

Instructions

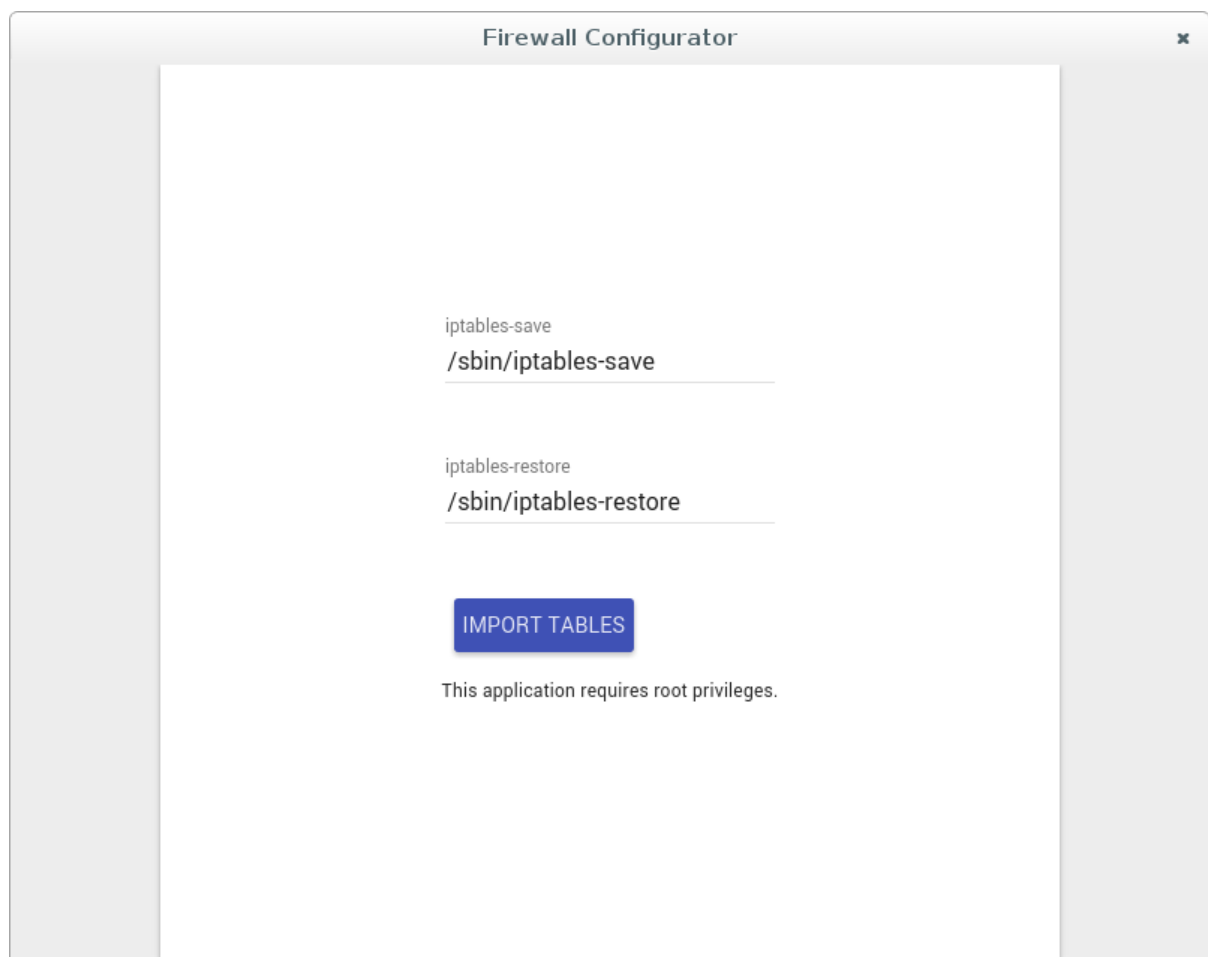
Installation

> npm install

Running the Application

> npm start

Launch screen

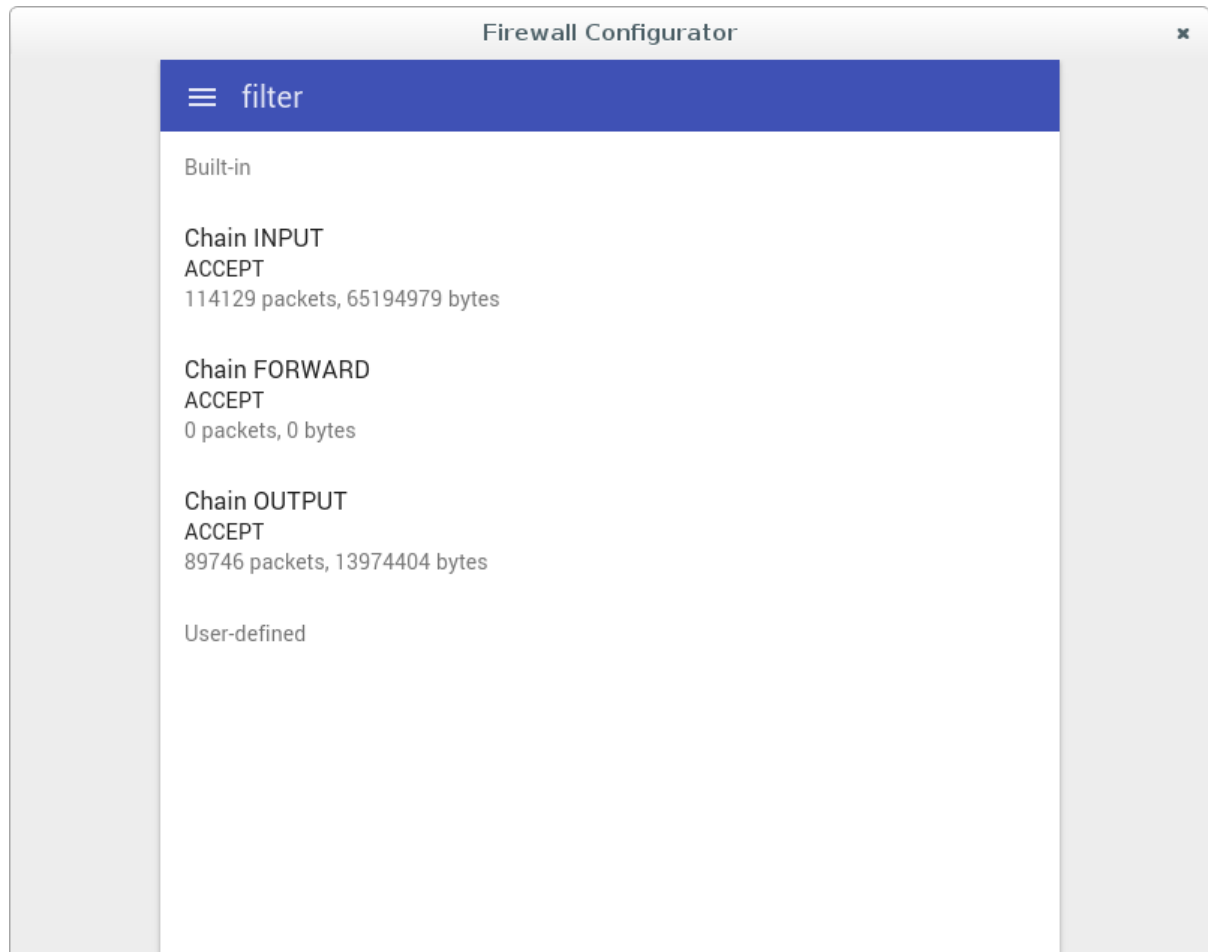


Input fields can be used to change the paths used for:

- iptables-save
- iptables-restore

Pressing 'Import Tables' will run iptables-save and start the application.

Main screen



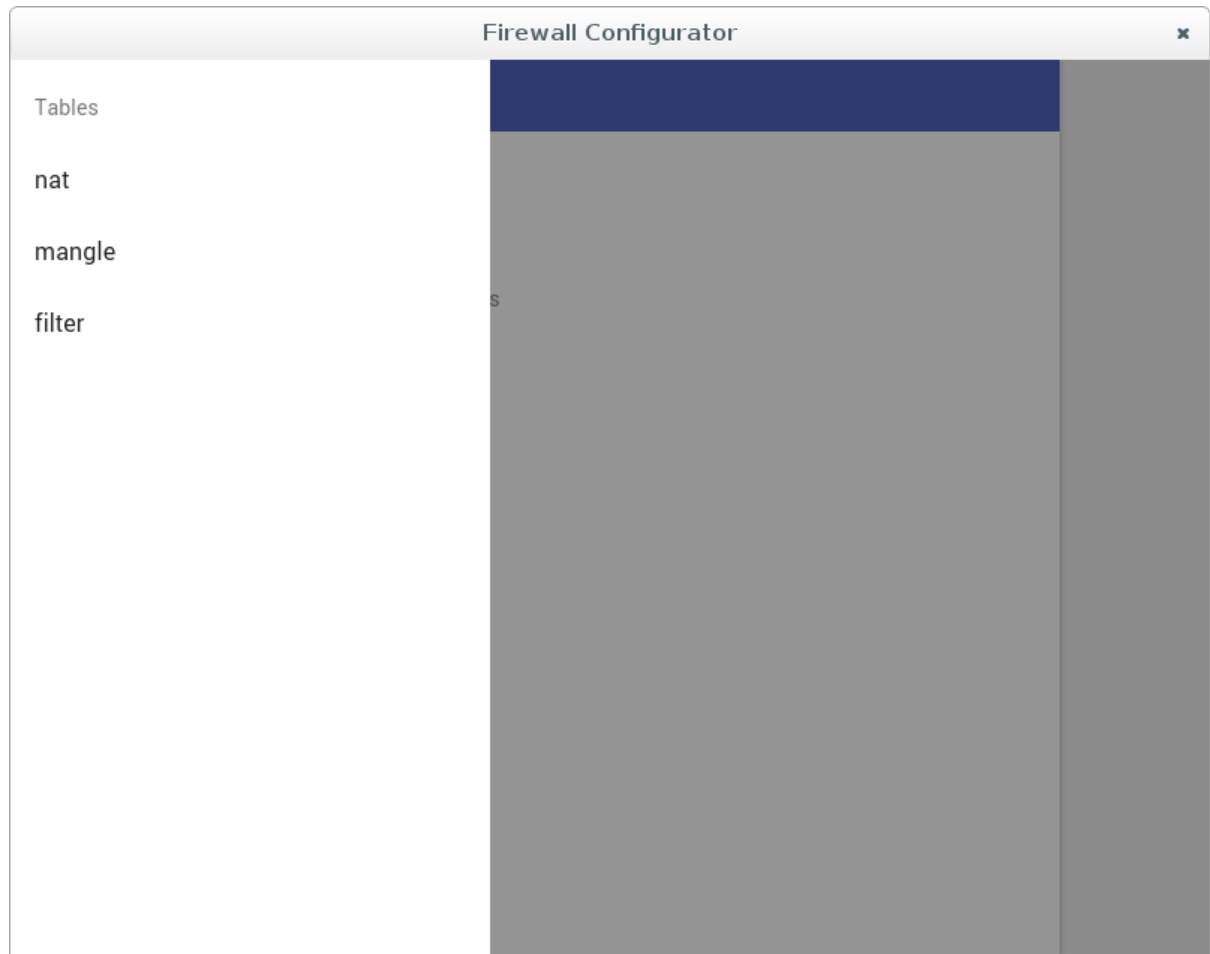
The default table will show up once the firewall rules are loaded.

Rule chains are separated into two categories:

- Built-in chains
- User-defined chains

Clicking on the chain will navigate to the rules screen.

Navigation drawer



Pressing on the menu button (hamburger) on the top left of the toolbar will open the navigation drawer. All of the tables retrieved by 'iptables-save' will be shown here.

Clicking on the table will navigate to the main screen.

Rules screen (FORWARD chain)

The screenshot shows the 'FORWARD' rules configuration window in the Firewall Configurator. The window has a title bar 'Firewall Configurator' and a close button. Inside, there's a blue header bar with a back arrow and the text 'FORWARD', and a save icon. Below the header, the 'Policy' is set to 'ACCEPT'. A 'New Rule' section contains a note: 'Note: Rules are appended to the top of the rules list.' Below this are input fields for 'Direction', 'Protocol', 'Port No.', and 'Permission', each with a dropdown arrow. Further down are fields for 'IP Address', 'Network Interface', and 'Gateway Interface'. At the bottom of this section are 'CLEAR' and 'CREATE' buttons. The bottom part of the window shows a list of existing rules under the heading 'Rules':
-A FORWARD -d 192.168.122.0/24 -o virbr0 -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -s 192.168.122.0/24 -i virbr0 -j ACCEPT

Details about the selected chain will be shown here.

If the selected chain is a built-in chain, then a policy input field will appear. This field can be used to change the default policy.

In the forward chain of the 'filter' table, a 'New Rule' section will appear. All of the input fields must be filled out for a rule to be created. The required fields include:

- Direction
- Protocol
- Port or Type Number
- Permission
- IP Address
- Network Interface
- Gateway Interface

Rules will be prepended to the rules chain in the text area below.

Examples

Firewall Configurator

← FORWARD

Policy
ACCEPT

New Rule

Note: Rules are appended to the top of the rules list.

Direction

Protocol

Port No.

Permission

Inbound

TCP

23

Allow

IP Address

Network Interface

Gateway Interface

192.168.1.1

eth0

wlan0

CLEAR

CREATE

Rules

-A FORWARD -d 192.168.122.0/24 -o virbr0 -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

-A FORWARD -s 192.168.122.0/24 -i virbr0 -j ACCEPT

Firewall Configurator

← FORWARD

Policy
ACCEPT

New Rule

Note: Rules are appended to the top of the rules list.

Direction

Protocol

Port No.

Permission

Inbound

TCP

23

Allow

IP Address

Network Interface

Gateway Interface

192.168.1.1

eth0

wlan0

CLEAR

CREATE

Rules

-A FORWARD -p tcp --dport 23 -m state --state NEW,ESTABLISHED -i wlan0 -o

New rule created