Firewall Appliance Configuration

Contents

Overview

Each Swivel appliance has a firewall protecting access to that sever. This document details how to add and change the Firewall configurations on Swivel appliances. For information on configuring Port Address Translation, see How to run PINsafe on non-default ports, this allows ports such as 443 or 80 to be used. Forinformation on ports used by Swivel appliances see Ports.

The Swivel Administration console access can also have IP access control, see Filter IP How to Guide

Prerequisites

Swivel Appliance 2.x

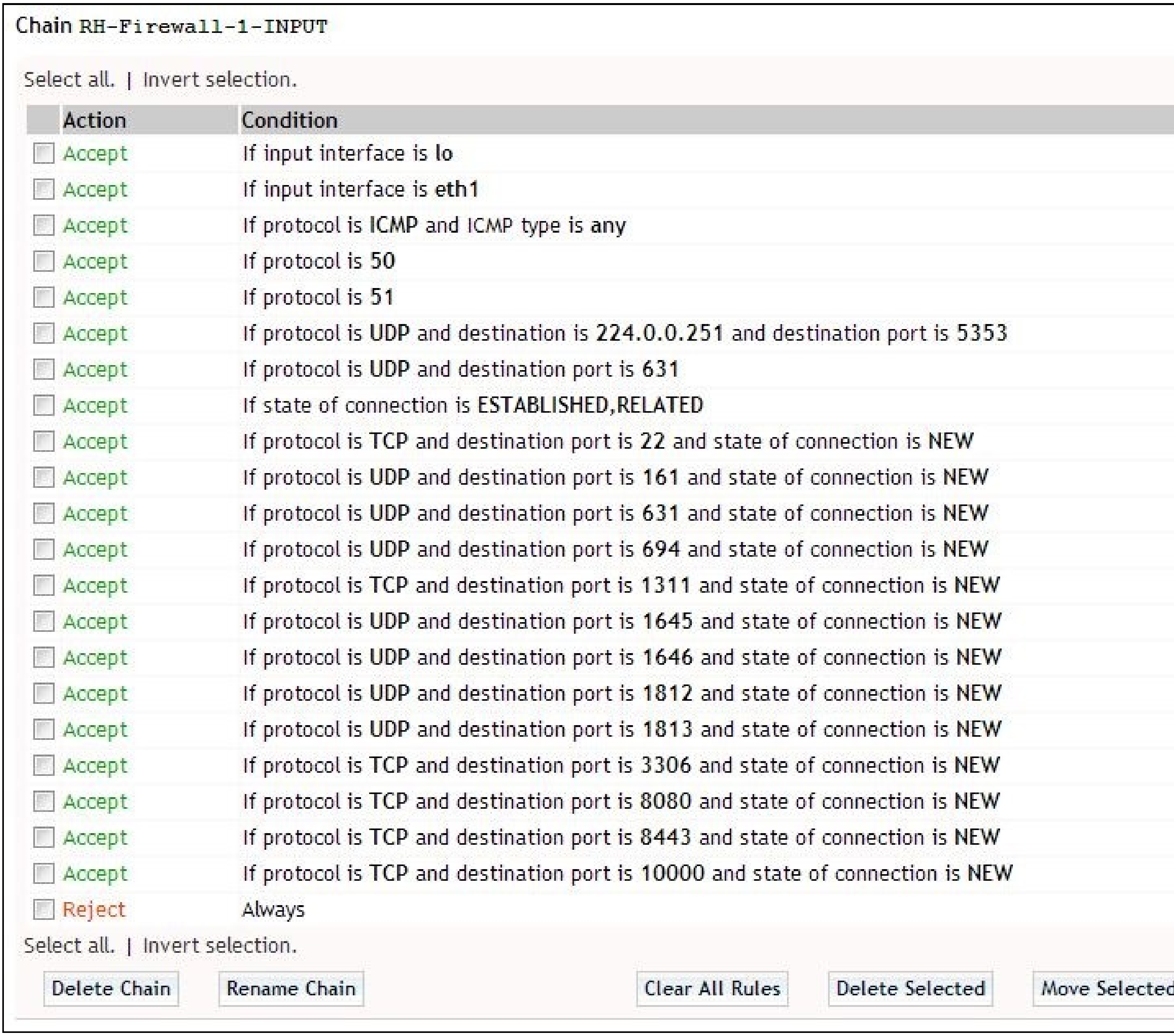
Configuring the Firewall

Webmin

Configuration of the firewall is usually carried out using Webmin

Firewall Add Rule

Once logged in select Networking then Firewall. Locate the Chain RH-Firewall-1-INPUT then below this click on **Add Rule**.



Chain RH-Firewall-1-INPUT

	Action	Condition
□	Accept	If input interface is **lo**
□	Accept	If input interface is **eth1**
□	Accept	If protocol is **ICMP** and ICMP type is **any**
□	Accept	If protocol is **50**
□	Accept	If protocol is **51**
□	Accept	If protocol is **UDP** and destination is **224.0.0.251** and destination port is **5353**
□	Accept	If protocol is **UDP** and destination port is **631**
□	Accept	If state of connection is **ESTABLISHED,RELATED**
□	Accept	If protocol is **TCP** and destination port is **22** and state of connection is **NEW**
□	Accept	If protocol is **UDP** and destination port is **161** and state of connection is **NEW**
□	Accept	If protocol is **UDP** and destination port is **631** and state of connection is **NEW**
□	Accept	If protocol is **UDP** and destination port is **694** and state of connection is **NEW**
□	Accept	If protocol is **TCP** and destination port is **1311** and state of connection is **NEW**
□	Accept	If protocol is **UDP** and destination port is **1645** and state of connection is **NEW**
□	Accept	If protocol is **UDP** and destination port is **1646** and state of connection is **NEW**
□	Accept	If protocol is **UDP** and destination port is **1812** and state of connection is **NEW**
□	Accept	If protocol is **UDP** and destination port is **1813** and state of connection is **NEW**
□	Accept	If protocol is **TCP** and destination port is **3306** and state of connection is **NEW**
□	Accept	If protocol is **TCP** and destination port is **8080** and state of connection is **NEW**
□	Accept	If protocol is **TCP** and destination port is **8443** and state of connection is **NEW**
□	Accept	If protocol is **TCP** and destination port is **10000** and state of connection is **NEW**
□	Reject	Always

Enter the following parameters:

Rule Comment description of the rule

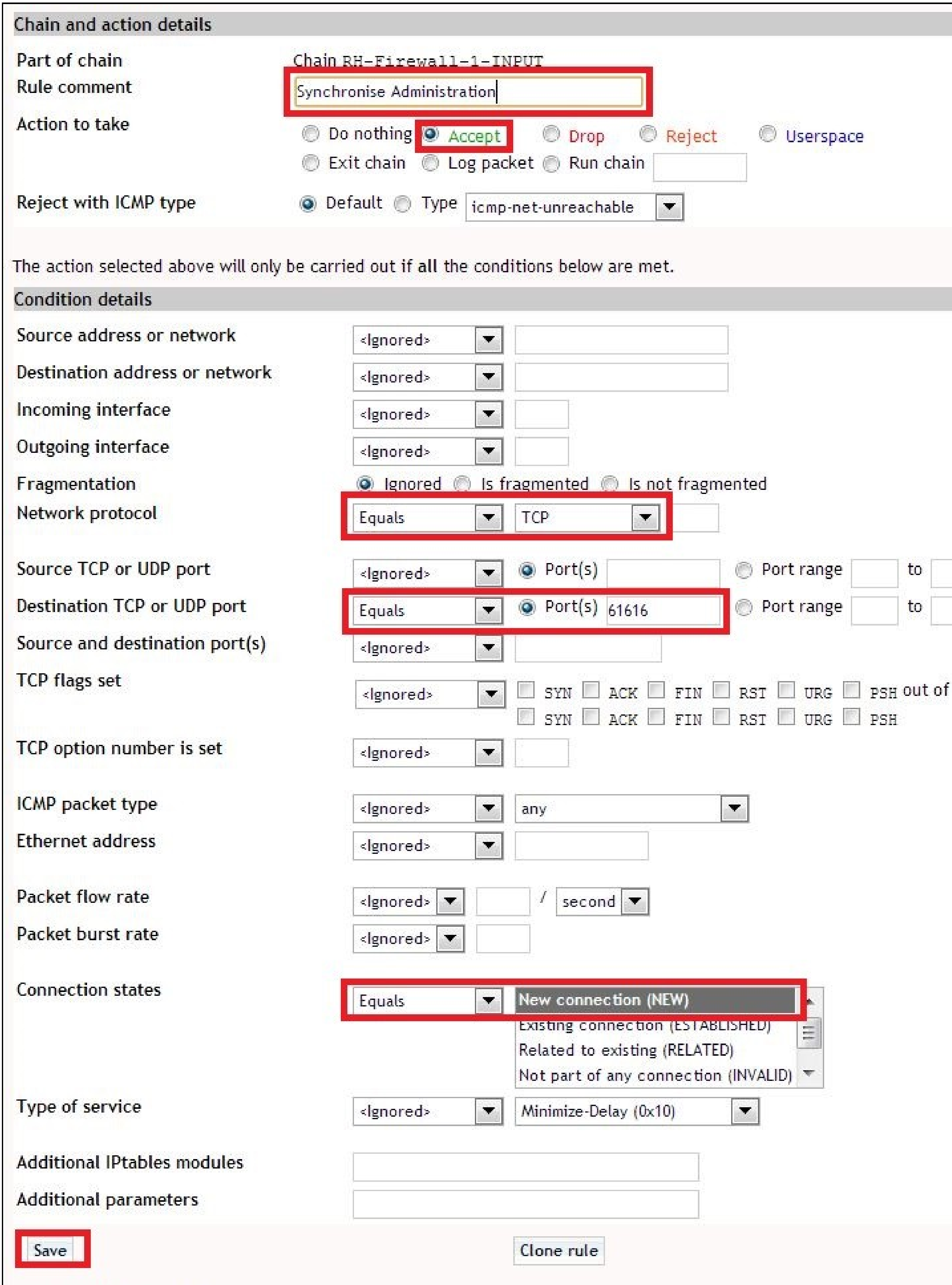
Action to take select **Accept** to allow the rule

'*Network Protocol **select** Equals* and TCP or UDP as appropriate

'*Destination TCP or UDP port **select** Equals* and set the port required

Connection states select **Equals** and **New connection (NEW)**

When complete click on Save.



Chain and action details

Part of chain	Chain RH-Firewall-1-INPUT
Rule comment	Synchronise Administration
Action to take	○ Do nothing ● Accept ○ Drop ○ Reject ○ Userspace ○ Exit chain ○ Log packet ○ Run chain
Reject with ICMP type	● Default ○ Type icmp-net-unreachable

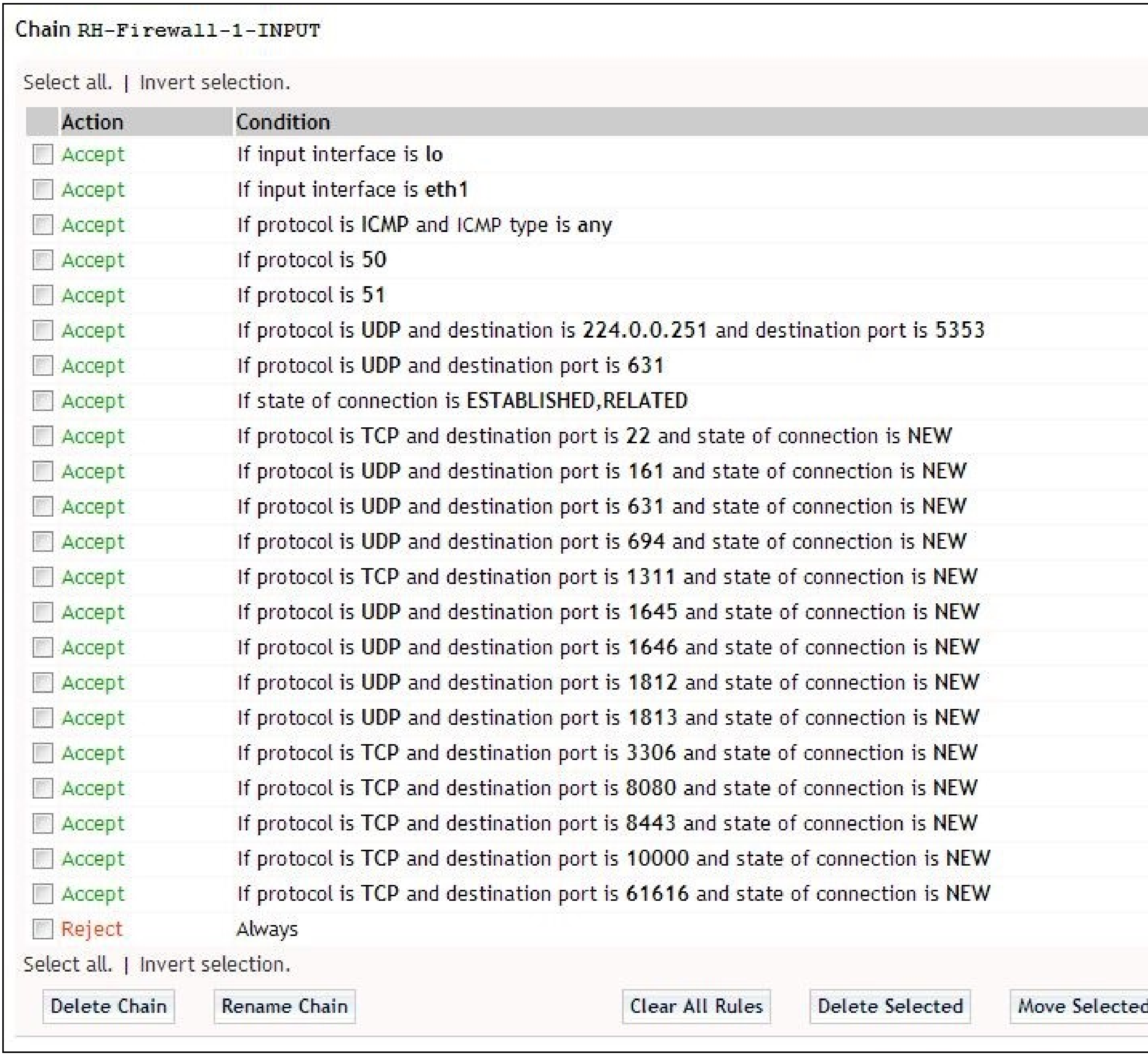
The action selected above will only be carried out if **all** the conditions below are met.

Condition details

Source address or network	<Ignored>
Destination address or network	<Ignored>
Incoming interface	<Ignored>
Outgoing interface	<Ignored>
Fragmentation	● Ignored ○ Is fragmented ○ Is not fragmented
Network protocol	Equals TCP
Source TCP or UDP port	<Ignored> ● Port(s) ○ Port range to
Destination TCP or UDP port	Equals ● Port(s) 61616 ○ Port range to
Source and destination port(s)	<Ignored>
TCP flags set	<Ignored> □ SYN □ ACK □ FIN □ RST □ URG □ PSH out of □ SYN □ ACK □ FIN □ RST □ URG □ PSH
TCP option number is set	<Ignored>
ICMP packet type	<Ignored> any
Ethernet address	<Ignored>
Packet flow rate	<Ignored> / second
Packet burst rate	<Ignored>
Connection states	Equals New connection (NEW) Existing connection (ESTABLISHED) Related to existing (RELATED) Not part of any connection (INVALID)
Type of service	<Ignored> Minimize-Delay (0x10)
Additional IPtables modules	
Additional parameters	

Change the rule priority

Increase the rule priority so that it is above the Reject rule by clicking on the green up arrow.



Chain RH-Firewall-1-INPUT

Select all. | Invert selection.

	Action	Condition
□	Accept	If input interface is lo
□	Accept	If input interface is eth1
□	Accept	If protocol is ICMP and ICMP type is any
□	Accept	If protocol is 50
□	Accept	If protocol is 51
□	Accept	If protocol is UDP and destination is 224.0.0.251 and destination port is 5353
□	Accept	If protocol is UDP and destination port is 631
□	Accept	If state of connection is ESTABLISHED,RELATED
□	Accept	If protocol is TCP and destination port is 22 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 161 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 631 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 694 and state of connection is NEW
□	Accept	If protocol is TCP and destination port is 1311 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 1645 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 1646 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 1812 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 1813 and state of connection is NEW
□	Accept	If protocol is TCP and destination port is 3306 and state of connection is NEW
□	Accept	If protocol is TCP and destination port is 8080 and state of connection is NEW
□	Accept	If protocol is TCP and destination port is 8443 and state of connection is NEW
□	Accept	If protocol is TCP and destination port is 10000 and state of connection is NEW
□	Accept	If protocol is TCP and destination port is 61616 and state of connection is NEW
□	Reject	Always

Select all. | Invert selection.

Apply Configuration

Click on Apply Configuration to make the firewall rules active.

[Image:Swivel Appliance Webmin Firewall apply configuration.JPG]]

Testing

Known Issues

Troubleshooting