

Exp.No.:11

Date:

INSTALLANDCONFIGUREIPTABLESFIREWALL

Aim: To install iptables and configure it for variety of options.

Common Configurations & outputs:

1. Start/stop/restart firewalls

```
[root@localhost ~]# systemctl start firewalld
[root@localhost ~]# systemctl restart firewalld
[root@localhost ~]# systemctl stop firewalld
[root@localhost ~]#
```

2. Check all existing IPtables Firewall Rules

```
[root@localhost ~]# iptables -L -n -v
[root@localhost ~]#
```

3. Block specific IP Address (eg. 172.16.8.10) in IPtables Firewall

```
[root@localhost ~]# iptables -A INPUT -s 172.16.8.10 -j DROP
[root@localhost ~]#
```

4. Block specific port on IPtables Firewall

```
[root@localhost ~]# iptables -A OUTPUT -p tcp --dport xxx -j DROP [root@localhost ~]#
```

5. Allow specific network range on particular port on iptables

```
[root@localhost ~]# iptables -A OUTPUT -p tcp -d 172.16.8.0/24 --dport xxx -j
ACCEPT
[root@localhost ~]#
```

6. Block Facebook on IPtables

[root@localhost ~]# host facebook.com facebook.com has address 157.240.24.35
facebook.com has IPv6 address 2a03:2880:f10c:283:face:b00c:0:25de
facebook.com mail is handled by 10 smtpin.vvv.facebook.com.

[root@localhost~]#whois157.240.24.35|grepCIDRCIDR:157.240.0.0/16
[root@localhost ~]#

[root@localhost~]#whois157.240.24.35[Queryingwhois.arin.net]
[whois.arin.net] #
#ARINWHOISdataandservicesaresubjecttotheTermsofUse#availableat:
<https://www.arin.net/resources/registry/whois/tou/> # #
Ifyouseeinaccuraciesintheresults,pleasereportat
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/ #
#Copyright1997-2019,AmericanRegistryforInternetNumbers,Ltd.#

NetRange: 157.240.0.0-157.240.255.255CIDR:157.240.0.0/16
NetName: THEFA-3 NetHandle: NET-157-240-0-0-1
Parent: NET157(NET-157-0-0-0-0)NetType:
DirectAssignmentOriginAS:
Organization:Facebook,Inc.(THEFA-3)RegDate: 2015-05-14
Updated: 2015-05-14
Ref:<https://rdap.arin.net/registry/ip/157.240.0.0>
OrgName: Facebook,Inc.OrgId: THEFA-3
Address: 1601WillowRd.City: MenloParkStateProv: CA
PostalCode: 94025Country: USRegDate: 2004-08-11
Updated: 2012-04-17
Ref:<https://rdap.arin.net/registry/entity/THEFA-3>

OrgTechHandle:OPERA82-ARINOrgTechName:OperationsOrgTechPhone:+1-
650-543-4800 OrgTechEmail: domain@facebook.com
OrgTechRef: <https://rdap.arin.net/registry/entity/OPERA82-ARIN>

OrgAbuseHandle:OPERA82-ARINOrgAbuseName:OperationsOrgAbusePhone:
+1-650-543-4800 OrgAbuseEmail:
domain@facebook.comOrgAbuseRef:
<https://rdap.arin.net/registry/entity/OPERA82-ARIN>

#

#ARINWHOISdataandservicesaresubjecttotheTermsofUse#availableat:
<https://www.arin.net/resources/registry/whois/tou/>

#

#Ifyouseeinaccuraciesintheresults,pleasereportat
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/ #
#Copyright1997-2019,AmericanRegistryforInternetNumbers,Ltd.#

[root@localhost~]#iptables-AOUTPUT-ptcp-d157.240.0.0/16-jDROPOpen browser
and check whether <http://facebook.com> is accessible

Toallowfacebookuse-Dinsteadof-Aoption

[root@localhost~]#iptables-DOUTPUT-ptcp-d157.240.0.0/16-jDROP
[root@localhost ~]#

6.BlockAccesstoyoursystemfromspecificMACAddress(say 0F:22:1E:00:02:30)

[root@localhost~]#iptables-AINPUT-mmact--mac-source0F:22:1E:00:02:30-j DROP
[root@localhost~]#

7.SaveIPtablesrulesto a file

[root@localhost~]#iptables-save>~/iptables.rules
[root@localhost ~]# vi iptables.rules
[root@localhost ~]#

8.RestrictnumberofconcurrentconnectionstoServer(Hererestrictto3 connections only)

```
[root@localhost~]#iptables-AINPUT-ptcp--syn--dport22-mconnlimit-connlimit-above 3 -j REJECT
```

9.DisableoutgoingmailsthroughIPtables

```
[root@localhost~]#iptables-AOUTPUT-ptcp--dport25-jREJECT [root@localhost ~]#
```

10.FlushIPtablesFirewallchainsorrules

```
[root@localhost~]#iptables-F[root@localhost~]#
```

Result: