Home > FAQ > Iptables

Linux: Block Port With IPtables

Posted By nixCraft <webmaster@cyberciti.biz> On December 10, 2010 @ 9:18 pm [11 Comments]

How do I block port number with iptables under Linux operating systems?

Port numbers which are recognized by Internet and other network protocols, enabling the computer to interact with others. Each Linux server has a port number (see /etc/services [2] file). For example:

1. TCP port 80 - HTTP Server
2. TCP port 443 - HTTPS Server
3. TCP port 25 - Mail Server
4. TCP port 22 - OpenSSH (remote) secure shell server
5. TCP port 110 - POP3 (Post Office Protocol v3) server
6. TCP port 143 - Internet Message Access Protocol (IMAP) — management of email messages
7. TCP / UDP port 53 - Domain Name System (DNS)
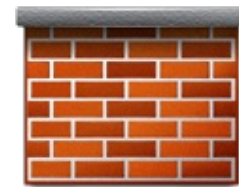
[1]

[3]

Block Incoming Port

The syntax is as follows to block incoming port using IPtables:

```
/sbin/iptables -A INPUT -p tcp --destination-port {PORT-NUMBER-HERE} -j DROP

### interface section use eth1 ###
/sbin/iptables -A INPUT -i eth1 -p tcp --destination-port {PORT-NUMBER-HERE} -j DROP

### only drop port for given IP or Subnet ##
/sbin/iptables -A INPUT -i eth0 -p tcp --destination-port {PORT-NUMBER-HERE} -s {IP-ADDRESS-HERE} -j DROP
/sbin/iptables -A INPUT -i eth0 -p tcp --destination-port {PORT-NUMBER-HERE} -s {IP/SUBNET-HERE} -j DROP
```

To block port 80 (HTTP server), enter (or add to your iptables shell script):
```
# /sbin/iptables -A INPUT -p tcp --destination-port 80 -j DROP
# /sbin/service iptables save
```

Block Incomming Port 80 except for IP Address 1.2.3.4

```
# /sbin/iptables -A INPUT -p tcp -i eth1 -s ! 1.2.3.4 --dport 80 -j DROP
```

Block Outgoing Port

The syntax is as follows:

```
/sbin/iptables -A OUTPUT -p tcp --dport {PORT-NUMBER-HERE} -j DROP

### interface section use eth1 ###
/sbin/iptables -A OUTPUT -i eth1 -p tcp --dport {PORT-NUMBER-HERE} -j DROP

### only drop port for given IP or Subnet ##
/sbin/iptables -A OUTPUT -i eth0 -p tcp --destination-port {PORT-NUMBER-HERE} -s {IP-ADDRESS-HERE} -j DROP
/sbin/iptables -A OUTPUT -i eth0 -p tcp --destination-port {PORT-NUMBER-HERE} -s {IP/SUBNET-HERE} -j DROP
```

To block outgoing port # 25, enter:
```
# /sbin/iptables -A OUTPUT -p tcp --dport 25 -j DROP
# /sbin/service iptables save
```
You can block port # 1234 for IP address 192.168.1.2 only:
```
# /sbin/iptables -A OUTPUT -p tcp -d 192.168.1.2 --dport 1234 -j DROP
```

```
# /sbin/service iptables save
```

How Do I Log Dropped Port Details?

Use the following syntax:

```
# Logging #
### If you would like to log dropped packets to syslog, first log it ###
/sbin/iptables -A INPUT -m limit --limit 5/min -j LOG --log-prefix "PORT 80 DROP: " --log-level 7

### now drop it ###
/sbin/iptables -A INPUT -p tcp --destination-port 80 -j DROP
```

How Do I Block Cracker (IP: 123.1.2.3) Access To UDP Port # 161?

```
/sbin/iptables -A INPUT -s 123.1.2.3 -i eth1 -p udp -m state --state NEW -m udp --dport 161 -j DROP

# drop students 192.168.1.0/24 subnet to port 80
/sbin/iptables -A INPUT -s 192.168.1.0/24 -i eth1 -p tcp -m state --state NEW -m tcp --dport 80 -j DROP
```

Important Message from nixCraft:

4000+ howtos and counting! Want to read more Linux / UNIX howtos, tips and tricks? We request you to sign up for the following to ensure that you make the most from our guides / howtos:

1. **RSS feed for nixCraft** - Get intimated about our new howtos / faqs as soon as it is released.
2. Daily **email newsletter** or **weekly newsletter** - Get intimated about our new howtos / faqs as soon as it is released via email.

URL to article: **http://www.cyberciti.biz/faq/iptables-block-port/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/category/iptables/**
[2] /etc/services: **http://www.cyberciti.biz/faq/find-out-which-service-listening-specific-port/**
[3] Image: **http://www.cyberciti.biz/faq/category/linux/**