

ip_conntrack: table full, dropping packet

Written by sdx

Tuesday, 07 May 2013 11:48 -

Last week, I found myself with a server under low load, but it couldn't make or receive network connections. When I ran `dmesg`, I found the following line repeating over and over:

```
ip_conntrack: table full, dropping packet
```

I'd seen this message before, but I headed over to [Red Hat's site](#) for more details. It turns out that the server was running iptables, but it was under a very heavy load and also handling a high volume of network connections. Generally, the `ip_conntrack_max` is set to the total MB of RAM installed multiplied by 16. However, this server had 4GB of RAM, but `ip_conntrack_max` was set to 65536:

```
# cat /proc/sys/net/ipv4/ip_conntrack_max 65536
```

I logged into another server with 1GB of RAM (RHES 5, 32-bit) and another with 2GB of RAM (RHES 4, 64-bit), and both had `ip_conntrack_max` set to 65536. I'm not sure if this is a known Red Hat issue, or if it's just set to a standard value out of the box.

If you want to check your server's current tracked connections, just run the following:

```
# cat /proc/sys/net/ipv4/netfilter/ip_conntrack_count
```

If you want to adjust it (as I did), just run the following as root:

```
# echo 131072 > /proc/sys/net/ipv4/ip_conntrack_max
```

This solves the problem at this moment, but after a reboot the initial value will be restored.

To make this persistent you have to add a line like `'net.ipv4.ip_conntrack_max=131072'` to `/etc/sysctl.conf`

Some distros apparently don't have that file; there you should use the echo-line in a boot script