RUTM50 Firewall

The information in this page is updated in accordance with firmware version **RUTM_R_00.07.08**.

□

Contents

Summary

RUTM50 devices use a standard Linux iptables package as its **firewall**, which uses routing chains

and policies to facilitate control over inbound and outbound traffic.

This chapter of the user manual provides an overview of the Firewall page for RUTM50 devices.

If you're having trouble finding this page or some of the parameters described here on your device's WebUI, you should **turn on "Advanced WebUI" mode**. You can do that by clicking the "Advanced" button, located at the top of the WebUI.

General Settings

The **General Settings** section 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	Value	Description
Drop invalid packets	off | on; default: **off**	If enabled, a "Drop" action will be performed on packets that are determined to be invalid.
Automatic helper assignment	off | on; default: **on**	Automatically assigns conntrack helpers based on traffic protocol and port. If turned off, conntrack helpers can be selected for each zone.
Input	Reject | Drop | Accept; default: **Reject**	Default action* of the INPUT chain if a packet does not match any existing rule on that chain.
Output	Reject | Drop | Accept; default: **Accept**	Default action* of the OUTPUT chain if a packet does not match any existing rule on that chain.
Forward	Reject | Drop | Accept; default: **Reject**	Default action* of the FORWARD chain if a packet does not match any existing rule on that 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 to the next chain.
- **Drop** – packet is stopped and deleted.
- **Reject** – packet is stopped, deleted and, differently from Drop, a message of rejection is sent to the source from which the packet came.

Routing/NAT Offloading

The **Routing/NAT Offloading** is used to turns software flow offloading on or off.

The device checks whether the flow (sequence of related packets) is of a received a packed is known. Packets of unknown flow are forwarded to the networking stack. Meanwhile, if the flow is known, NAT is applied (if matched) and the packet is forwarded to the correct destination port. This process is called **software flow offloading**. **Hardware flow offloading** is used to execute

functions of the router using the hardware directly, instead of a process of software functions.

Field	Value	Description
Software flow offloading	off | on; default: **on**	Turns software flow offloading on or off.
Hardware flow offloading	off | on; default: **on**	Turns hardware flow offloading on or off.

Zones

The **Zones** section is used to manage default traffic forwarding policies between different device zones. The figure below is an example of the Zones section and the table below provides information on the fields contained in that section:

You can change a zone's settings from this page by interacting with entries in the zones table. For a more in-depth configuration click the edit button  next to a zone:

Zones: General Settings

Field	Value	Description
Name	string; default: **newzone**	A custom name for the zone. Used for easier management purposes.
Input	Reject | Drop | Accept; default: **Accept**	Default policy for traffic entering the zone.
Output	Reject | Drop | Accept; default: **Accept**	Default policy for traffic originating from and leaving the zone.
Forward	Reject | Drop | Accept; default: **Reject**	Default policy for traffic forwarded between the networks belonging to the zone.
Masquerading	off | on; default: **off**	Turns Masquerading off or on. MASQUERADE is an iptables target that can be used instead of the SNAT (source NAT) target when the external IP of the network interface is not known at the moment of writing the rule (when the interface gets the external IP dynamically).
MSS clamping	off | on; default: **off**	Turns MSS clamping off or on. MSS clamping is a workaround used to change the maximum segment size (MSS) of all TCP connections passing through links with an MTU lower than the Ethernet default of 1500.
Covered networks	network interface(s); default: **none**	Network or networks that belong to the zone.

Zones: Advanced Settings

Field	Value	Description
Restrict to address family	IPv4 and IPv6 | IPv4 only | IPv6 only; default: **IPv4 and IPv6**	IP address family to which to rule will apply.
Restrict Masquerading to given source subnets	network/subnet; default: **none**	Applies Masquerading only to the specified source network/subnet.
Restrict Masquerading to given destinations subnets	network/subnet; default: **none**	Applies Masquerading only to the specified destination network/subnet.
Force connection tracking	off | on; default: **off**	Always maintains connection state (NEW, ESTABLISHED, RELATED) information.
Enable logging on this zone	off | **on**; default: **off**	Logs packets that hit this rule.
Limit log messages	integer/minute; default: **none**	Limit how many messages can be logged in the span of 1 minute. For example, to log 50 packets per minute use: *50/minute*.
Conntrack helpers	Amanda backup and archiving proto (AMANDA) | FTP passive connection tracking (FTP) | RAS proto tracking (RAS) | Q.931 proto tracking (Q.931) | IRC DCC connection tracking (IRC) | NetBIOS name service broadcast tracking (NETBIOS-NS) | PPTP VPN connection tracking (PPTP) | SIP VoIP connection tracking (SIP) | SNMP monitoring connection tracking (SNMP) | TFTP connection tracking (TFTP); default: **none**	**This option appears only when automatic helper assignment option in the firewall's general settings is disabled.** Explicitly choses allowed connection tracking helpers for zone traffic.

Zones: Inter-zone Forwarding

The **Inter-zone forwarding** options control the forwarding policies between the currently edited zone and other zones.

Field	Value	Description
Allow forward to destination zones	zone(s); default: **none**	Allows forward traffic to specified destination zones. Destination zones cover forwarded traffic originating from this source zone.

Allow forward from source zones	zone(s); default: **none**	Allows forward traffic to specified source zones. Source zones match forwarded traffic originating from other zones that is targeted at this zone.

Port Forwards

Port forwarding is a way of redirecting an incoming connection to another IP address, port or the combination of both:

The Port forwards table displays configured port forwarding rules currently configured on the device.

Add New Port Forward

The **Add New Port Forward** section is used to quickly add additional port forwarding rules. The figure below is an example of the Add New Port Forward section and the table below provides information on the fields contained in that section:

Field	Value	Description
Name	string; default: **none**	Name of the rule. This is used for easier management purposes.
External port	integer [0..65535] | range of integers [0..65534] - [1..65535] | port inversion [!0..!65535]; default: **none**	The port number to which hosts will be connecting.
Internal IP address	ip; default: **none**	The IP address to which the incoming connection will be redirected.
Internal port	integer [0..65535] | range of integers [0..65534] - [1..65535] | port inversion [!0..!65535]; default: **none**	The port number to which the incoming connection will be redirected.

Port Forwards Configuration

While the New port forward section provides the possibility to add port forwarding rules fast, it does not contain all possible configuration options to customize a rule. In order to create a more complicated rule, add one using the New port forward section and click the edit button  next to it:

You will be redirected to that rule's configuration general settings page:

Field	Value	Description
Enable	off | on ; default: **on**	Turns the rule on or off
Name	string; default: **none**	Name of the rule. This is used for easier management purposes.
Protocol	TCP | UDP | ICMP | All | +Add new; default: **TCP+UDP**	Specifies to which protocols the rule should apply.
Source zone	firewall zone name; default: **wan**	The zone to which the third party will be connecting. (Same thing as "External zone" in the New port forward section.)
External port	integer [0..65535] | range of integers [0..65534] - [1..65535] | port inversion [!0..!65535]; default: **none**	Port number(s) to which hosts will be connecting. The rule will apply only to hosts that connect to the port number(s) specified in this field. Leave empty to make the rule skip external port matching.
Internal zone	firewall zone name; default: **lan**	The zone to which the incoming connection will be redirected.
Internal IP address	Device LAN IP; default: **Device LAN IP**	The IP address to which the incoming connection will be redirected.
Internal port	integer [0..65535] | range of integers [0..65534] - [1..65535] | port inversion [!0..!65535]; default: **none**	The port number to which the incoming connection will be redirected.

Advanced settings:

Field	Value	Description
Source MAC address	mac; default: **none**	MAC address of connecting hosts. The rule will apply only to hosts that match MAC addresses specified in this field. Leave empty to make the rule skip MAC address matching.
Source IP address	ip | ip/netmask; default: **any**	IP address or network segment used by connecting hosts. The rule will apply only to hosts that connect from IP addresses specified in this field. To specify a network segment instead of one IP address, add a forward slash followed by the netmask length after the network indication (for example, *10.0.0.0/8*).
Source port	integer [0..65535] | range of integers [0..65534] - [1..65535] | port inversion [!0..!65535]; default: **none**	Port number(s) used by the connecting host. The rule will match the source port used by the connecting host with the port number(s) specified in this field. Leave empty to make the rule skip source port matching.

External IP address	ip | ip/netmask; default: **any**	IP address or network segment to which hosts will be connecting. The rule will apply only to hosts that connect to IP addresses specified in this field. To specify a subnet instead of one IP, add a forward slash followed by the netmask length after the network indication (for example, *10.0.0.0/8*).
Enable NAT loopback	off | on ; default: **on**	NAT loopback a.k.a. NAT reflection a.k.a. NAT hairpinning is a method of accessing an internal server using a public IP. NAT loopback enables your local network (i.e., behind your NAT device) to connect to a forward-facing IP address of a machine that it also on your local network.
Extra arguments	string; default: **none**	Adds extra iptables options to the rule.

Traffic Rules

The **Traffic rules** tab is used to set firewall rules that filter traffic moving through the device. The figure below is an example of the Traffic rules table:

Traffic Rule Configuration

In order to begin editing a traffic rule, click the edit button  next to it:

You will be redirected to that rule's configuration page:

General settings

Field	Value	Description
Enable	off | on; default **on**	Turns the rule on or off.
Name	string; default **none**	Name of the rule. This is used for easier management purposes.
Protocol	TCP | UDP | All | +Add new |ICMP; default: **depends on the rule**	Specifies to which protocols the rule should apply.
Match ICMP type	Any | ICMP-type | + Add new; default: **none**	Allows matching specific ICMP types.
Source zone	firewall zone name; default: **wan**	The zone to which the third party will be connecting.

Source IP address	ip | ip/netmask; default: **any**	IP address or network segment used by connecting hosts. The rule will apply only to hosts that connect from IP addresses specified in this field. To specify a network segment instead of one IP address, add a forward slash followed by the netmask length after the network indication (for example, *10.0.0.0/8*).
Source port	integer [0..65535] | range of integers [0..65534] - [1..65535] | port inversion [!0..!65535]; default: **none**	Port number(s) used by the connecting host. The rule will match the source port used by the connecting host with the port number(s) specified in this field. Leave empty to make the rule skip source port matching. Port negation using is also available, for ex. **!1**.
Destination zone	firewall zone; default: **Device (input)**	Target zone of the incoming connection.
Destination address	ip | ip/netmask; default: **any**	Tagert IP address or network segment of the incoming connection.
Destination port	integer [0..65535] | range of integers [0..65534] - [1..65535] | port inversion [!0..!65535]; default: **none**	Tagert port or range of ports of the incoming connection. Port negation using is also available, for ex. **!1**.
Action	Drop | Accept | Reject | Don't track | DSCP | Mark; default: **Accept**	Action that is to be taken when a packet matches the conditions of the rule. • **Drop** – packet is stopped and deleted. • **Accept** – packet gets to continue to the next chain. • **Reject** – packet is stopped, deleted and, differently from Drop, an ICMP packet containing a message of rejection is sent to the source from which the dropped packet came. • **Don't track** – packet is no longer tracked as it moves forward. • **DSCP** – packet is marked with specified DiffServ Code Point value. • **Mark** – packet is marked with specified firewall mark..

Advanced settings

Restrict to address family	IPv4 and IPv6 | IPv4 only | IPv6 only; default: **IPv4 and IPv6**	IP address family to which the rule will apply to.
Source MAC address	mac; default: **none**	MAC address(es) of connecting hosts. The rule will apply only to hosts that match MAC addresses specified in this field. Leave empty to make the rule skip MAC address matching.
DSCP: Set Target value	Default | DSCP values; default: **Default**	If specified, target traffic against the given firewall DSCP value.

Mark: Set Target value	hex; default: **none**	If specified, target traffic against the given firewall mark, e.g. FF or ff to target mark 255.
Match	DSCP | Mark; default: **none**	Match traffic against the given DSCP value or firewall mark
DSCP: Set Match value	Default | DSCP values; default: **Default**	Match traffic against the given firewall DSCP value.
Mark: Set Match value	hex; default: **none**	If specified, match traffic against the given firewall mark, e.g. FF or ff to match mark 255.
Extra arguments	string; default: **none**	Adds extra .iptables options to the rule.

Time restrictions

Week days	days of the week [Monday..Sunday]; default: **none**	Specifies on which days of the week the rule is valid.
Month days	days of the month [1..31]; default: **none**	Specifies on which days of the month the rule is valid.
Start Time (hh:mm:ss)	time [0..23:0..59:0..59]; default: **none**	Indicates the beginning of the time period during which the rule is valid.
Stop Time (hh:mm:ss)	time [0..23:0..59:0..59]; default: **none**	Indicates the end of the time period during which the rule is valid.
Start Date (yyyy-mm-dd)	date [0000..9999:1..12:1..31]; default: **none**	Indicates the first day of the date of the period during which the rule is valid.
Stop Date (yyyy-mm-dd)	date [0000..9999:1..12:1..31]; default: **none**	Indicates the last day of the date of the period during which the rule is valid.
Time in UTC	off | on; default: **no**	Specifies whether the device should use UTC time. If this is disabled, the time zone specified in the System → Administration → NTP page will be used.

Open Ports on Router

In the **Add new instance** section, select **Open ports on router**. This provides a quick way to set simple rules that allow traffic on specified ports of the device. The figure below is an example of the Open ports on device section and the table below provides information on the fields contained in that section:

Field	Value	Description
Name	string; default: **none**	The name of the rule. This is used for easier management purposes. The name field is filled automatically when port numbers are specified, unless the name was specified beforehand by the user.

Protocol	TCP | UDP | ICMP | All | +Add new; default: **none**	Specifies to which protocols the rule should apply.
External port	integer [0..65535] | range of integers [0..65534] - [1..65535] | port inversion [!0..!65535]; default: **none**	Specifies which port(s) should be opened.

Add New Forward Rule

In the **Add new instance** section, select **Add new forward rule**. This is used to create firewall rules that control traffic on the FORWARD chain. The figure below is an example of the Add New Forward Rule section and the table below provides information on the fields contained in that section:

Field	Value	Description
Name	string; default: **none**	The name of the rule. This is used for easier management purposes.
Source zone	firewall zone; default: **wan**	The zone from which traffic has originated.
Destination zone	firewall zone; default: **lan**	The zone to which traffic will be forwarded to.
Add	- (interactive button)	Creates the rule and redirects you to the rule's configuration page

NAT Rules

Network address translation (**NAT**) is method of modifying the source/destination address and/or port information in a packet's IP header.

Source NAT

Source NAT (**SNAT**) is a form of masquerading used to change a packet's source address and/or port number to a static, user-defined value. SNAT is performed in the POSTROUTING chain, just before a packet leaves the device.

The Source NAT section displays currently existing SNAT rules.

Add New Source NAT

The **Add New Source NAT** section is used to create new source NAT rules.

Field	Value	Description

Name	string; default: **none**	The name of the rule. Used only for easier management purposes.
Source zone	firewall zone; default: **lan**	Matches traffic originated from the specified zone.
Destination Zone	firewall zone; default: **wan**	Matches traffic destined for the specified zone.
To source IP	ip | do not rewrite; default: **none**	Changes the source IP address in the packet header to the value specified in this field.
To Source Port	integer [0..65335] | port inversion [!0..!65535] | do not rewrite; default: **none**	Changes the source port in the packet header to the value specified in this field.
Add	- (interactive button)	Creates the rule in accordance with the given parameter and redirects you to the rule's configuration page.

Source NAT Configuration

In order to begin editing a traffic rule, click the edit button next to it:

You will be redirected to that rule's configuration page:

Field	Value	Description
Enable	off | on; default **on**	Turns the rule on or off.
Name	string; default **none**	Name of the rule. This is used for easier management purposes.
Protocol	TCP | UDP | ICMP | +Add new; default: **All protocols**	Specifies to which protocols the rule should apply.
Source zone	firewall zone; default: **lan**	Matches traffic originated from the specified zone.
Source IP address	ip | ip/netmask; default: **Any**	Mathes traffic originated from specified IP address or network segment.
Source port	integer [0..65535] | range of integers [0..65534] - [1..65535] | port inversion [!0..!65535]; default: **none**	Mathes traffic originated from specified port number.
Destination zone	firewall zone; default: **wan**	Matches traffic destined for the specified zone.
Destination IP address	ip | ip/netmask; default: **any**	Matches traffic destined for the specified IP address or network segment.
Destination port	integer [0..65535] | range of integers [0..65534] - [1..65535] | port inversion [!0..!65535]; default: **none**	Matches traffic destined for the specified port number.
Rewrite port	integer [0..65535] | range of integers [0..65534] - [1..65535] | port inversion [!0..!65535]; default: **No rewrite**	Rewrite matched traffic to the given source port.

Field	Value	Description
Extra arguments	string; default: **none**	Adds extra .iptables options to the rule.

Field	Value	Description
Week days	days of the week [Monday..Sunday]; default: **none**	Specifies on which days of the week the rule is valid.
Month days	days of the month [1..31]; default: **none**	Specifies on which days of the month the rule is valid.
Start Time (hh:mm:ss)	time [0..23:0..59:0..59]; default: **none**	Indicates the beginning of the time period during which the rule is valid.
Stop Time (hh:mm:ss)	time [0..23:0..59:0..59]; default: **none**	Indicates the end of the time period during which the rule is valid.
Start Date (yyyy-mm-dd)	date [0000..9999:1..12:1..31]; default: **none**	Indicates the first day of the date of the period during which the rule is valid.
Stop Date (yyyy-mm-dd)	date [0000..9999:1..12:1..31]; default: **none**	Indicates the last day of the date of the period during which the rule is valid.
Time in UTC	off | on; default: **no**	Specifies whether the device should use UTC time. If this is disabled, the time zone specified in the System → Administration → NTP page will be used.

Attack Prevention

The **Attack Prevention** menu tab provides the possibility to configure protections against certain types of online attacks.

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	Value	Description
Enable SYN flood protection	off | on; default: **on**	Turns the rule on or off.
SYN flood rate	integer; default: **5**	Set rate limit (packets per second) for SYN packets above which the traffic is considered flooded
SYN flood burst	integer; default: **10**	Sets burst limit for SYN packets above which the traffic is considered flooded if it exceeds the allowed rate
TCP SYN cookies	off | on; default: **on**	Enables 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	Value	Description
Enable ICMP requests	off | on; default: **on**	Turns the rule on or off.
Enable ICMP limit	off | on; default: **off**	Turns ICMP echo-request limit in selected period on or off.
Limit period	Second | Minute | Hour | Day; default: **Second**	Period length for matching the conditions of the rule.
Limit	integer; default: **5**	Maximum ICMP echo-request number during the period.
Limit burst	integer; default: **10**	Indicates the maximum burst before the above limit kicks in.

SSH Attack Prevention

This protection prevent **SSH attacks** by limiting connections in a defined period.

Field	Value	Description
Enable SSH limit	off | on; default: **off**	Turns the rule on or off.
Limit period	Second | Minute | Hour | Day; default: **Second**	Period length for matching the conditions of the rule.
Limit	integer [1..10000]; default: **none**	Maximum SSH connections during the set period
Limit burst	integer [1..10000]; default: **none**	Indicates 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	Value	Description
Enable HTTP limit	off | on; default: **off**	Turns the rule on or off.
Limit period	Second | Minute | Hour | Day; default: **Second**	Period length for matching the conditions of the rule.
Limit	integer [1..10000]; default: **none**	Maximum HTTP connections during the set period.
Limit burst	integer [1..10000]; default: **none**	Indicates 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	Value	Description
Enable HTTPS limit	off | on; default: **off**	Turns the rule on or off.
Limit period	Second | Minute | Hour | Day; default: **Second**	Period length for matching the conditions of the rule.
Limit	integer [1..10000]; default: **none**	Maximum HTTPS connections during the set period.
Limit burst	integer [1..10000]; default: **none**	Indicates the maximum burst number before the above limit kicks in.

Port Scan

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 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. 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	Value	Description
Enable	off | on; default: **off**	Turns the function on or off.
Scan count	integer [5..10000]; default: **none**	How many port scans before blocked.
Interval	integer [10..4096]; default: **none**	Time interval in seconds in which port scans are counted.
SYN-FIN attack	off | on; default: **off**	Turns protection from SYN-FIN attacks on or off.
SYN-RST attack	off | on; default: **off**	Turns protection from SYN-RST attacks on or off.
X-Mas attack	off | on; default: **off**	Turns protection from X-Mas attacks on or off.
FIN scan	off | on; default: **off**	Turns protection from FIN scan attacks on or off.
NULLflags attack	off | on; default: **off**	Turns protection from NULLflags attacks on or off.

Custom Rules

The **Custom rules** tab provides you with the possibility to execute **iptables** commands which are not otherwise covered by the device's firewall framework. The commands are executed after each firewall restart, right after the default rule set has been loaded.

Note: Custom rules are not recommended to be used with *hostnames*. The rules will not remain active after reboot due to security reasons.

The figure below is an example of the Custom rules tab:

The rules added here are saved in the **/etc/firewall.user** file. Feel free to edit that file instead for the same effect in case you don't have access to the device's WebUI.

The **Save** button restarts the firewall service. Thus, adding the custom rules specified in this section to the device's list of firewall rules.

The **Reset** button resets the custom rules field to its default state.

DMZ

The **DMZ** is a security concept. It comprises the separation of the LAN-side network into at least two networks: the user LAN and the DMZ. Generally the DMZ is imprisoned: only access to certain ports from the Internet are allowed into the DMZ, while the DMZ is not allowed to establish new connections to the WAN-side or LAN-side networks. That way, if a server inside of the DMZ is hacked the potential damage that can be done remains restricted! The whole point of the DMZ is to cleanly create a unique firewall rule set that dramatically restricts access in to, and out of the, DMZ.

Field	Value	Description
Enable	off | on; default: **off**	Enables the DMZ configuration.
Host IP	ipv4; default: **none**	Specifies the IP address of the DMZ host.
Protocol	All | TCP | UDP | ICMP; default: **None**	Specifies for which protocols the DMZ will be used.

Ports	0..65535 | port range | port negation; default: **none**	Match incoming traffic directed at the given destination port or port range on DMZ host IP.