# Cisco PCP-PNR Port Usage Information

**EDCS-1109712**

Table of Contents

# 1 Introduction

This document provides details of CISCO PCP / CNR port usage information. Within the scope of this document Linux IPTable rules are mentioned which should be applied on the Linux based installations.

# 2 Prerequisites

Readers of this document should have knowledge of the following:

- Linux OS [RHEL 5.x/6.x & RHEL 5.x/6.x]
- CISCO PCP Admin/Port configuration information (incase any port configuration has been changed during the installation/management. Ref)
- CNR Admin/Port configuration information (incase any port configuration has been changed during the installation/management. Ref)

Version of Products used as scope of this document

- Broadband Access Center (Cisco PCP) 5.0,5.1
- Cisco Network Registrar (Cisco PNR) 8.x

# 3 Glossary

## 3.1 CISCO PCP Local Machine

These ports are used for communication on the given machine only (nothing outside of the machine should be able to access these ports)

### 3.1.1 CISCO PCP Component

These ports are used for communication between CISCO PCP components (these ports should be protected from subscribers)

### 3.1.2 CISCO PCP Administrator

These ports are used for communication or for user interfaces to be used by CISCO PCP Administrators (these ports should be protected from subscribers)

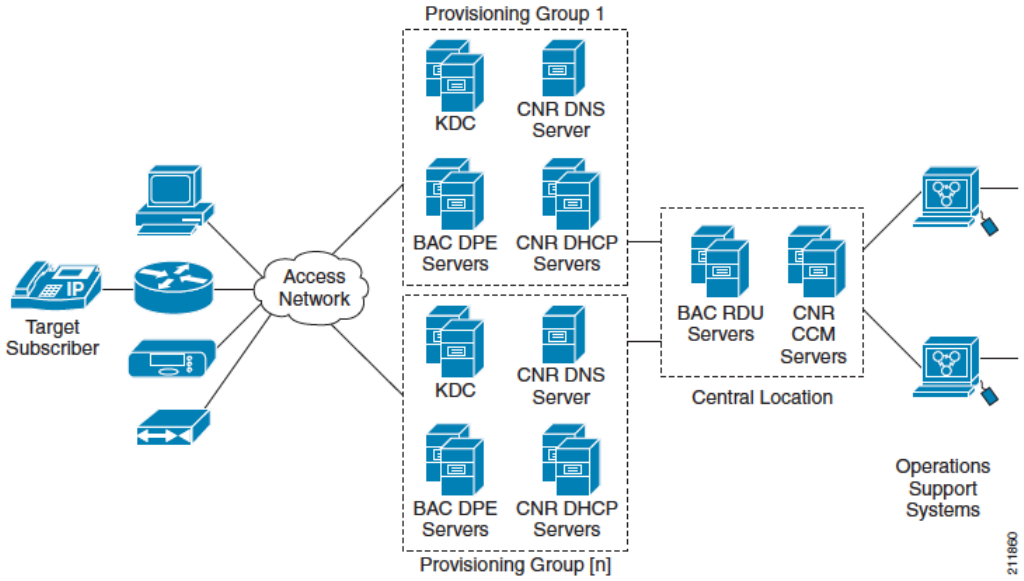
### 3.1.3 CISCO PCP Device Provisioning

These ports are used for communication with subscriber devices on the network (these ports should be reachable from subscribers)

The ports listed here are only the ports that the CISCO PCP servers listen on; they do not include the ports that are used to connect from (e.g. in the case of a TCP based client connecting to a TCP based server).

## 3.2 CISCO PCP Components

## 3.2.1 Sample Deployment: Cisco CNR and CISCO PCP




## 3.2.2 CISCO PCP RDU Server Port Usage information

### 3.2.2.1 Local Machine Ports

| Port/Protocol | Comments |
|---|---|
| 49888/TCP | • CISCO PCP Watchdog (bprAgent) listens on this port. The port value is configurable. You will need to edit a property entry (/agent/agentport=49888) in $CISCO BPR_HOME/agent/conf/agent.conf as well as a property entry (/snmp/statusServer/port=49888) in $CISCO BPR_HOME/rdu/snmp/conf/agent.properties. Make sure that the two properties have the same port value. |
| 49887/TCP | • RDU SNMP Agent's listening port (for watchdog) The port value is configurable. You will need to edit a property entry (/agent/statusport=49887) in $CISCO BPR_HOME/agent/conf/agent.conf as well as a property entry (/snmp/statusReceiver/port=49887) in $CISCO BPR_HOME/rdu/snmp/conf/agent.properties. Make sure that the two properties have the same port value. |

| | |
|---|---|
| 8001/UDP | • RDU SNMP Agent's SNMP port<br>The port value is configurable. A script rduSnmpAgent.sh located in $CISCO BPR_HOME/rdu/snmp/bin directory can be used to modify the default port value. |

#### 3.2.2.2 CISCO PCP RDU Port usage for DHCP lease query support

| | |
|---|---|
| 67/UDP | • DHCPv4 Lease Query between the RDU and the DHCP servers. |
| 547/UDP | • DHCPv6 Lease Query between the RDU and the DHCP servers |

#### 3.2.2.3 CISCO PCP RDU Port usage for RDU Redundancy Solution

| | |
|---|---|
| 5405/UDP | • Multicast port, for Totem ring support. |
| 5407/UDP | • Multicast port, for Totem ring support. |
| 7788/TCP | • File block level Data sync for bprData resource |
| 7789/TCP | • File block level Data sync for bprHome resource |
| 7790/TCP | • File block level Data sync for bprLog resource |

### 3.2.3 CISCO PCP Component Ports

| | |
|---|---|
| 49187/TCP | • The default port used by the RDU server. This port is also used by Db utilities (this is because we actually want to prevent the RDU from running when Db utilities are in use).<br>The port value is configurable. ServerProperties.SERVER_PORT_KEY or /server/port is used to change the port value. |
| 49188/TCP | • RDU secure communication |

#### 3.2.3.1 CISCO PCP Administrator Ports

| | |
|---|---|
| 8100/TCP | • The default HTTP port used by CISCO PCP Admin UI |
| 8443/TCP | • The default HTTPS port used by CISCO PCP Admin UI |

### 3.2.3.2 Device Provisioning Ports

None

## 3.2.4 CISCO PCP DPE Server

### 3.2.4.1 Local Machine Ports

| | |
|---|---|
| 8008/UDP | • Internal Registration Service to SNMP Service (only if PacketCable is enabled) |
| 8001/UDP | • Appliance DPEs native SNMP agent's port |
| ***Random/UDP*** | • ***Internal SNMP Service*** |
| ***Random/UDP*** | • ***Internal Kerberos Service*** |

### 3.2.4.2 CISCO PCP Component Ports

| | |
|---|---|
| 49186 UDP | • The default port used by DPE server.<br>The port value is configurable. Use DPE CLI "dpe port <port>" to change the port value. Make sure your DPE is stopped when you change the port value. |
| 2246/UDP | • Inbound messages from KDC (only if PacketCable is enabled) |

### 3.2.4.3 CISCO PCP Administrator Ports

| | |
|---|---|
| 2323/TCP | • Software DPE CLI listens on 2323 by default<br>The port value is configurable. You will need to edit a property entry /cli/port=2323 in $CISCO BPR_HOME/cli/conf/cli.properties. |
| 23/TCP | • Appliance DPE CLI listens on 23 by default |
| 21/TCP | • Appliance FTP server |
| 161/UDP | • Appliance DPE SNMP agent port |
| 23/TCP | • Appliance DPE CLI listens on 23 by default |
| 21/TCP | • Appliance FTP server |
| 161/UDP | • Appliance DPE SNMP agent port |

### 3.2.4.4 Device Provisioning Ports

| | |
|---|---|
| 37/UDP | • Time of day port |
| 37/TCP | • Time of day port |
| 162/UDP | • Inbound MTA messages to SNMP Service (only if PacketCable is |

| | |
|---|---|
| | enabled) |
| 1293/UDP | • Registration Server to MTA (only if PacketCable is enabled) |

## 3.2.5 CNR Port Usage information

### 3.2.5.1 CNR-DNS Process Port usage

| | |
|---|---|
| 1234/TCP | • localhost only, port configurable at installation |
| 53/TCP | • IANA assigned port for DNS |
| 53/UDP | • IANA assigned port for DNS |
| 653/UDP | • Used only when HA-DNS configured |

### 3.2.5.2 CNR-DHCP Process Port usage

| | |
|---|---|
| 547/UDP | • The default port number that the DHCP server should listen on for DHCPv6 messages. |
| 546/UDP | • The default port used as the destination for packets sent to DHCPv6 clients. |
| 67/UDP | • The default port number that the DHCP server should listen on. |
| 68/UDP | • The default port used as the destination for packets sent to DHCP clients. |
| 647/UDP | • The port assigned to the DHCP failover protocol. |

### 3.2.5.3 CNR-CCM Process Port usage

| | |
|---|---|
| 1234/TCP | • SCP Communications |

### 3.2.5.4 CNR-WebServer Process Port usage

| | |
|---|---|
| 8080/TCP | Default Webserver port for http communication |
| 8443/TCP | Webserver HTTPS port |

### 3.2.5.5 CNR-SNMP Process Port usage

| | |
|---|---|
| 4444/TCP | • The port to listen on for incoming SNMP queries. |

### 3.2.5.6 CNR-TFTP Process Port usage

| | |
|---|---|
| 69/TCP | • TFTP port |

## 3.2.6 CISCO PCP CNR Extension Point Ports

- N/A

### 3.2.6.1 Local Machine Ports

- N/A

### 3.2.6.2 CISCO PCP Component Ports

1 random UDP port for status messages to the DPEs for each DPE, 16 random UDP ports connected to that DPE for configuration queries. NOTE: My advice here is to leave open the DPE port (49186) from the CNR server and allow traffic from the DPE to the CNR servers because the DPE will reply to where the packet came from.

### 3.2.6.3 CISCO PCP Administrator Ports

- N/A

Device Provisioning Ports

- N/A

## 3.2.7 CISCO PCP KDC Ports

### 3.2.7.1 Local Machine Ports

- N/A

#### 3.2.7.2 CISCO PCP Component Ports

- N/A

#### 3.2.7.3 CISCO PCP Administrator Ports

- N/A

#### 3.2.7.4 Port Configuration

| | |
|---|---|
| 88/UDP | default port used by KDC server |
| 2246/UDP | KDC sends on UDP port 2246 (FQDN-REQ) |

## 3.3 IPTables

Included with Red Hat Enterprise Linux are advanced tools for network *packet filtering* — the process of controlling network packets as they enter, move through, and exit the network stack within the kernel. Kernel versions prior to 2.4 relied on `ipchains` for packet filtering and used lists of rules applied to packets at each step of the filtering process. The 2.4 kernel introduced `iptables` (also called *netfilter*), which is similar to `ipchains` but greatly expands the scope and control available for filtering network packets.

The default firewall mechanism in the 2.4 and later kernels is `iptables`, but `iptables` cannot be used if `ipchains` is already running. If `ipchains` is present at boot time, the kernel issues an error and fails to start `iptables`.
The functionality of `ipchains` is not affected by these errors.

### 3.3.1 Packet Filtering

The Linux kernel uses the **Netfilter** facility to filter packets, allowing some of them to be received by or pass through the system while stopping others. This facility is built in to the Linux kernel, and has three built-in *tables* or *rules lists*, as follows:

- `filter` — The default table for handling network packets.
- `nat` — Used to alter packets that create a new connection and used for *Network Address Translation* (*NAT*).
- `mangle` — Used for specific types of packet alteration.

Each table has a group of built-in *chains*, which correspond to the actions performed on the packet by `netfilter`.

The built-in chains for the `filter` table are as follows:

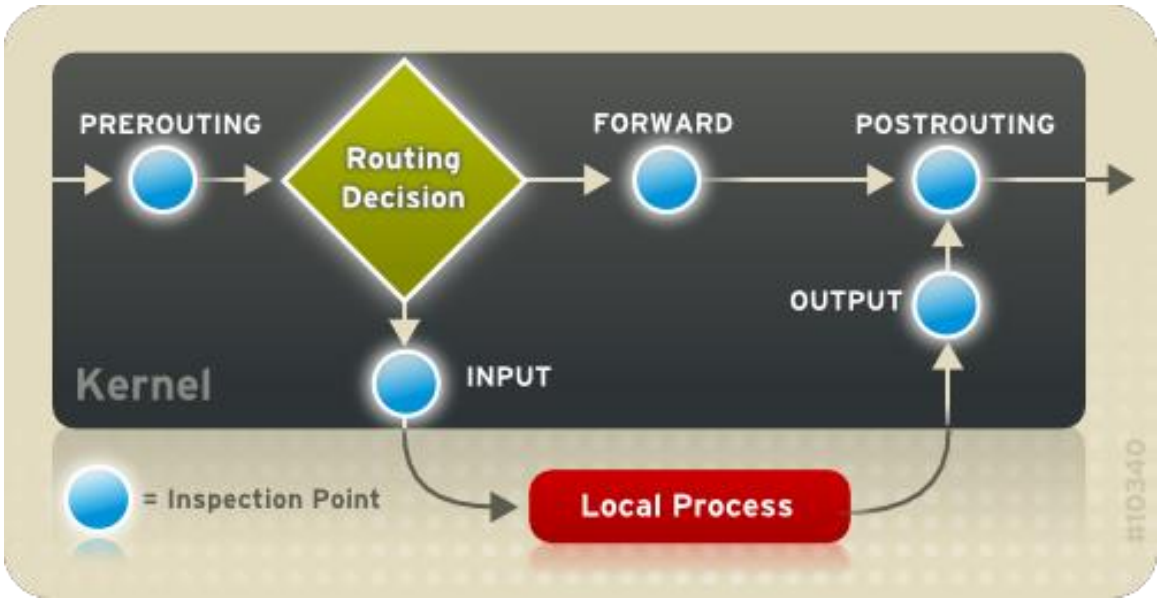
- *INPUT* — Applies to network packets that are targeted for the host.
- *OUTPUT* — Applies to locally-generated network packets.
- *FORWARD* — Applies to network packets routed through the host.

The built-in chains for the `nat` table are as follows:

- *PREROUTING* — Alters network packets when they arrive.
- *OUTPUT* — Alters locally-generated network packets before they are sent out.
- *POSTROUTING* — Alters network packets before they are sent out.

The built-in chains for the `mangle` table are as follows:

- *INPUT* — Alters network packets targeted for the host.
- *OUTPUT* — Alters locally-generated network packets before they are sent out.
- *FORWARD* — Alters network packets routed through the host.
- *PREROUTING* — Alters incoming network packets before they are routed.
- *POSTROUTING* — Alters network packets before they are sent out.




By default, firewall rules are saved in the `/etc/sysconfig/iptables` or `/etc/sysconfig/ip6tables` files.

Regardless of their destination, when packets match a particular rule in one of the tables, a *target* or action is applied to them. If the rule specifies an `ACCEPT` target for a matching packet, the packet skips the rest of the rule checks and is allowed to continue to its destination. If a rule specifies a `DROP` target, that packet is refused access to the system and nothing is sent CIsco PCPk to the host that sent the packet. If a rule specifies a `QUEUE` target, the packet is passed to user-space. If a rule specifies the optional `REJECT` target, the packet is dropped, but an error packet is sent to the packet's originator.

## EDCS-1109712

Every chain has a default policy to `ACCEPT`, `DROP`, `REJECT`, or `QUEUE`. If none of the rules in the chain apply to the packet, then the packet is dealt with in accordance with the default policy.

## 3.4 Modify Firewall Rules (IPTables)

### Step 1: EDIT iptables rules

```
#vi /etc/sysconfig/iptables
```

### Step 2: Edit the properties as mentioned in respective section

a. Regional Distribution Unit
b. Device Provisioning Engine
c. Cisco Network Registrar

### Step 3: RESTART iptables service to commission new/edited rules

```
# service iptables stop
Flushing firewall rules:                                   [  OK  ]
Setting chains to policy ACCEPT: filter                    [  OK  ]
Unloading iptables modules:                                [  OK  ]

# service iptables start
Applying iptables firewall rules:                                      [  OK  ]
Loading additional iptables modules: ip_conntrack_netbios_n            [  OK  ]
```

## 3.5 Recommended Configuration

### 3.5.1 CISCO PCP – RDU [ /etc/sysconfig/iptables ] entries to allow CISCO PCP setup functioning.

```
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8100 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8443 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 49887 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 49888 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 49187 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 7788 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 7789 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 7790 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 161 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 162 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 67 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 547 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 8001 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 5405 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 5407 -j ACCEPT
```

### 3.5.2 CISCO PCP – DPE [ /etc/sysconfig/iptables ] entries to allow CISCO PCP setup functioning.

```
#Generated by iptables-save v1.3.5 on Fri Feb  3 02:03:31 2012
*filter
:INPUT ACCEPT [3359:1211794]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [2857:218490]
:RH-Firewall-1-INPUT - [0:0]
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 2323 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 49187 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 37 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8009 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 9006 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 37 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 49186 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 8001 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 8005 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 161 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 162 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 69 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1293 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 88 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 2246 -j ACCEPT
COMMIT

# Completed on Fri Feb  3 02:03:31 2012
```

### 3.5.3 CNR [ /etc/sysconfig/iptables ] entries to allow CISCO PCP-CNR setup functioning.

```
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
#cnr-dns
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 53 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 53 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 653 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 653 -j ACCEPT
#cnr-dhcp
-A RH-Firewall-1-INPUT -p udp -m udp --dport 547 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 546 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 67 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 67 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 68 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 647 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 389 -j ACCEPT
#cnr-WebServer
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8005 -j ACCEPT
#cnr-snmp
-A RH-Firewall-1-INPUT -p udp -m udp --dport 4444 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 4444 -j ACCEPT
#snmp-traps “Server to Server”
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 162 -j ACCEPT
#cnr-TFTP
-A RH-Firewall-1-INPUT -p udp -m udp --dport 69 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

### 3.5.4 CNR CCM [ /etc/sysconfig/iptables ] entries

```
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

#cnr-ccm
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 1234 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 1244 -j ACCEPT

-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 5480 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8090 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8443 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8453 -j ACCEPT
COMMIT
```

# 4 References


1. Redhat Documentation [url: http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/sect-Security_Guide-IPTables.html ]
2. Cisco PCP 5.0 Installation Guide [url: http://www.cisco.com/en/US/docs/net_mgmt/prime/cable_provisioning/5.0/quick/start/guide/quick_start_guide.html ]
3. Cisco PCP 5.0 User Guide [url: http://www.cisco.com/en/US/docs/net_mgmt/prime/cable_provisioning/5.0/user/guide/user_guide.html ]
4. Cisco PNR 8.1 Installation Guide [ http://www.cisco.com/en/US/partner/docs/net_mgmt/prime/network_registrar/8.1/installation/guide/CPNR_8_1_Install_Guide.html ]
5. Cisco PNR 8.1 User Guide [http://www.cisco.com/en/US/partner/docs/net_mgmt/prime/network_registrar/8.1/user/guide/CPNR_8_1_User_Guide.html]