 -p tcp --dport 139 -j ACCEPT
$IPTABLES -A INPUT -i eth0 -p udp --dport 138 -j ACCEPT
$IPTABLES -A INPUT -i eth0 -p udp --dport 139 -j ACCEPT
```

Allow pings, but reject the rest

```
$IPTABLES -A INPUT -i eth0 -p icmp -j ACCEPT
$IPTABLES -A INPUT -i eth0 -j REJECT
```

#here are the ones that I want to exclude, based upon their recent attacks on my system.

```
$IPTABLES -A INPUT -s xxx.xx.xxx.xx/24 -j DROP
$IPTABLES -A INPUT -s yyy.yy.yy.yyy/24 -j DROP
```

(repeats about 45–50 times with varying IPs).

echo "done."

::

(stop and restart cases follow then esac)

Thanks in advance for any help,

73 de Jim

.