iptables

Debian TS-WXL

I want to filter DDOS packets from botnets with iptables.
It would be nice if the kernel could use iptables.

Install and verify iptables.

Install iptables

```
tswxl:~# apt-get install iptables
Reading package lists... Done
Building dependency tree
Reading state information... Done
iptables is already the newest version.
The following packages were automatically installed and are no longer required:
  libnet-ssleay-perl libnet-libidn-perl
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
odxl: ~ #
```

that? I'm already here.
libnet-ssleay-perl libnet-libidn-perl

Does iptable work?

```
tswxl:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
odxl: ~ #
```

Looks like it is moving normally.

Filter settings

Try setting a filter to deny access from your current machine

```
tswxl:~# iptables -A INPUT -p tcp --dport 80 -s  192.168.2.173 -j DROP
tswxl:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  x31l.yamasita.jp     anywhere            tcp dpt:www

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

```
target     prot opt source               destination
odxl: ~ #
```

When I tried to access it from a browser, it said, "Google Chrome could not connect to 192.168.2.70." \ ^ _ ^ /

Try to erase rules

```
tswxl:~# iptables -D INPUT 1
tswxl:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
odxl: ~ #
```

When I accessed it again from the browser, I could access it properly this time.

Alright, filtering now has a trick.

But I decided to take a log and grin,

```
tswxl:~# iptables -A INPUT -p tcp --dport 80 -s  192.168.2.173 -j LOG
iptables: No chain/target/match by that name
odxl: ~ #
```

LOG is not implemented.

```
tswxl: ~ # ls /lib/modules/2.6.22.18-mv78100/kernel/net
802  appletalk  llc
odxl: ~ #
```

Also kernel module. .

← Install PostTweet plugin

Hack of record LinkStation / **KuroBox** trying to hack

→ Block bots with iptables
