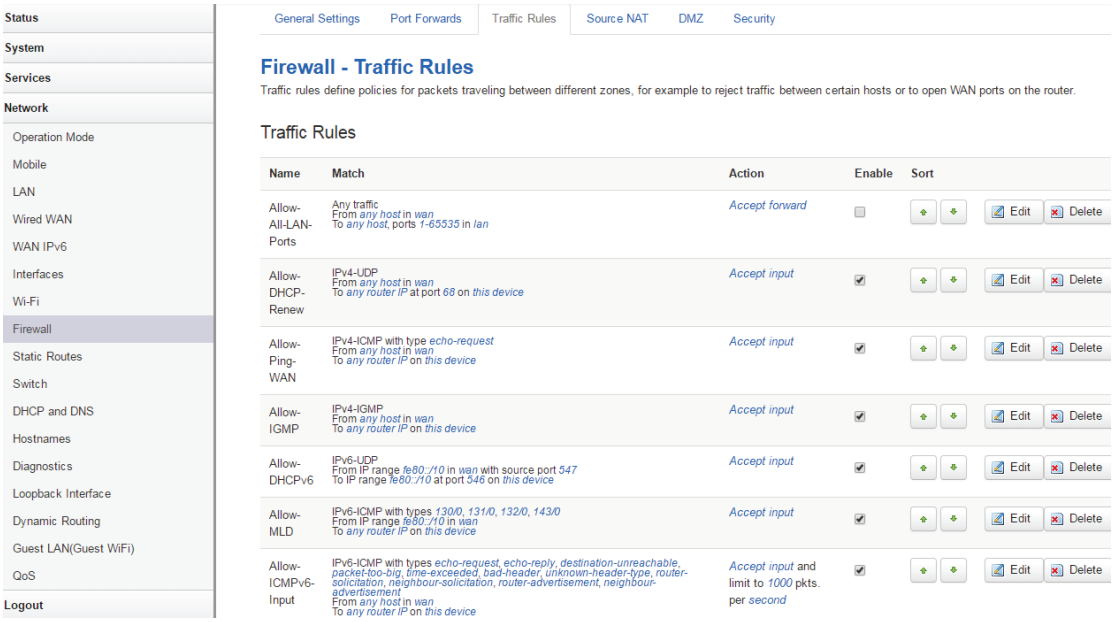
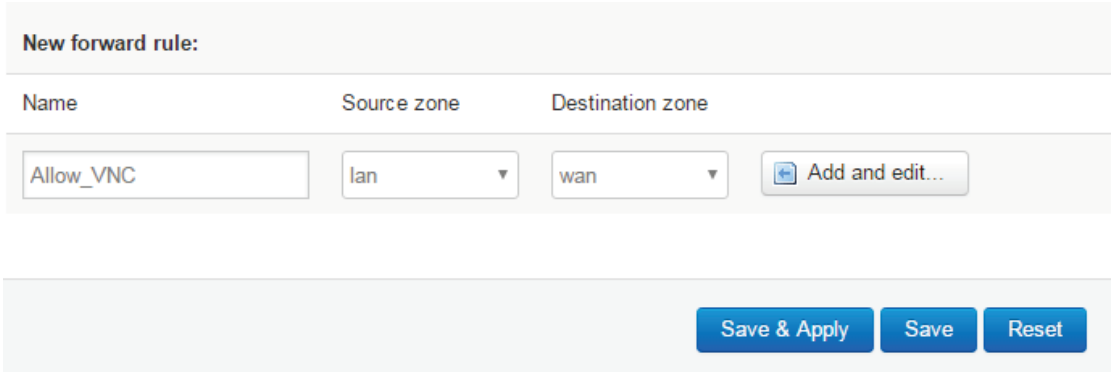
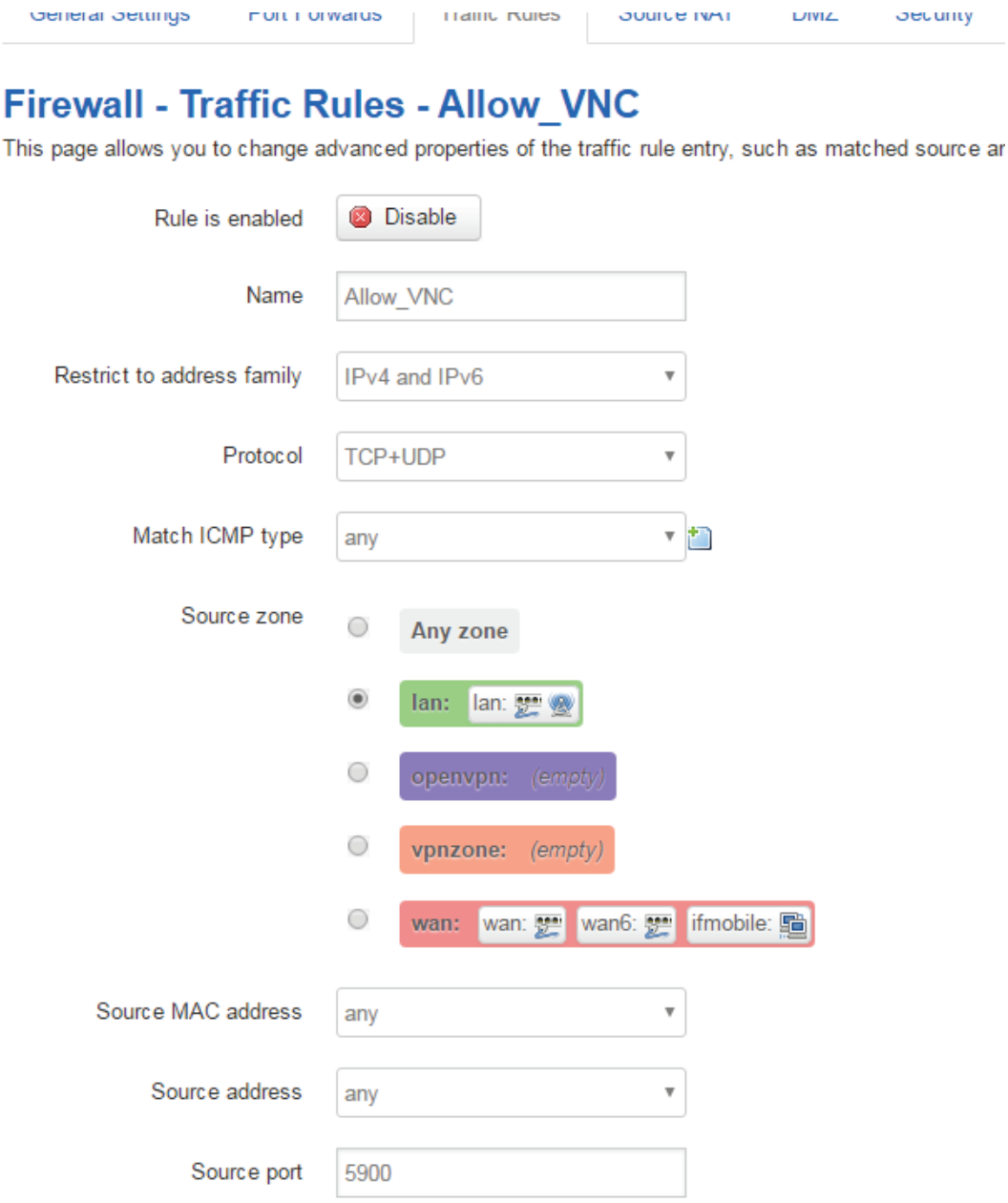
1. Open page Network→Firewall→Traffic Rules



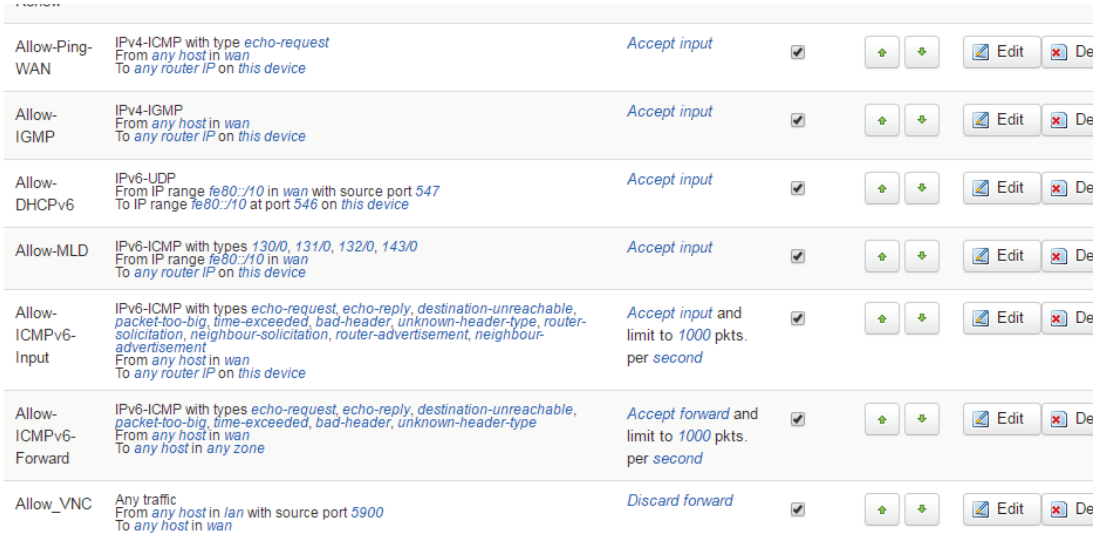
2. Scroll down, goto“New forward rule:”, configure it then click button “Add and edit…”



3. Configure “Source port” as 5900, Then click button “Save &Apply”

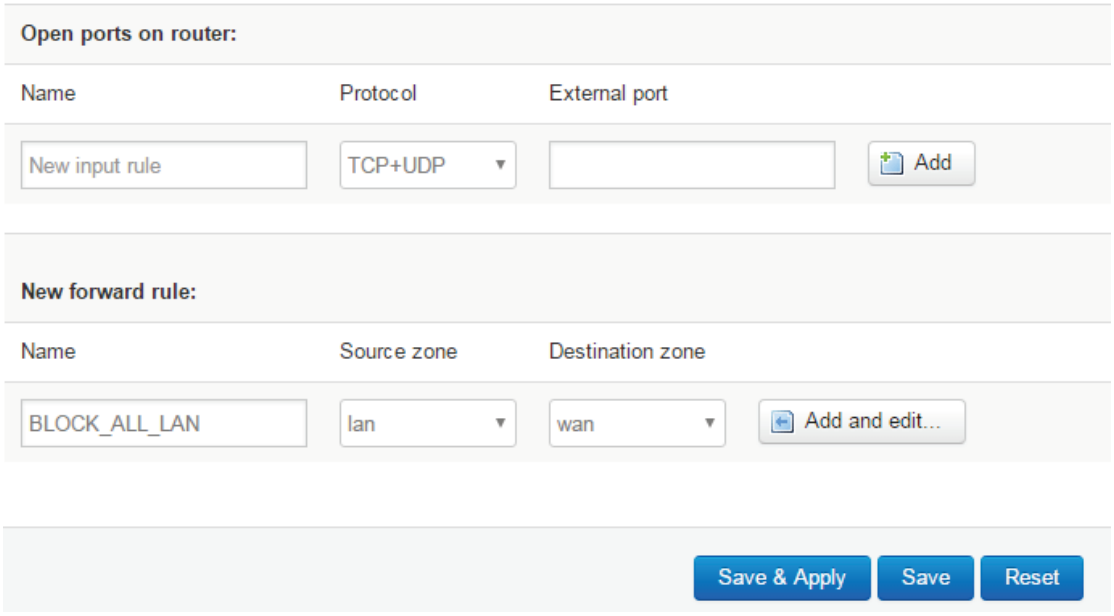


4. Then new rule at the bottom of the rule list.

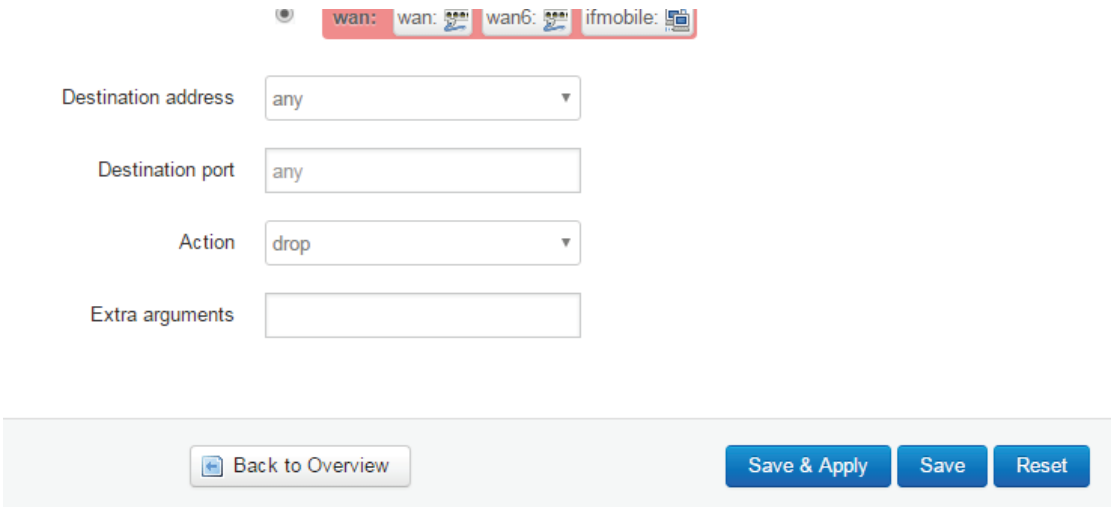


Allow-Ping-WAN	IPv4-ICMP with type *echo-request* From *any host* in *wan* To *any router IP* on *this device*	*Accept input*	☑	Edit De
Allow-IGMP	IPv4-IGMP From *any host* in *wan* To *any router IP* on *this device*	*Accept input*	☑	Edit De
Allow-DHCPv6	IPv6-UDP From IP range *fe80::/10* in *wan* with source port *547* To IP range *fe80::/10* at port *546* on *this device*	*Accept input*	☑	Edit De
Allow-MLD	IPv6-ICMP with types *130/0, 131/0, 132/0, 143/0* From IP range *fe80::/10* in *wan* To *any router IP* on *this device*	*Accept input*	☑	Edit De
Allow-ICMPv6-Input	IPv6-ICMP with types *echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-solicitation, router-advertisement, neighbour-advertisement* From *any host* in *wan* To *any router IP* on *this device*	*Accept input* and limit to *1000* pkts. per *second*	☑	Edit De
Allow-ICMPv6-Forward	IPv6-ICMP with types *echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type* From *any host* in *wan* To *any host* in *any zone*	*Accept forward* and limit to *1000* pkts. per *second*	☑	Edit De
Allow_VNC	Any traffic From *any host* in *lan* with source port *5900* To *any host* in *wan*	*Discard forward*	☑	Edit De

5. Create rules for port 465,587,as same as port 5900.
6. Create a rule to block all ports. Input the name as BLOCK_ALL_LAN, then click “Add and edit…”



7. change“Action”from accept to drop, then click button “Save & Apply”



8. The rule BLOCK_ALL_LAN MUST at the bottom of rule list. Since it disables all rules behind of BLOCK_ALL_LAN .