

1. Open page Network→Firewall→Traffic Rules

General Settings Port Forwards Traffic Rules Source NAT DMZ Security

Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Traffic Rules

Name	Match	Action	Enable	Sort		
Allow-All-LAN-Ports	Any traffic From any host in wan To any host, ports 1-65535 in lan	Accept forward	<input type="checkbox"/>	+	+	Edit Delete
Allow-DHCP-Renew	IPv4-UDP From any host in wan To any router IP at port 68 on this device	Accept input	<input checked="" type="checkbox"/>	+	+	Edit Delete
Allow-Ping-WAN	IPv4-ICMP with type echo-request From any host in wan To any router IP on this device	Accept input	<input checked="" type="checkbox"/>	+	+	Edit Delete
Allow-IGMP	IPv4-IGMP From any host in wan To any router IP on this device	Accept input	<input checked="" type="checkbox"/>	+	+	Edit Delete
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	<input checked="" type="checkbox"/>	+	+	Edit Delete
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	<input checked="" type="checkbox"/>	+	+	Edit Delete
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	<input checked="" type="checkbox"/>	+	+	Edit Delete

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

New forward rule:





Name	Source zone	Destination zone	
Allow_VNC	lan	wan	Add and edit...

Save & Apply Save Reset

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

Firewall - Traffic Rules - Allow_VNC

This page allows you to change advanced properties of the traffic rule entry, such as matched source ar

Rule is enabled	<input type="checkbox"/> Disable
Name	<input type="text" value="Allow_VNC"/>
Restrict to address family	<input type="text" value="IPv4 and IPv6"/>
Protocol	<input type="text" value="TCP+UDP"/>
Match ICMP type	<input type="text" value="any"/>
Source zone	<input type="radio"/> Any zone <input checked="" type="radio"/> lan: lan:  <input type="radio"/> openvpn: (empty) <input type="radio"/> vpnzone: (empty) <input type="radio"/> wan: wan:  wan6:  ifmobile: 
Source MAC address	<input type="text" value="any"/>
Source address	<input type="text" value="any"/>
Source port	<input type="text" value="5900"/>

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

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

Open ports on router:

Name	Protocol	External port	
<input type="text" value="New input rule"/>	TCP+UDP ▼	<input type="text"/>	Add

New forward rule:

Name	Source zone	Destination zone	
<input type="text" value="BLOCK_ALL_LAN"/>	lan ▼	wan ▼	Add and edit...

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

wan: wan: wan6: ifmobile:

Destination address

Destination port

Action

Extra arguments

[Back to Overview](#) [Save & Apply](#) [Save](#) [Reset](#)

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