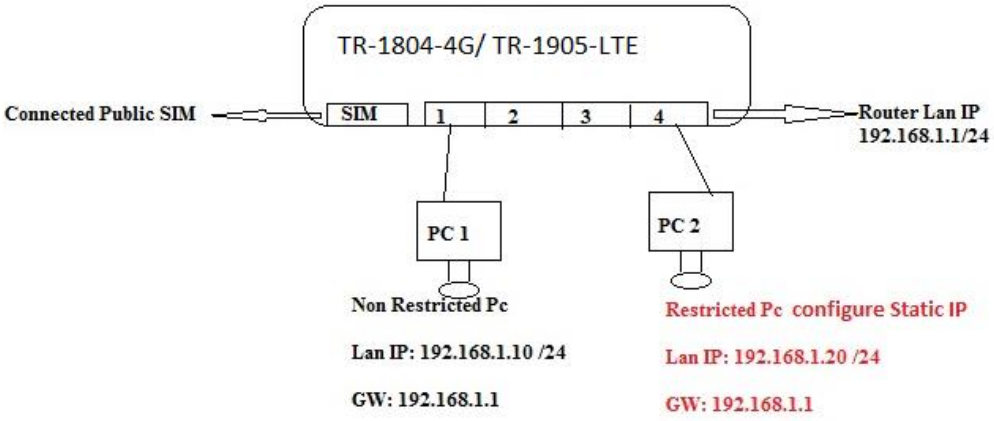


Topology

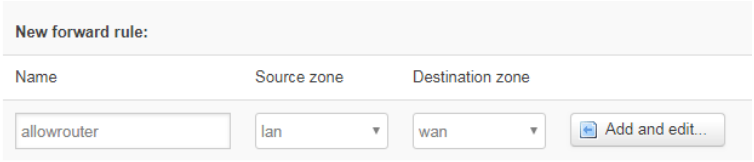
Test cases :-

1) If restricted PC when i given static IP, that time restricted pc can ping non-restricted PC & global internet dns also can ping. Similarly non restricted pc also can ping restricted pc static IP.

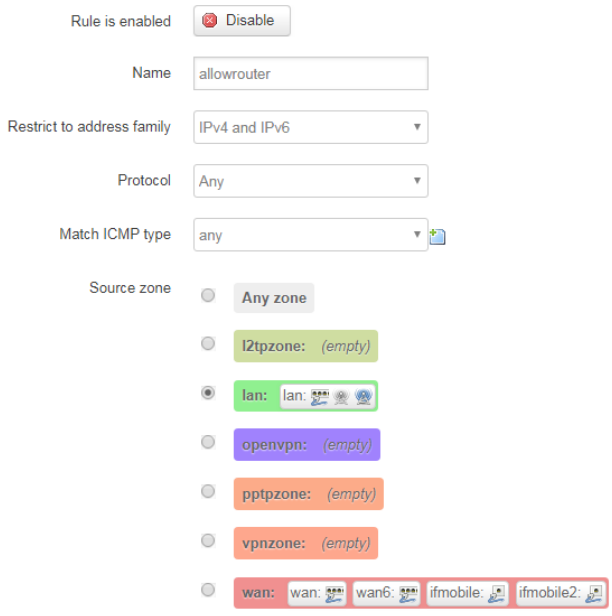
2) If in this case i create one policy (source mac any and source IP address any) for internet access that time restricted pc also can allowed internet access.

3) we need separately Create policy for every pc for internet allowed. (Please allow add multiple source mac and multiple source IP address in one policy).

1 Traffic rules, and then scroll down. Add new forward rule then click button Add and edit.

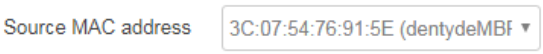


2 set protocol to Any



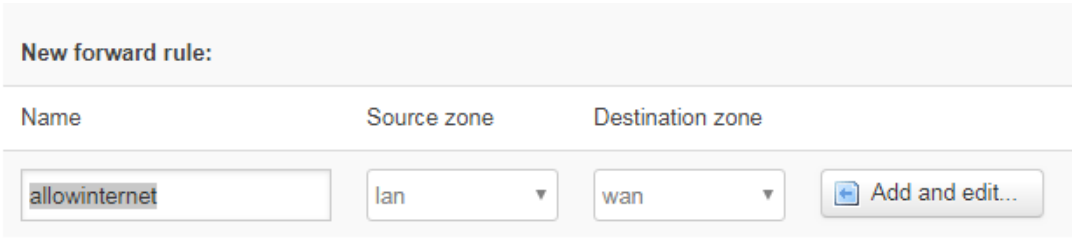
3 change destination zone to Device

4 set Source MAC address



5 save & apply

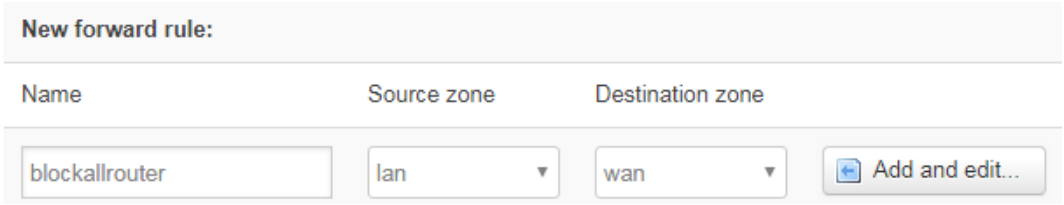
6 create new forward rules



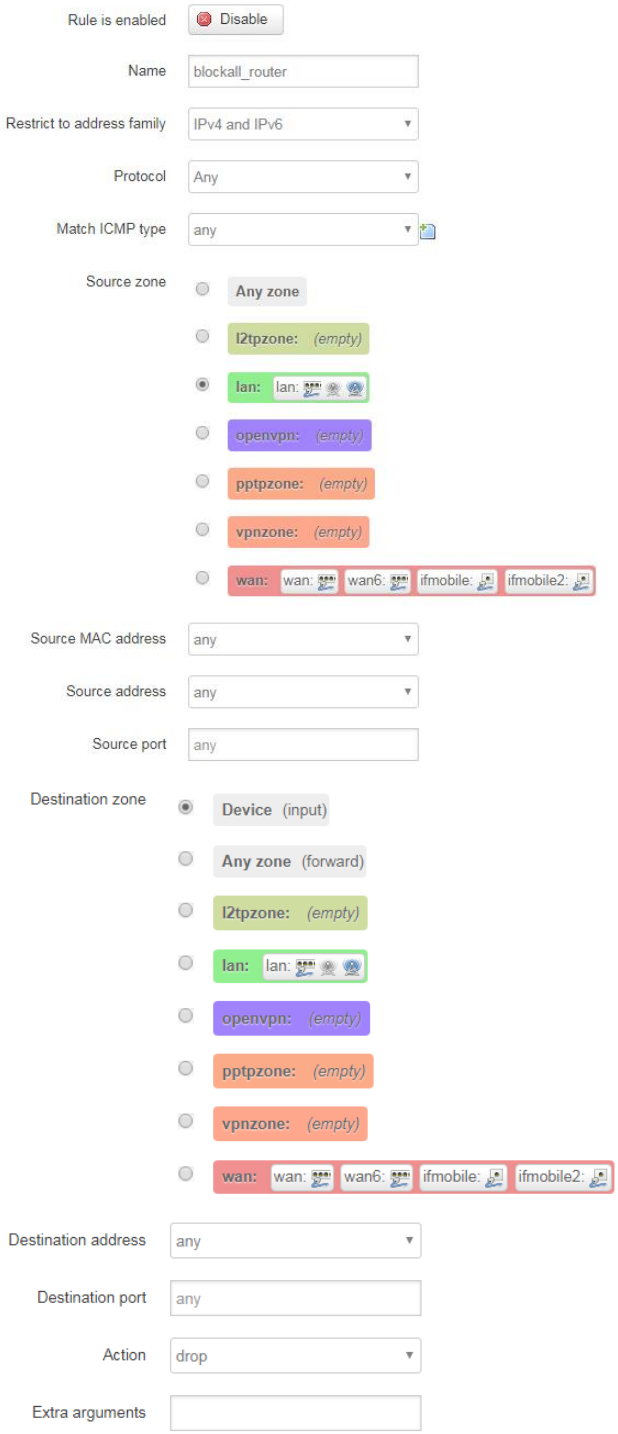
7 all configurations are same as rule allow router, except destination is Any zone

8 Repeat step1~7 if you want to allow any other MAC address to access router.

9 Create new forward rules to block all LAN access. Click add and edit.



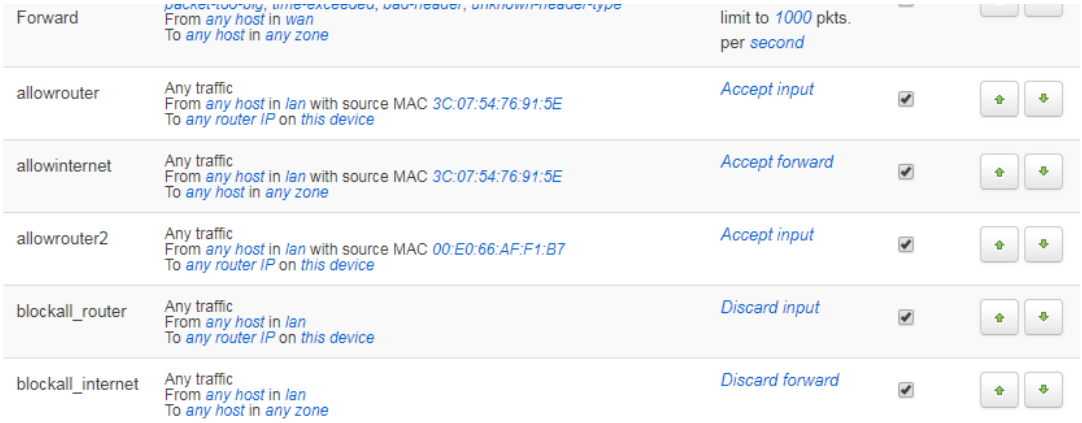
10 Set protocol to Any, destination zone to Device, action to drop. Then save &apply



11 Create rules to block all internet access, all configuration are same as rule block all router except destination is Any zone.


Firewall - Traffic Rules - blockall_internet
This page allows you to change advanced properties of the traffic rule entry, such as matched source and
Rule is enabled
Disable
Name
blockall_internet
Restrict to address family
IPv4 and IPv6
Protocol
Any
Match ICMP type
any
Source zone
Any zone
l2tpzone: (empty)
lan: lan:
openvpn: (empty)
pptpzone: (empty)
vpnzone: (empty)
wan: wan: wan6: ifmobile: ifmobile2:
Source MAC address
any
Source address
any
Source port
any
Destination zone
Device (input)
Any zone (forward)
l2tpzone: (empty)
lan: lan:
openvpn: (empty)
pptpzone: (empty)
vpnzone: (empty)
wan: wan: wan6: ifmobile: ifmobile2:
Destination address
any
Destination port
any
Action
drop
Extra arguments

12 Rule list



Forward	From *any host* in *wan* To *any host* in *any zone*	limit to *1000* pkts. per *second*		
allowrouter	Any traffic From *any host* in *lan* with source MAC *3C:07:54:76:91:5E* To *any router IP* on *this device*	*Accept input*	☑	↑ ↓
allowinternet	Any traffic From *any host* in *lan* with source MAC *3C:07:54:76:91:5E* To *any host* in *any zone*	*Accept forward*	☑	↑ ↓
allowrouter2	Any traffic From *any host* in *lan* with source MAC *00:E0:66:AF:F1:B7* To *any router IP* on *this device*	*Accept input*	☑	↑ ↓
blockall_router	Any traffic From *any host* in *lan* To *any router IP* on *this device*	*Discard input*	☑	↑ ↓
blockall_internet	Any traffic From *any host* in *lan* To *any host* in *any zone*	*Discard forward*	☑	↑ ↓

13 DO NOT create block all rules at first time, we must create allow router at beginning.