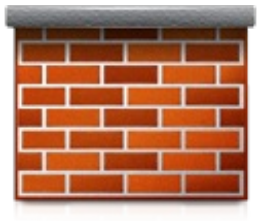
Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

Iptables: Invert IP, Protocol, Or Interface Test With !

Posted by Vivek Gite <vivek@nixcraft.com>



How do I invert a protocol or ip address test while writing iptables based shell scripts?

The iptables command comes with ! operator. The most of these rules can be preceded by a ! to invert the sense of the match. A match can be:

1. Source or dest ip address
2. Interface name
3. Protocol name etc

[1]

Examples

The following will match all protocol except UDP:

```
iptables -A INPUT -p ! UDP
```

The following match allows IP address range matching and it can be inverted using the ! sign:

```
iptables -A INPUT -d 192.168.0.0/24 -j DROP
iptables -A OUTPUT -d ! 202.54.1.2 -J ACCEPT
# we trust 202.54.1.5 so skip it
iptables -A OUTPUT -s ! 202.54.1.5 -J DROP
```

The exclamation mark inverts the match so this will result is a match if the IP is anything except one in the given range 192.168.1.0/24:

```
iptables -A INPUT -s ! 192.168.1.0/24 -p tcp --dport 80 -J DROP
```

You can skip your own ip from string test:

```
iptables -A FORWARD -i eth0 -p tcp ! -s 192.168.1.2 --sport 80 -m string --string '|7F|ELF'
```

Accept port 22 traffic on all interfaces except for eth1 which is connected to the Internet:

```
iptables -A INPUT -i !eth1 -p tcp --dport 22  -j ACCEPT
```

Recommended readings:

```
man iptables
```

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/category/iptables/**
