EW500A0203 User Guide

Connect
Ideas.
Shape
solutions.

Sommario

Introduction ***3***

Hardware description ***3***

EW500A login and status ***4***

Step 1: Power On 4

Step 2: Connect to your computer 4

Step 3: Login 5

EW500A basic programming ***6***

Wired network 7

Mobile network 8

Wireless network 9

EW500A advanced programming ***10***

Firewall policies 10

Traffic rules 11

Port forwarding 13

Introduction

ESA EW500A series mobile wifi externder is a compact router mainly intended for Iot 4.0 applications.

It is based on a powerful 32 bits industrial communication processor and real time operating system Linux based.

It the ESA device portfolio it must be used in order to provide wifi or 3G/4G connectivity to the device that do not have integrated wifi peripherails for the internet connection.

Hardware description

- DC power supply (7.5v – 32v)
- RJ45 - LAN port connection
- RJ45 – WAN port connection
- 3G – 4G sim card slot
- Wifi client mode connection
- Wifi antenna
- 3G / 4G antenna

EW500A login and status

Step 1: Power On

Connect the power supply unit to the power connector (12V DC / 1.5 A) or any external power supply (7.5 V DC – 32 V DC).

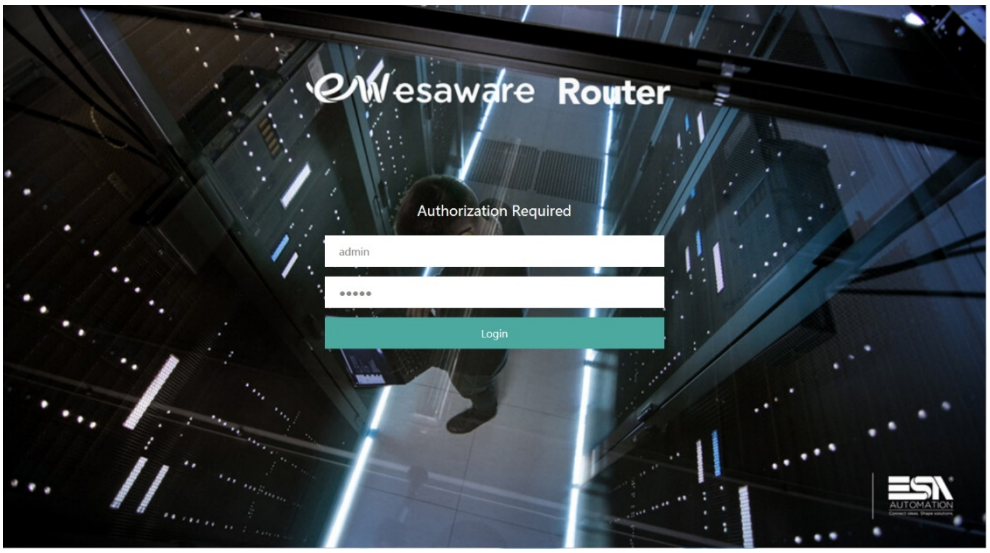
Step 2: Connect to your computer

Use a standard RJ45 ethernet cable to connect the LAN port to your computer ethernet port.

The router is equipped with a DHCP server so you can set DHCP support in your computer ethernet port setting.
The default Ip address of the EW500x LAN port is 196.168.1.1

Step 3: Login

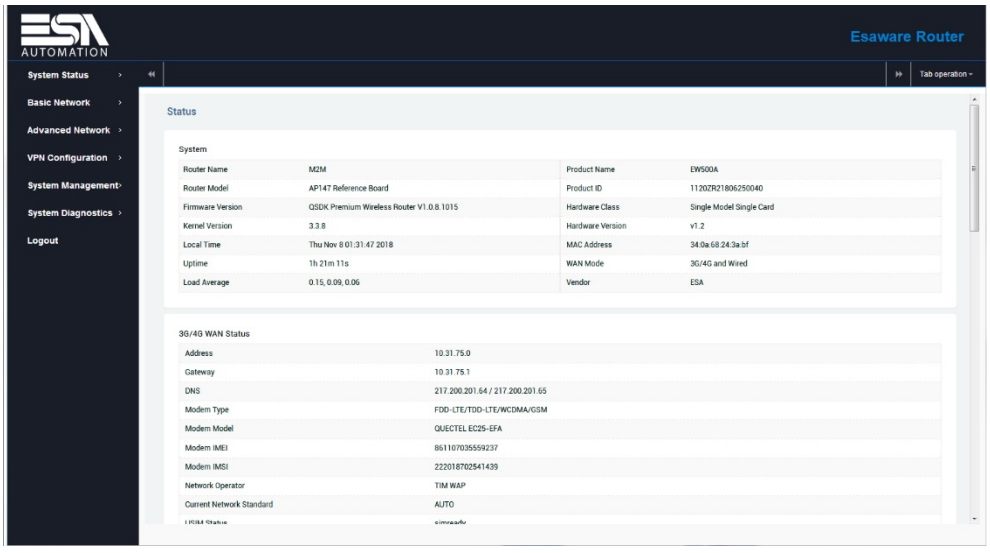
As soon as the ethernet connection is established the following login page is displayed:



The default login parameters are:

Username: admin
Password: admin

Once logged in the page below will be displayed:

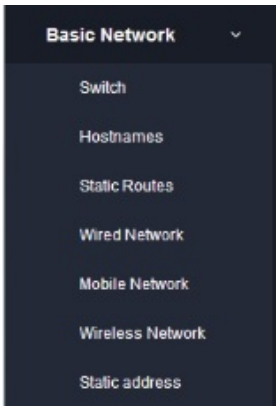


This page will show the current situation:

System informations
3G/4G WAN status
Wired WAN status
DHCP connections

EW500A basic programming

Open the Basic Network Menu in order to display the different connections parameters:

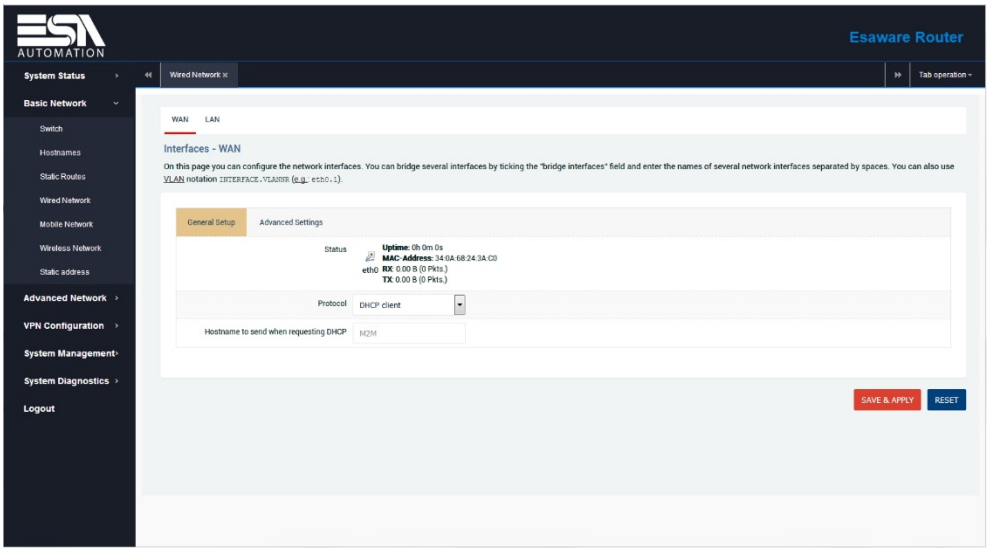


Here below the most important settings necessary for the different possible connections.

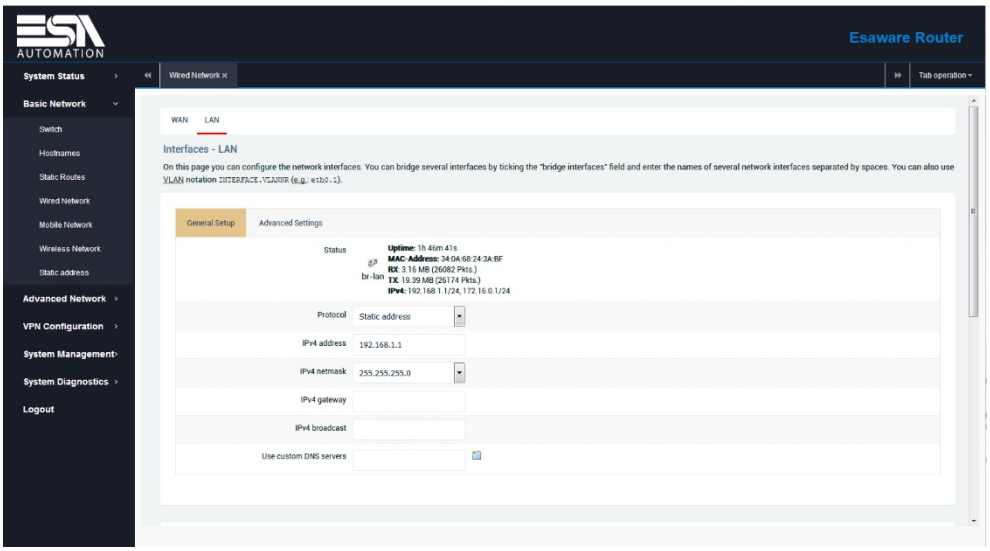
Wired network

The below page will be displayed with the parameter settings for both the WAN and LAN connections.

WAN:

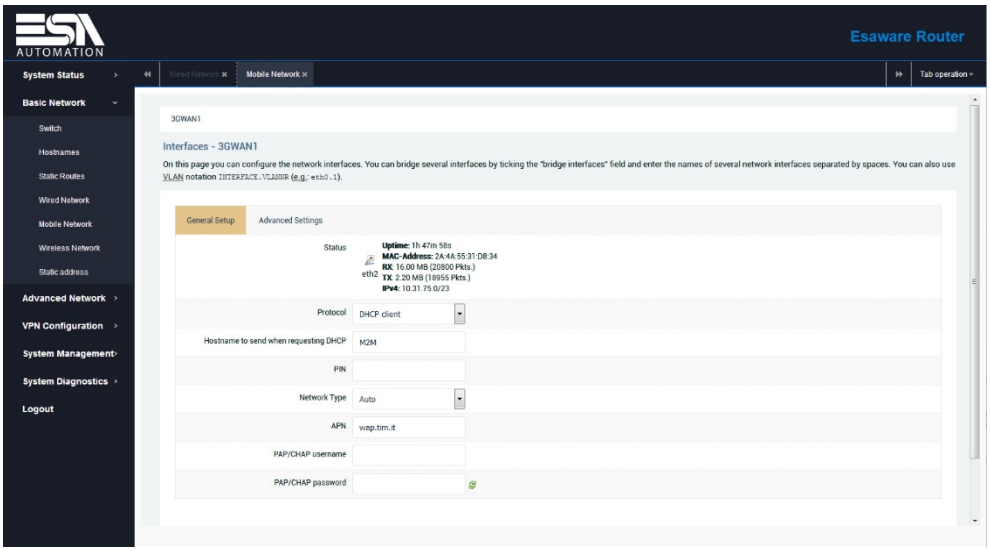


LAN:



Mobile network

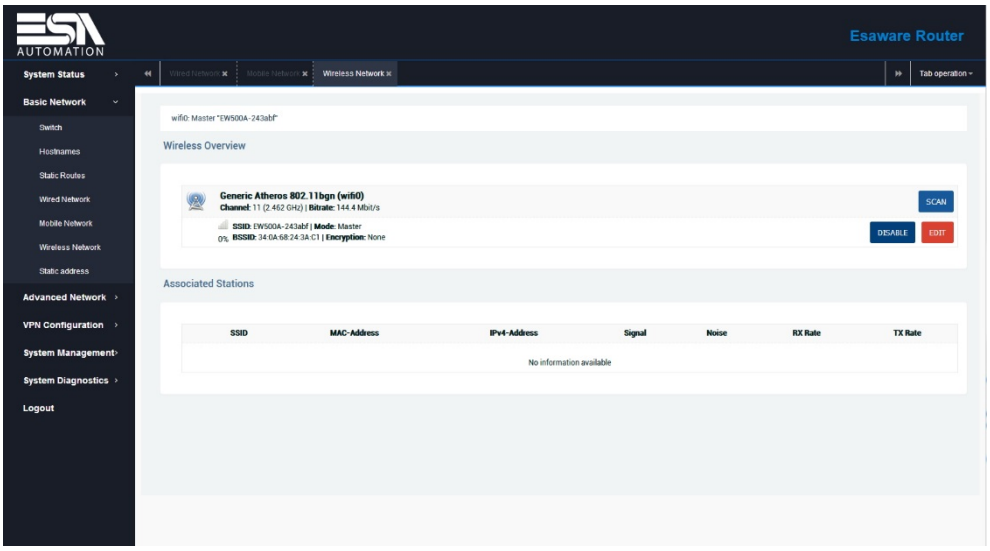
The below page does include all the setting parametrs necessary for a 3G / 4G mobile Network connection.



The 3G / 4G antenna must be connected to the 3G/4G connector.

Wireless network

The user can force a SCAN of the wifi connection available, select the one he wants to use and insert the connection password.

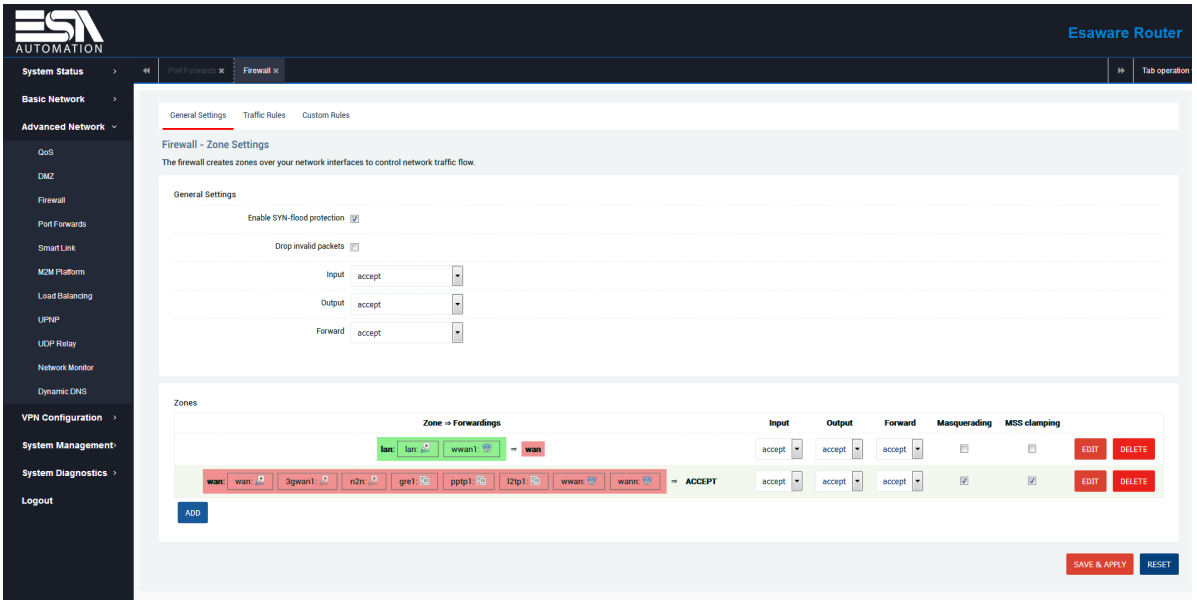


The wifi antenna must be connected to the Aux connector.

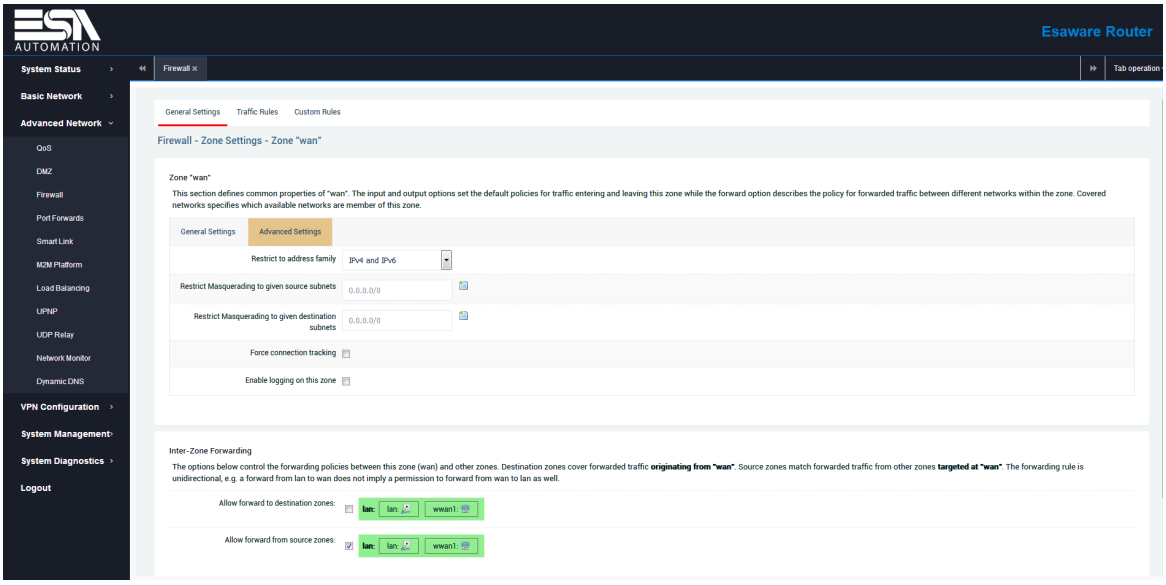
EW500A advanced programming

Firewall policies

In this section the user can define the product firewall policies.
This is necessary in case the EW500 is the entry point for the LAN internet connection.
The default configuration is intended in order to provide the default filtering configuration for a standard http or https support.



Here below the Advanced setting section where the user can define very strict firewall policies based on Ip address sorce and destinations and even log all the traffic.



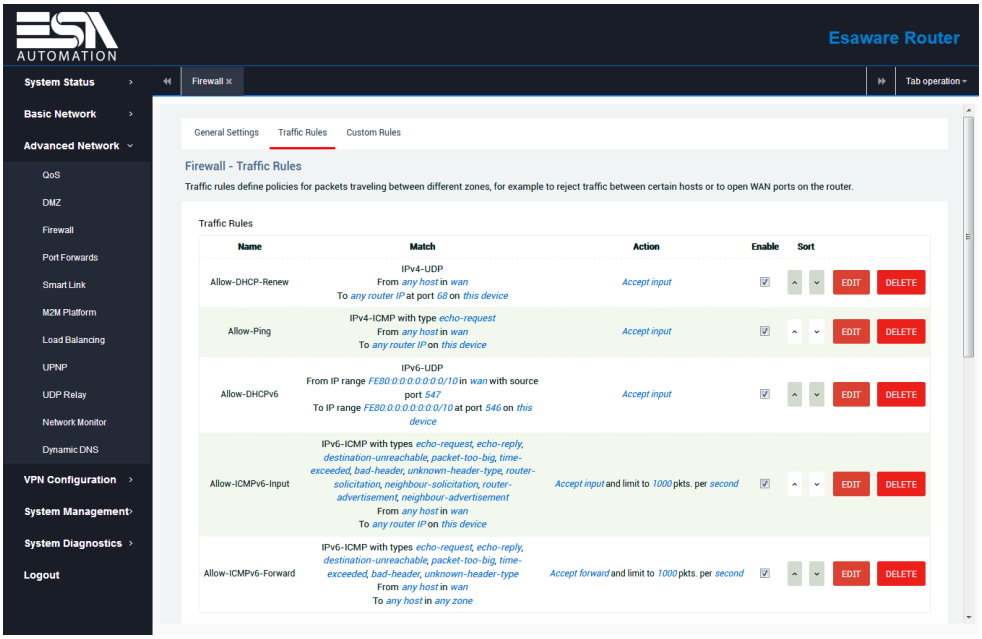
Traffic rules

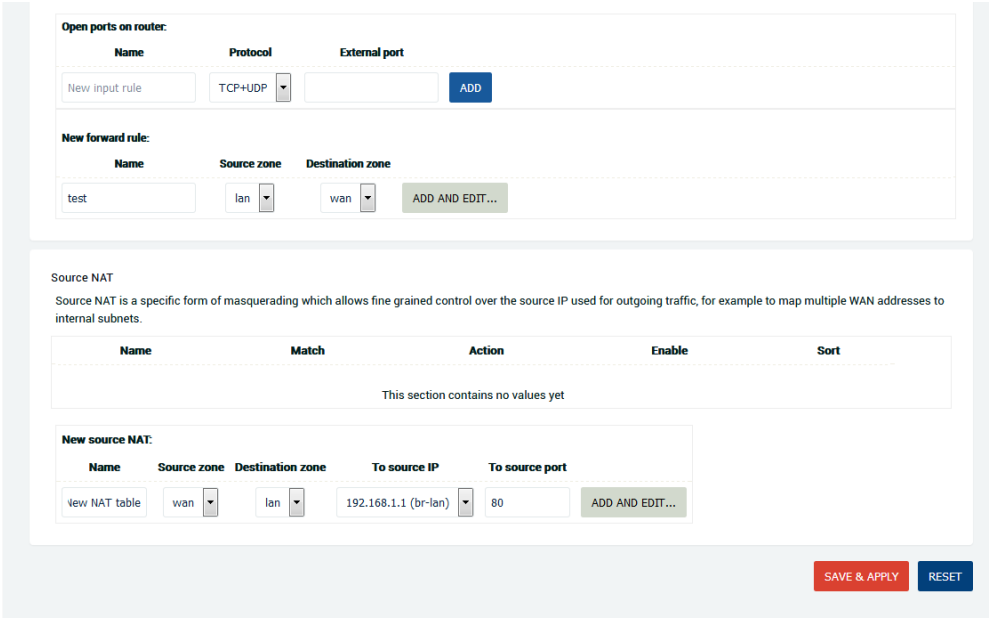
In this section the user is free to do some traffic restrictions in incoming and outgoing directions by clicking Add New Forward rules.

The restriction can be based on the following parameters:

Network port
Ip address
MAC address

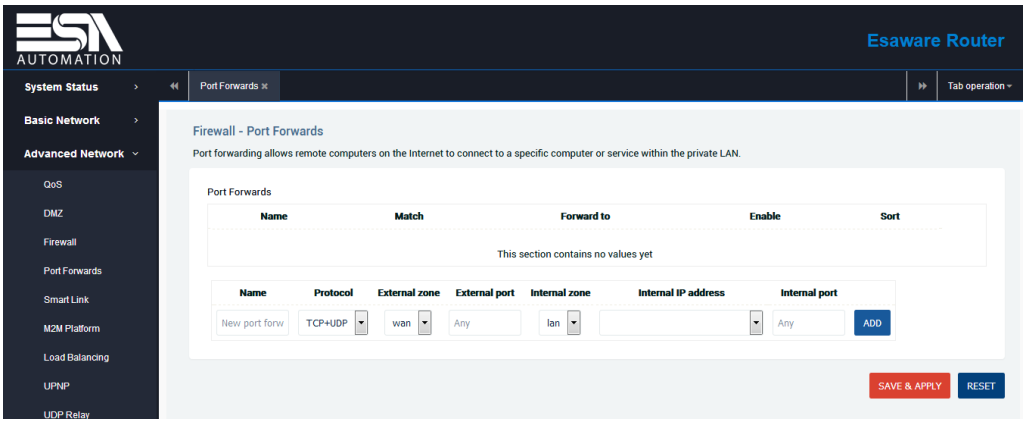
And also based on specific communication protocols.


AUTOMATION
Esaware Router
System Status
Basic Network
Advanced Network
QoS
DMZ
Firewall
Port Forwards
Smart Link
M2M Platform
Load Balancing
UPNP
UDP Relay
Network Monitor
Dynamic DNS
VPN Configuration
System Management
System Diagnostics
Logout
Firewall
Tab operation
General Settings
Traffic Rules
Custom Rules
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-DHCP-Renew
IPv4-UDP
From any host in wan
To any router IP at port 68 on this device
Accept input
EDIT
DELETE
Allow-Ping
IPv4-ICMP with type echo-request
From any host in wan
To any router IP on this device
Accept input
EDIT
DELETE
Allow-DHCPv6
IPv6-UDP
From IP range FE80:0:0:0:0:0:0:0/10 in wan with source port 547
To IP range FE80:0:0:0:0:0:0:0/10 at port 546 on this device
Accept input
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
EDIT
DELETE
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
DELETE

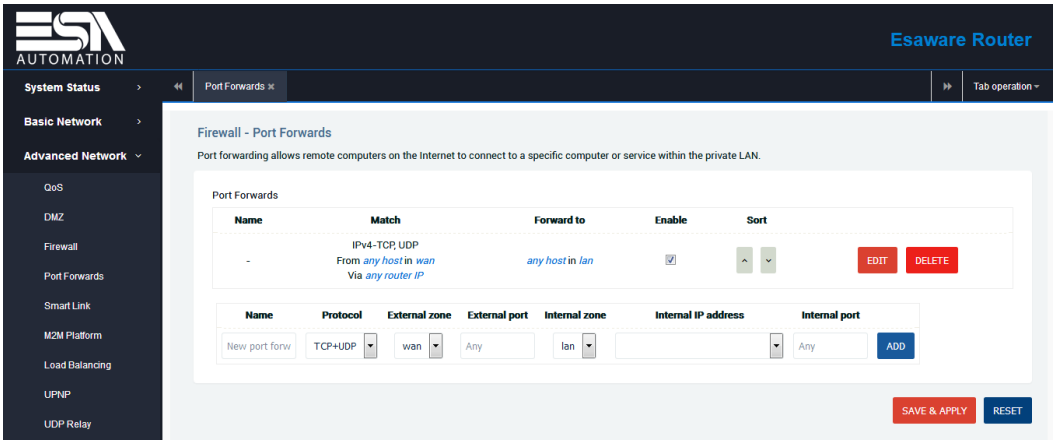

Open ports on router:
Name
Protocol
External port
New input rule
TCP+UDP
ADD
New forward rule:
Name
Source zone
Destination zone
test
lan
wan
ADD AND EDIT...
Source NAT
Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.
Name
Match
Action
Enable
Sort
This section contains no values yet
New source NAT:
Name
Source zone
Destination zone
To source IP
To source port
New NAT table
wan
lan
192.168.1.1 (br-lan)
80
ADD AND EDIT...
SAVE & APPLY
RESET

Port forwarding

The user can add port forwarding rules.
Port forwarding allows remote computers to connect a specific computer or service in the private LAN.



In case of more specific filtering required via the Edit button the user can create his own more precise configuration.



Connect
ideas.
shape
solutions.