How to solve (work around) an /etc/init.d/iptables failed issues caused by iptables Unknown error 18446744073709551615 on CentOS 5.5 Final

Author : admin

Today I have encountered an oddity on **CentOS release 5.5 (Final)**. The problem consisted in the iptables firewall not loading it's rules.
After a bit of debugging I've found out that the whole issue was caused by a failure for **/sbin/iptables-save** to read the **/etc/sysconfig/iptables** stored iptables rules.

I've reviewed all the rules in the */etc/sysconfig/iptables* and all of them appeared to be absolutely syntax correct, however since the **iptables-restore** command parser failed to load on a line after which was contaned the following iptables rules:

-A RH-Firewall-1-INPUT -m state --state NEW -p tcp -m tcp --syn -m recent --name synflood --set
-A RH-Firewall-1-INPUT -m state --state NEW -p tcp -m tcp --syn -m recent --name synflood --update --seconds 1 --hitcount 100 -j DROP

Which had to deal with the server **SYN Flood Protection** I've decided to attempt to issue the iptables rules directly from the command line like so:

[root@centos-server ~]# iptables -A INPUT -m state --state NEW -p tcp -m tcp --syn -m recent --name synflood --set
[root@centos-server ~]# iptables -A INPUT -m state --state NEW -p tcp -m tcp --syn -m recent --name synflood --update --seconds 1 --hitcount 100 -j DROP

Executing the above iptables lines I was unpleasently surprised by the error:

iptables: Unknown error 18446744073709551615

Googling for the error led me to many discussions none of which has suggested a concrete reasons that causes the issue, so I finally decided to experiment on my own in order to find the solution.

By the way it's imporant to mention that I have encounted the **iptables: Unknown error 18446744073709551615** problem on a CentoS 5.5 (Final running kernel version:
Linux centos-server 2.6.18-194.3.1.el5 #1 SMP Thu May 13 13:08:30 EDT 2010 x86_64 x86_64 x86_64 GNU/Linux

What is even more interesting is that another CentOS server running a kernel version:

Linux centos-server1 2.6.18-128.7.1.el5 #1 SMP Mon Aug 24 08:21:56 EDT 2009 x86_64 x86_64 x86_64 GNU/Linux

is executing the above anti SYN flood iptables rules absolutely correctly.
Well I have to admit this is quite ODD. I have checked a module by module all modules related to iptables to assure myself that the error **iptables: Unknown error 18446744073709551615** is not caused by a missing iptables related module on the server.
However all the iptables modules which was loaded on the server which was able to properly execute the iptables command without errors were loaded on the server where the error persisted.

Finally I've decided to completely remove the iptables anti-flood lines:

-A RH-Firewall-1-INPUT -m state --state NEW -p tcp -m tcp --syn -m recent --name synflood --set
-A RH-Firewall-1-INPUT -m state --state NEW -p tcp -m tcp --syn -m recent --name synflood --update --seconds 1 --hitcount 100 -j DROP

And substitute my **ANTI SYN FLOOD** protection rules in **/etc/sysconfig/iptables** with the following iptable rules:

-N syn-flood
-A INPUT -i eth0 -p tcp --syn -j syn-flood
-A syn-flood -m limit --limit 1/s --limit-burst 4 -j RETURN
-A syn-flood -j DROP

The above iptables rules to **protect against SYN FLOODS** worked like a charm a simple restart of the firewall loaded the firewall with the new substituted rules.

[root@centos-server ~]# /etc/init.d/iptables restartFlushing firewall rules: [OK]
Setting chains to policy ACCEPT: filter [OK]
Unloading iptables modules: [OK]
Applying iptables firewall rules: [OK]
Loading additional iptables modules: ip_conntrack_netbios_n[OK]