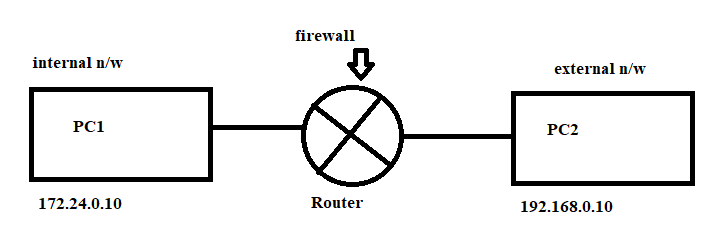
**Firewall Implementation**

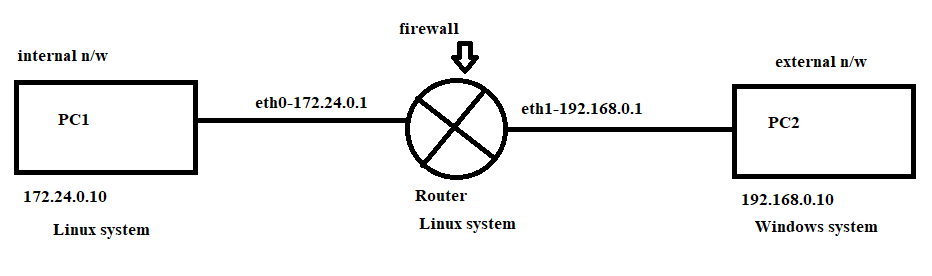


Input direction firewall

Note🡪 there are two directions of firewall (input and output) direction and one forward direction firewall which means router cannot be used as intermediate (banning of route).

Types of firewall…

* |chk point
* |Iptables (open source)



**Firstly, to make a Linux machine to act like a router firstly assign it two network IPs.**

If some problem takes place, then go to /etc/sysconfig/network-scripts

And rename the adapter as per your troubleshooting and then

|service network restart

**Routing using Linux system**

The routing file is placed in the following

|vi /etc/sysctl.conf configure it as

Routing forwarding on: 1

|sysctl -p

Now configure the gateway settings in client since it would be impossible for the client to determine that the packet would be traversing through the router.

|system-config-firewall

Enter the default Gateway IP and check the configuration by |route -n

Note🡪 troubleshooting: firewall of any system could be on.

Download several packages on Linux like telnet and SSh for remote desktop computing.

Task- implement the input direction firewall so that one machine could not ping the router.

|iptables -t filter -A INPUT -s 172.24.0.10 -p icmp -j DROP

|iptables -t <type> <to add/to del> <input/output> -s <source IP> -p <protocol> -jump <DROP>

Note🡪 ping uses the protocol ICMP (internet control message protocol)

Note🡪 since when ping takes place there is an acknowledgement packet also but when ping is blocked for an IP it is not possible to ping it back since ack packet will follow the same route therefore the following command is used…

|iptables -t filter -A INPUT -s 172.24.0.10 -p icmp –icmp-type echo-request -j DROP

**To block the web packet**

|Iptables -t filter -A OUTPUT -m tcp -p tcp -d 172.24.0.11 -j DROP

m stands for module

|Iptables -t filter -A OUTPUT -m tcp -p tcp -d 172.24.0.11 -dport 80 -j DROP