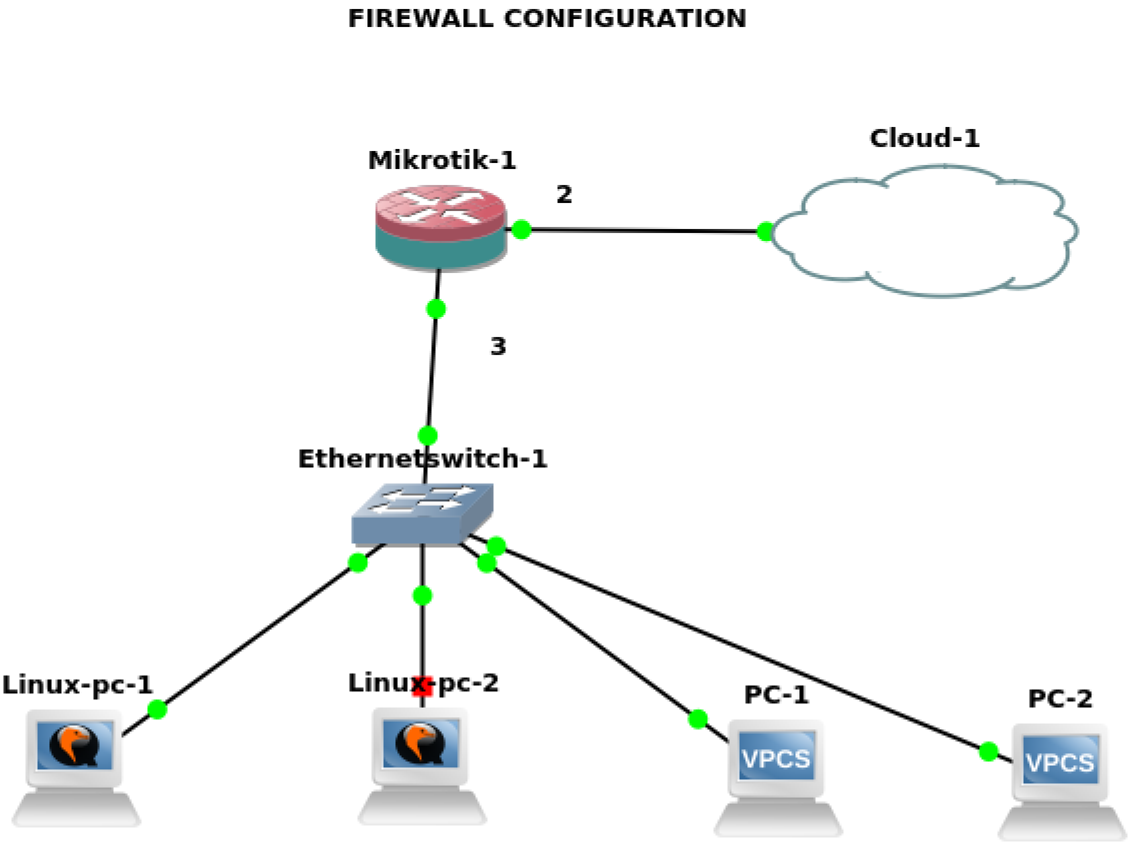
# MIKROTIK FIREWALL CONFIGURATION

## TARGET:

1) First make all the ip assigning make the routing and NAT and connect to the world (pre work)
2) connect all the 4 pc 2 are linux and 2 are VPCS
3) ip are

   **1→192.168.88.10**
   **2→192.168.88.11**
   **3→192.168.88.12**
   **4→192.168.88.13**

create a basic firewall rule to access onle first and second can access to the internet other cant connect even they are connected to the router.



Router configuration:

```
[admin@MikroTik] > ip address add address=10.42.0.99/24 interface=ether2
[admin@MikroTik] > ip address add address=192.168.88.1/24 interface=ether3
[admin@MikroTik] > ip route add gateway=10.42.0.1
[admin@MikroTik] > ip dns set servers=8.8.8.8
[admin@MikroTik] > ip firewall address-list add list=Allowed
address=192.168.88.10
[admin@MikroTik] > ip firewall address-list add list=Allowed
address=192.168.88.11
[admin@MikroTik] /ip firewall nat>
[admin@MikroTik] /ip firewall nat> add chain=srcnat src-address-
list=Allowed  action=masquerade
```

VPCS with ip address 192.168.88.10/24

```
PC-2> ip 192.168.88.10/24 192.168.88.1
Checking for duplicate address...
PC1 : 192.168.88.10 255.255.255.0 gateway 192.168.88.1

PC-2> ip dns 8.8.8.8

PC-2> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=116 time=143.448 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=116 time=96.479 ms
```

vpcs with 192.168.88.12/24 ip:

```
 PC-1> ip 192.168.88.12/24 192.168.88.1
Checking for duplicate address...
PC1 : 192.168.88.12 255.255.255.0 gateway 192.168.88.1
PC-1> ip dns 8.8.8.8
PC-1> ping 8.8.8.8

8.8.8.8 icmp_seq=1 timeout
8.8.8.8 icmp_seq=2 timeout
8.8.8.8 icmp_seq=3 timeout
8.8.8.8 icmp_seq=4 timeout
```

### Adding 192.168.88.11/24 ip in  a linux pc

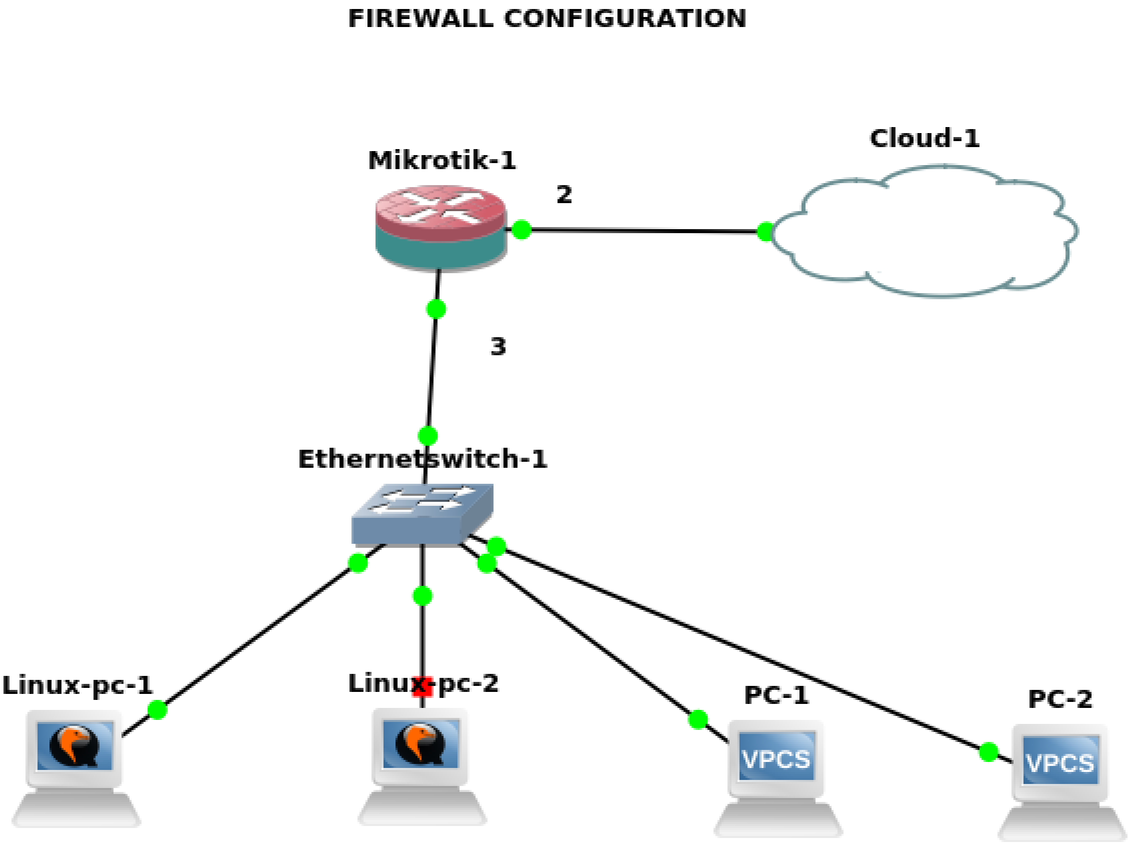
```
gns3@box:~$ sudo ip addr add 192.168.88.11/24 dev eth0
gns3@box:~$ sudo ip addr add 192.168.88.11/24 dev eth0
gns3@box:~$ sudo route add default gw 192.168.88.1
gns3@box:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=116 time=57.029 ms
64 bytes from 8.8.8.8: seq=1 ttl=116 time=55.171 ms
64 bytes from 8.8.8.8: seq=2 ttl=116 time=57.991 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 55.171/56.730/57.991 ms
```

## input firewall settings:

input chain states that the altering the request to the router from the WAN and LAN router can all do the things but we apply firewall so the WAN and Lan  cant do all the things

### Target:

we stop the icmp (internet control messaging protocol ) so the WAN and LAN cant get a ping request.but other internet service will run smoothly. only no one can discover the router with ping request



router configuration:

```
[admin@MikroTik] > ip address add address=10.42.0.99/24 interface=ether2
[admin@MikroTik] > ip address add address=192.168.88.1/24 interface=ether3
[admin@MikroTik] > ip route add gateway=10.42.0.1
[admin@MikroTik] > ip dns set servers=8.8.8.8
[admin@MikroTik] > ip firewall address-list add list=Allowed
address=192.168.88.10
[admin@MikroTik] > ip firewall address-list add list=Allowed
address=192.168.88.11
[admin@MikroTik] /ip firewall nat>
[admin@MikroTik] /ip firewall nat> add chain=srcnat action=masquerade
[admin@MikroTik] > ip firewall filter add chain=input protocol=icmp
action=drop
```

checking from VPCS:

```
PC-1> ip 192.168.88.10/24 192.168.88.1
Checking for duplicate address...
PC1 : 192.168.88.10 255.255.255.0 gateway 192.168.88.1

PC-1> ip dns 8.8.8.8
```

```
PC-1> ping yahoo.com
yahoo.com resolved to 98.138.219.232

84 bytes from 98.138.219.232 icmp_seq=1 ttl=49 time=288.155 ms
84 bytes from 98.138.219.232 icmp_seq=2 ttl=49 time=286.394 ms
```

//now ping the router

```
PC-1> ping 192.168.88.1

192.168.88.1 icmp_seq=1 timeout
192.168.88.1 icmp_seq=2 timeout
```

checking from the Linux PC:

```
gns3@box:~$ sudo ip addr add 192.168.88.13/24 dev eth0
gns3@box:~$ sudo route add default gw 192.168.88.1
gns3@box:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=116 time=54.832 ms
64 bytes from 8.8.8.8: seq=1 ttl=116 time=55.084 ms
```

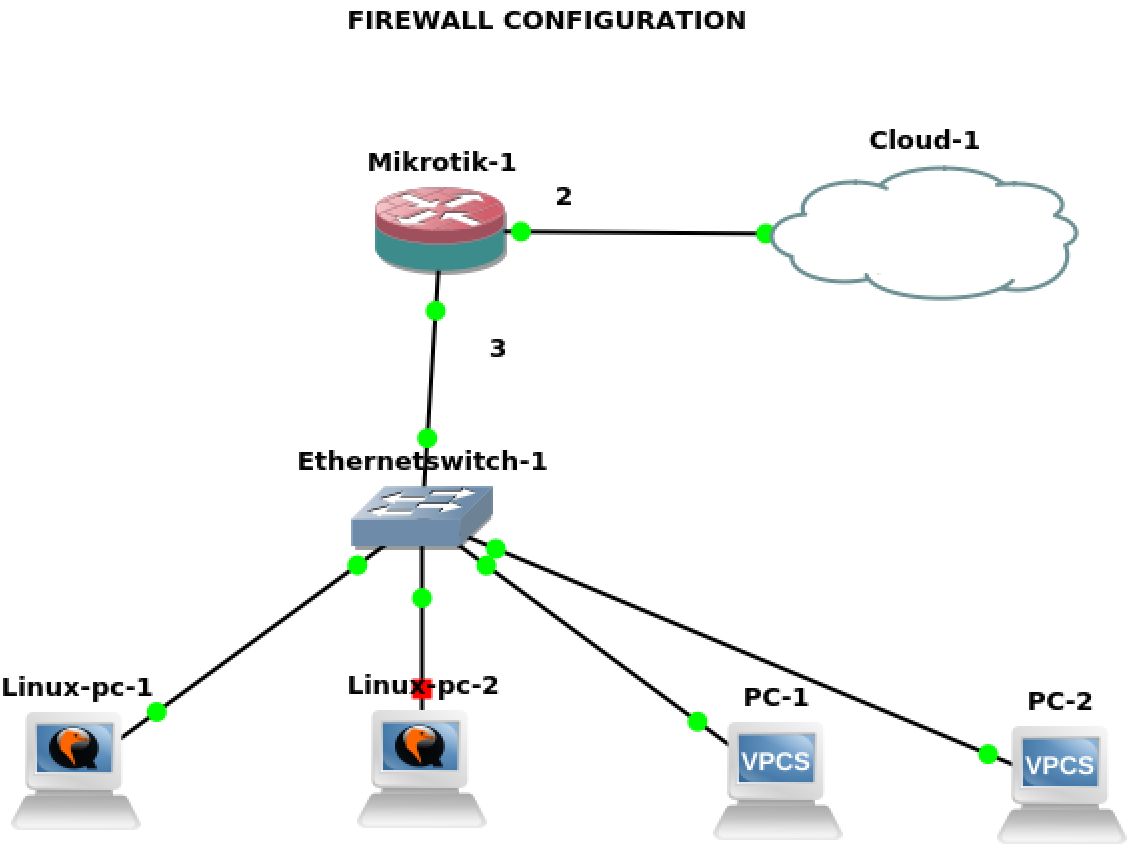
//now ping the router

```
gns3@box:~$ ping 192.168.88.1
PING 192.168.88.1 (192.168.88.1): 56 data bytes
^C
--- 192.168.88.1 ping statistics ---
10 packets transmitted, 0 packets received, 100% packet loss
```

//no ping

# forward chain firewall:

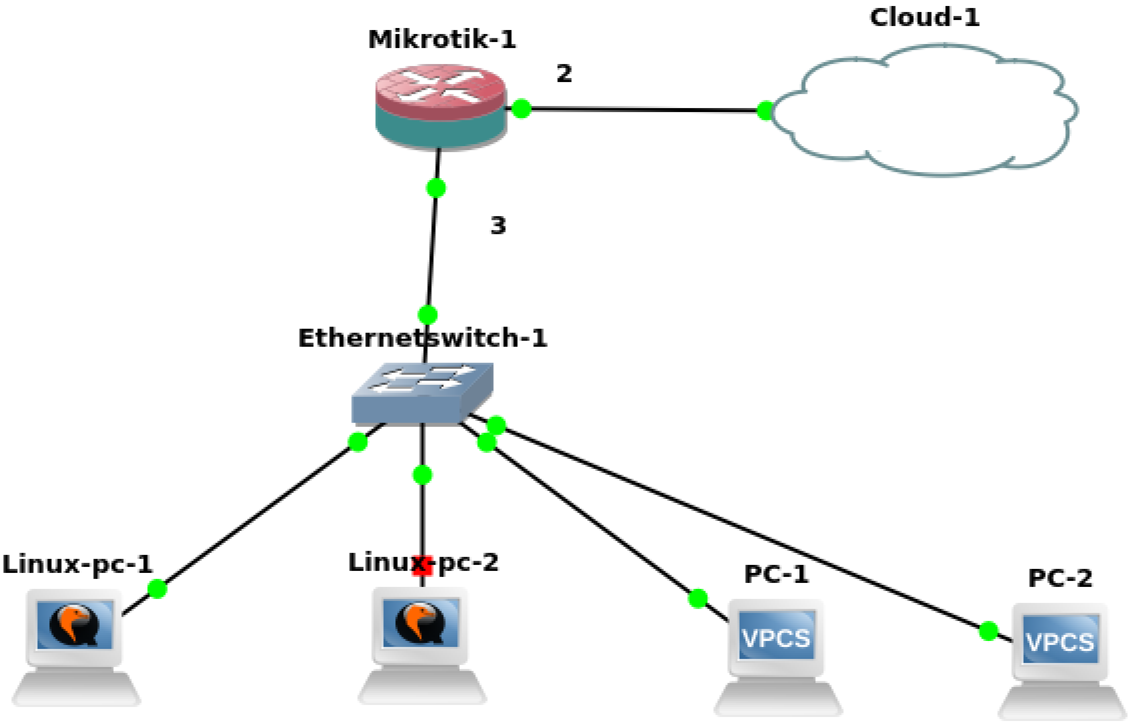
In forward firewall setting we controll the trafic that fo through via router LAN to router to WAM or WAN to router to LAN.



Target:

we try to block the facebok that has a request from the Linux pc of ip 192.168.88.10/24

## FIREWALL CONFIGURATION



router configuration:

---

```
[admin@MikroTik] > ip address add address=10.42.0.99/24 interface=ether2
[admin@MikroTik] > ip address add address=192.168.88.1/24 interface=ether3
[admin@MikroTik] > ip route add gateway=10.42.0.1
[admin@MikroTik] > ip dns set servers=8.8.8.8
[admin@MikroTik] > ip firewall address-list add list=Allowed address=192.168.88.10
[admin@MikroTik] > ip firewall address-list add list=Allowed address=192.168.88.11
[admin@MikroTik] /ip firewall nat>
[admin@MikroTik] /ip firewall nat> add chain=srcnat action=masquerade
```

adding dns

```
gns3@box:~$ vi /etc/resolv.conf
        nameserver 8.8.8.8
:wq
```

```
gns3@box:~$ tce-load -w -i appbrowser-cli.tcz
gns3@box:~$appbrowser-cli
```