

Edit



## Edit Firewall Rule

### Action

Block ▼

Choose what to do with packets that match the criteria specified below.

Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

### Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

### Interface

WAN ▼

Choose the interface from which packets must come to match this rule.

### Address Family

IPv4+IPv6 ▼

Select the Internet Protocol version this rule applies to.

### Protocol

TCP/UDP ▼

Choose which IP protocol this rule should match.

## Source

### Source

☐ Invert match

Any ▼

Source Address / 32 ▼

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.



## Destination

☐ Invert match

This Firewall (self) ▼

Destination Address / 32 ▼

## Destination Port Range

SSH (22) ▼

From

Custom

SSH (22) ▼

To

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

## Extra Options

### Log


☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

### Description

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset label and displayed in the firewall log.

### Advanced Options

 Display Advanced

## Rule Information

### Tracking ID

1552344662

### Created

3/11/19 18:51:02 by admin@192.168.1.20 (Local Database)

### Updated

2/12/20 10:17:35 by admin@192.168.1.20 (Local Database)

