https://wiki.teltonika-networks.com/view/RUT850_Firewall

RUT850 Firewall

□

Contents

Summary

RutOS uses a standard Linux iptables package as its **firewall**, which uses routing chains and policies to facilitate control over inbound and outbound traffic. This chapter is an overview of the Firewall section.

General Settings

The **General Settings** tab is used to configure the main policies of the device's firewall. The figure below is an example of the General Settings section and the table below provides information on the fields contained in that section:

field name	value	description
Drop invalid packets	yes | no; Default: **no**	A “Drop” action is performed on a packet that is determined to be invalid
Input	Reject | Drop | Accept; Default: **Accept**	Action* that is to be performed for packets that pass through the Input chain
Output	Reject | Drop | Accept; Default: **Accept**	Action* that is to be performed for packets that pass through the Output chain
Forward	Reject | Drop | Accept; Default: **Reject**	Action* that is to be performed for packets that pass through the Forward chain

***When a packet goes through a firewall chain it is matched against all the rules of that specific chain. If no rule matches said packet, an according Action (Drop, Reject or Accept) is performed**

Accept – packet gets to continue down to the next chain

Drop – packet is stopped and deleted

Reject – packet is stopped, deleted and, differently from Drop, an ICMP packet containing a message of rejection is sent to the source of the dropped packet

DMZ

By enabling **DMZ** for a specific internal host (e.g., your computer), you will expose that host and its services to the router’s WAN network (i.e. – the Internet).

field name	value	description
Source zone	yes | no; Default: **no**	Toggles DMZ On or Off
DMZ host IP address	ip; Default: " "	Internal host to which the DMZ rule will be applied

Zone Forwarding

A zone section groups one or more interfaces and serves as a source or destination for forwardings, rules and redirects. The **Zone Forwarding** section allows you to configure these forwardings.

field name	value	description

Source zone	gre: gre tunnel | hotspot: | l2tp: l2tp | pptp: pptp | vpn: openvpn | wan: ppp | lan: lan	The source zone from which data packets will redirected from
Destination zones	gre: gre tunnel | hotspot: | l2tp: l2tp | pptp: pptp | vpn: openvpn | wan: ppp | lan: lan	The destination zone to which data packets will be redirected to
Default forwarding action	Reject | Drop | Accept	Action to be performed with the redirected packets

Port Forwarding

The **Port Forwarding** window is used to set up servers and services on local LAN machines. Below is an overview of Port Forwarding default rules.

New Port Forward Rule

If none of the default rules suit your purposes, you can create custom rules using the **New Port Forward Rule** tab.

field name	value	description
Name	string; Default: " "	Name of the rule, used purely for easier management purposes
Protocol	TCP+UDP | TCP | UDP | ICMP | --custom --; Default: **TCP+UDP**	Type of protocol of incoming packet
External port	integer [0..65535] | range of integers [0..65534] - [1..65535]; Default: " "	Traffic will be forwarded from this port on the WAN network
Internal IP address	ip; Default: " "	The IP address of the internal machine that hosts some service that you want to access from the outside
Internal port	integer [0..65535] | range of integers [0..65534] - [1..65535]; Default: " "	The rule will redirect the traffic to this port on the internal machine

Once you have submitted the required information, click the **Add** button located in the New Port Forward Rule tab.

Port Forward Rule Configuration

To configure a Port Forward rule, click the **Edit** button located next to it. Below is a continuation of the previous New Port Forward Rule example, where we look at the configuration of the newly created rule.

field name	value	description
Enable	yes | no; Default: **no**	Toggles a rule ON or OFF
Name	string; Default: " "	The name of the rule. This is used for easier management purposes
Protocol	TCP+UDP | TCP | UDP | ICMP | -- custom --; Default: **TCP+UDP**	Specifies to which protocols the rule should apply
Source zone	gre: gre tunnel | hotspot: | l2tp: l2tp | pptp: pptp | vpn: openvpn | wan: ppp | lan: lan ; Default: **wan: ppp**	The source zone from which data packets will redirected from
Source MAC address	mac; Default: " "	Matches incoming traffic from these MACs only
Source IP address	ip; Default: " "	Matches incoming traffic from this IP or range of IPs only
Source port	integer [0..65535] | range of integers [0..65534] - [1..65535]; Default: " "	Matches incoming traffic originating from the given source port or port range on the client host only
External IP address	ip; Default: " "	Matches incoming traffic directed at the given IP address only
External port	integer [0..65535] | range of integers [0..65534] - [1..65535]; Default: " "	Specifies the external port, i.e., the port from which the third party is connecting
Internal zone	gre: gre tunnel | hotspot: | l2tp: l2tp | pptp: pptp | vpn: openvpn | wan: ppp | lan: lan ; Default: **lan: lan**	Specifies the internal zone, i.e., the zone where the incoming connection will be redirected to
Internal IP address	ip; Default: " "	Specifies the internal IP address, i.e., the IP address to which the incoming connection will be redirected to
Internal port	integer [0..65535] | range of integers [0..65534] - [1..65535]; Default: " "	Specifies the internal port, i.e., the port to which the incoming connection will be redirected to
Enable NAT loopback	yes | no; Default: **no**	NAT loopback enables your local network (i.e., behind your router/modem) to connect to a forward-facing IP address (such as 208.112.93.73) of a machine that it also on your local network
Extra arguments	string; Default: " "	Passes additional arguments to iptables. **Use with care!**

Traffic Rules

The **Traffic Rules** page contains a more generalized rule definition. With it you can block or open ports, alter how traffic is forwarded between LAN and WAN and many other things.

FIELD NAME	DESCRIPTION
Name	Name of the rule, used purely for easier management purposes
Protocol	Type of protocol of incoming packet
Source	The source zone from which data packets will redirected from
Destination	Redirect matched traffic to the given IP address and destination port
Action	Action to be performed with the packet if it matches the rule
Enable	Toggles the rule ON or OFF. If unchecked, the rule will not be deleted, but it also will not be loaded into the firewall
Sort	When a packet arrives, it gets checked for a matching rule. If there are several matching rules, only the first one is applied, i.e., the order of the rule list impacts how your firewall operates, therefore you are given the ability to sort your list however you deem fit

Traffic Rule Configuration

To customize a Traffic Rule, click the **Edit** button located next to it. This way you can fine tune a rule to near perfection, if you should desire that. The figure below is an example of the "Allow-DHCP-Relay" default rule editing. All rules are configured in an identical manner but with different settings.

field name	value	description
Enable	yes | no; Default: **no**	Turns the rule ON or OFF
Name	string; Default: " "	The name of the rule. This is used for easier management purposes
Restrict to address family	IPv4 and IPv6 | IPv4 only | IPv6 only; Default: **IPv4 and IPv6**	Name of the rule, used purely for easier management purposes
Protocol	TCP+UDP | TCP | UDP | ICMP | -- custom --; Default: **TCP+UDP**	Specifies to which protocols the rule should apply
Source zone	gre: gre tunnel | hotspot: | l2tp: l2tp | pptp: pptp | vpn: openvpn | wan: ppp | lan: lan ; Default: **wan: ppp**	Specifies the external zone, i.e., the zone from which the third party connection will come
Source MAC address	mac; Default: " "	Specifies the mac address of the external host, i.e., the rule will apply only to hosts that have the MAC addresses specified in this field
Source IP address	ip; Default: " "	Specifies the IP address or range of IPs of the external host, i.e., the rule will apply only to hosts that have the IP addresses specified in this field
Source port	integer [0..65535] | range of integers [0..65534] - [1..65535]; Default: " "	Specifies the port or range of ports that the external host host will using as their source, i.e., the rule will apply only to hosts that use source ports specified in this field
External IP address	ip | ip/netmask | ANY; Default: **ANY**	Specifies the external IP address or range of external IPs of the local host, i.e., the rule will apply only to the external IP addresses specified in this field

External port	integer [0..65535] | range of integers [0..65534] - [1..65535]; Default: " "	Specifies the external port, i.e., the port from which the third party is connecting
Destination zone	gre: gre tunnel | hotspot: | l2tp: l2tp | pptp: pptp | vpn: openvpn | wan: ppp | lan: lan ; Default: **lan: lan**	Match forwarded traffic to the given destination zone only
Destination address	ip; Default: " "	Match forwarded traffic to the given destination IP address or IP range only
Destination port	integer [0..65535] | range of integers [0..65534] - [1..65535]; Default: " "	Match forwarded traffic to the given destination port or port range only
Action	Drop | Accept | Reject | Don't track; Default: **no**	Action to be taken on the packet if it matches the rule. You can also define additional options like limiting packet volume, and defining to which chain the rule belongs. **Don't track** - connections with the specified parameters will not be monitored by the Firewall, i.e., no other Firewall rules will be applied to the specified configuration
Extra arguments	string; Default: " "	Adds extra options (specified in this field) to the rule

Open Ports On Router

Open Ports On Router rules can open certain ports and redirect hosts connecting to the router from specified zones to specified ports.

field name	value	description
NAME	string; Default: " "	The name of the rule. This is used for easier management purposes. The NAME field auto-filled when port numbers are specified, unless the NAME was specified beforehand by the user
PROTOCOL	TCP+UDP | TCP | UDP | Other; Default: **TCP+UDP**	Specifies to which protocols the rule should apply
EXTERNAL PORT	integer [0..65535] | range of integers [0..65534] - [1..65535]; Default: " "	Specifies which port should be opened

New Forward Rule

New Forward Rules lets you create custom zone forwarding rules

field name	value	description
Name	string; Default: " "	Name of the rule, used purely for easier management purposes
Source	GRE | HOTSPOT | L2TP | LAN | PPTP | VPN | WAN; Default: **LAN**	Match incoming traffic from selected address family only
Destination	GRE | HOTSPOT | L2TP | LAN | PPTP | VPN | WAN; Default: **WAN**	Forward incoming traffic to selected address family only

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.

field name	value	description
Name	string; Default: " "	Name of the rule, used purely for easier management purposes
Protocol	TCP+UDP | TCP | UDP | Other...; Default: **TCP+UDP**	Protocol of the packet that is being matched against traffic rules
Source	GRE | HOTSPOT | L2TP | LAN | PPTP | VPN | WAN; Default: **LAN**	Match incoming traffic from selected address family only
Destination	GRE | HOTSPOT | L2TP | LAN | PPTP | VPN | WAN; Default: **LAN**	Forward incoming traffic to selected address family only
SNAT	ip and port [0..65535]; Default: " "	SNAT (Source Network Address Translation) rewrites packet's source IP address and port
Enable	yes | no; Default: **no**	Toggles the rule ON or OFF

Custom Rules

The Custom Rules page provides ultimate freedom in defining your own rules – you can enter them straight into the **iptables** program. Just type a rule into the text field ant it will get executed as a Linux shell script. If you are unsure of how to use iptables, we advise that you consult with an expert or check the Internet for manuals, examples and explanations.

DDOS Prevention

The **DDOS Prevention** page allows you to set up protections from various types of DDOS attacks. You will find information on all of these methods bellow.

SYN Flood Protection

SYN Flood Protection allows you to protect yourself from attacks that exploit part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive. Essentially, with SYN flood DDOS, the offender sends TCP connection requests faster than the targeted machine can process them, causing network over-saturation.

field name	value	description
Enable SYN flood protection	yes | no; Default: **yes**	Toggles the rule ON or OFF
SYN flood rate	integer; Default: **25**	Set rate limit (packets per second) for SYN packets above which the traffic is considered flooded
SYN flood burst	integer; Default: **50**	Set burst limit for SYN packets above which the traffic is considered flooded if it exceeds the allowed rate
TCP SYN cookies	yes | no; Default: **no**	Enable the use of SYN cookies (particular choices of initial TCP sequence numbers by TCP servers)

Remote ICMP Requests

Some attackers use **ICMP echo** request packets directed to IP broadcast addresses from remote locations to generate denial-of-service attacks. You can set up some custom restrictions to help protect your router from ICMP bursts.

field name	value	description
Enable ICMP requests	yes | no; Default: **yes**	Toggles the rule ON or OFF
Enable ICMP limit	yes | no; Default: **no**	Toggles ICMP echo-request limit in selected period ON or OFF
Limit period	Second | Minute | Hour | Day; Default: **Second**	Select ICMP echo-request period limit
Limit	integer; Default: **10**	Maximum ICMP echo-request number during the period
Limit burst	integer; Default: **5**	Indicate the maximum burst before the above limit kicks in

SSH Attack Prevention

Prevent SSH (allows a user to run commands on a machine's command prompt without them being

physically present near the machine) attacks by limiting connections in a defined period.

field name	value	description
Enable SSH limit	yes | no; Default: **yes**	Toggles the rule ON or OFF
Limit period	Second | Minute | Hour | Day; Default: **Second**	The period in which SSH connections are to be limited
Limit	integer; Default: **10**	Maximum SSH connections during the set period
Limit burst	integer; Default: **5**	Indicate the maximum burst before the above limit kicks in

HTTP Attack Prevention

An HTTP attack sends a complete, legitimate HTTP header, which includes a 'Content-Length' field to specify the size of the message body to follow. However, the attacker then proceeds to send the actual message body at an extremely slow rate (e.g. 1 byte/100 seconds.) Due to the entire message being correct and complete, the target server will attempt to obey the 'Content-Length' field in the header, and wait for the entire body of the message to be transmitted, hence slowing it down.

field name	value	description
Enable HTTP limit	yes | no; Default: **yes**	Toggles the rule ON or OFF
Limit period	Second | Minute | Hour | Day; Default: **Second**	The period in which HTTP connections are to be limited
Limit	integer; Default: **10**	Maximum HTTP connections during the set period
Limit burst	integer; Default: **10**	Indicate the maximum burst before the above limit kicks in

HTTPS Attack Prevention

This section allows you to enable protection against **HTTPS** attacks, also known as **man-in-the-middle attacks** (**MITM**).

In cryptography and computer security, a man-in-the-middle attack (MITM) is an attack where the perpetrator secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. One example of man-in-the-middle attacks is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

field name	value	description
Enable HTTPS limit	yes | no; Default: **yes**	Toggles the rule ON or OFF
Limit period	Second | Minute | Hour | Day; Default: **Second**	The period in which HTTPS connections are to be limited
Limit	integer; Default: **10**	Maximum HTTPS connections during the set period
Limit burst	integer; Default: **10**	Indicate the maximum burst before the above limit kicks in

Port Scan Prevention

Port scan attacks scan which of the targeted host's ports are open. Network ports are the entry points to a machine that is connected to the Internet. A service that listens on a port is able to receive data from a client application, process it and send a response back. Malicious clients can sometimes exploit vulnerabilities in the server code so they gain access to sensitive data or execute malicious code on the machine remotely.

Port Scan

Port scanning is usually done in the initial phase of a penetration test in order to discover all network entry points into the target system. The Port Scan section provides you with the possibility to enable protection against port scanning software.

field name	value	description
Enable	yes | no; Default: **yes**	Toggles the function ON or OFF
Interval	integer [10..60]; Default: **30**	Time interval in seconds in which port scans are counted
Scan count	integer [5..65534]; Default: **10**	How many port scans before blocked

Defending Type

The Defending Type section provides the possibility for the user to enable protections from certain types of online attacks. These include **SYN-FIN**, **SYN-RST**, **X-Mas**, **FIN scan** and **NULLflags** attacks.

field name	value	description
SYN-FIN attack	yes | no; Default: **no**	Toggles protection from SYN-FIN attacks ON or OFF
SYN-RST attack	yes | no; Default: **no**	Toggles protection from SYN-RST attacks ON or OFF
X-Mas attack	yes | no; Default: **no**	Toggles protection from X-Mas attacks ON or OFF
FIN scan	yes | no; Default: **no**	Toggles protection from FIN scan attacks ON or OFF
NULLflags attack	yes | no; Default: **no**	Toggles protection from NULLflags attacks ON or OFF

Helpers

The **NAT Helpers** section provides you the option to add firewall exceptions for some VoIP protocols, namely SIP and H.323. In other words, these functions provide a pass-through for VoIP communications between the router's LAN and WAN.

Technical explanation:

FTP, SIP and H.323 protocols are harder to filter by firewalls since they violate layering by introducing OSI layer 3/4 parameters in the OSI layer 7. NAT helpers are modules that are able to assist the firewall in tracking these protocols. These helpers create the so-called expectations that can be used to open necessary ports for RELATED connections. For example: FTP, GRE and PPTP helpers are enabled by default.

field name	value	description
H323	yes | no; Default: **no**	Toggles H323 filtering ON or OFF
SIP	yes | no; Default: **no**	Toggles SIP filtering ON or OFF

[[Category:{{{name}}} Network section]]