# Table Of Contents

Home > Faq > CentOS

Understanding CentOS Default -A RH-Firewall-1-INPUT -p 50 -j ACCEPT Firewall Rule

Posted by Vivek Gite <vivek@nixcraft.com>

Q.Can you explain the meaning of following two firewall rules present in my /etc/sysconfig/iptables rules under CentOS Enterprise Linux version 5.2?

-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT

A. This is related to Internet Protocol Security (IPsec) is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream.
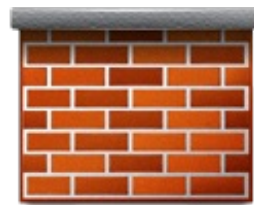
[1]

The -p option is used to specify protocol name such as tcp, udp, icmp or it can be a numeric value, representing one of these protocols or a different one. A protocol name from /etc/protocols is allowed. In short

- **50** is Encap Security Payload (esp / IPSEC-ESP) protocol
- **51** is IPSEC-AH - Authentication Header protocol

Above two rules allowing IPsec communication i.e. IPSEC packets passed via your firewall. If you would like to block IPsec, change rules as follows:

```
-A RH-Firewall-1-INPUT -p 50 -j REJECT
-A RH-Firewall-1-INPUT -p 51 -j REJECT
```

Reload firewall, enter:

```
# service iptables restart
```

For further information refer to iptables man page and /etc/protocols:

```
man iptables
```

Sample /etc/protocols file

```
$ cat /etc/protocols
```

Output:

```
# Internet (IP) protocols
#
# Updated from http://www.iana.org/assignments/protocol-numbers and other
# sources.
# New protocols will be added on request if they have been officially
# assigned by IANA and are not historical.
# If you need a huge list of used numbers please install the nmap package.

ip      0       IP              # internet protocol, pseudo protocol number
#hopopt 0       HOPOPT          # IPv6 Hop-by-Hop Option [RFC1883]
icmp    1       ICMP            # internet control message protocol
igmp    2       IGMP            # Internet Group Management
ggp     3       GGP             # gateway-gateway protocol
ipencap 4       IP-ENCAP        # IP encapsulated in IP (officially ``IP'')
st      5       ST              # ST datagram mode
tcp     6       TCP             # transmission control protocol
egp     8       EGP             # exterior gateway protocol
igp     9       IGP             # any private interior gateway (Cisco)
pup     12      PUP             # PARC universal packet protocol
udp     17      UDP             # user datagram protocol
```

```
hmp       20         HMP              # host monitoring protocol
xns-idp 22           XNS-IDP          # Xerox NS IDP
rdp       27         RDP              # "reliable datagram" protocol
iso-tp4 29           ISO-TP4          # ISO Transport Protocol class 4 [RFC905]
xtp       36         XTP              # Xpress Transfer Protocol
ddp       37         DDP              # Datagram Delivery Protocol
idpr-cmtp 38         IDPR-CMTP        # IDPR Control Message Transport
ipv6      41         IPv6             # Internet Protocol, version 6
ipv6-route 43        IPv6-Route       # Routing Header for IPv6
ipv6-frag 44         IPv6-Frag        # Fragment Header for IPv6
idrp      45         IDRP             # Inter-Domain Routing Protocol
rsvp      46         RSVP             # Reservation Protocol
gre       47         GRE              # General Routing Encapsulation
esp       50         IPSEC-ESP        # Encap Security Payload [RFC2406]
ah        51         IPSEC-AH         # Authentication Header [RFC2402]
skip      57         SKIP             # SKIP
ipv6-icmp 58         IPv6-ICMP        # ICMP for IPv6
ipv6-nonxt 59        IPv6-NoNxt       # No Next Header for IPv6
ipv6-opts 60         IPv6-Opts        # Destination Options for IPv6
rspf      73         RSPF CPHB        # Radio Shortest Path First (officially CPHB)
vmtp      81         VMTP             # Versatile Message Transport
eigrp     88         EIGRP            # Enhanced Interior Routing Protocol (Cisco)
ospf      89         OSPFIGP          # Open Shortest Path First IGP
ax.25     93         AX.25            # AX.25 frames
ipip      94         IPIP             # IP-within-IP Encapsulation Protocol
etherip 97           ETHERIP          # Ethernet-within-IP Encapsulation [RFC3378]
encap     98         ENCAP            # Yet Another IP encapsulation [RFC1241]
#         99                          # any private encryption scheme
pim       103        PIM              # Protocol Independent Multicast
ipcomp    108        IPCOMP           # IP Payload Compression Protocol
vrrp      112        VRRP             # Virtual Router Redundancy Protocol
l2tp      115        L2TP             # Layer Two Tunneling Protocol [RFC2661]
isis      124        ISIS             # IS-IS over IPv4
sctp      132        SCTP             # Stream Control Transmission Protocol
fc        133        FC               # Fibre Channel
```

4000+ howtos and counting! Want to read more Linux / UNIX howtos, tips and tricks? Subscribe to our daily email newsletter or weekly newsletter to make sure you don't miss a single tip/tricks. Alternatively, subscribe via RSS/XML feed.

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/centos-linux-ipsec-firewall-rules/**

URLs in this post:

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