

## Add rule: allow all machines in DMZ can reach anywhere

**Edit Firewall Rule**

**Action**

Pass

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**

DMZ

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

**Address Family**

IPv4

Select the Internet Protocol version this rule applies to.

**Protocol**

Any

Choose which IP protocol this rule should match.

**Source**

**Source**

☐ Invert match

DMZ net

Source Address

/

**Destination**

**Destination**

☐ Invert match

any

Destination Address

/

**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**

Hihi

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

## Add rule: allow ICMP packets can reach DMZ

Firewall / Rules / Edit

**Edit Firewall Rule**

**Action**

Pass

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**

DMZ

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

**Address Family**

IPv4

Select the Internet Protocol version this rule applies to.

**Protocol**

ICMP

Choose which IP protocol this rule should match.

**ICMP Subtypes**

any

Alternate Host  
Datagram conversion error  
Echo reply

For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

**Source**

**Source**

☐ Invert match

DMZ net

Source Address

/

**Destination**

**Destination**

☐ Invert match

DMZ net

Destination Address

/

**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 and displayed in the firewall log.

**Advanced Options**

Display Advanced

## Edit Firewall Rule

**Action** Reject 

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** LAN 

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


**Address Family** IPv4 

Select the Internet Protocol version this rule applies to.

**Protocol** TCP 

Choose which IP protocol this rule should match.

## Source

**Source** ☐ Invert match any Source Address /   [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

**Destination** ☐ Invert match Network 192.168.100.123 / 24 **Destination Port Range** SSH (22) From Custom To SSH (22)  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 ruleHint: 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 and displayed in the firewall log.

**Advanced Options**  [Display Advanced](#) [Save](#)