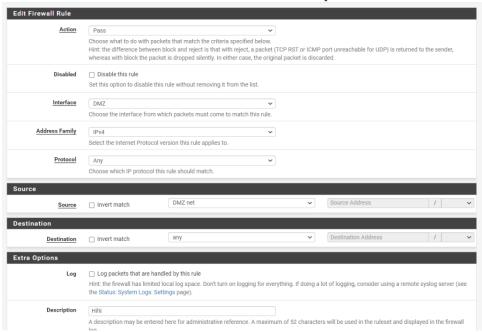
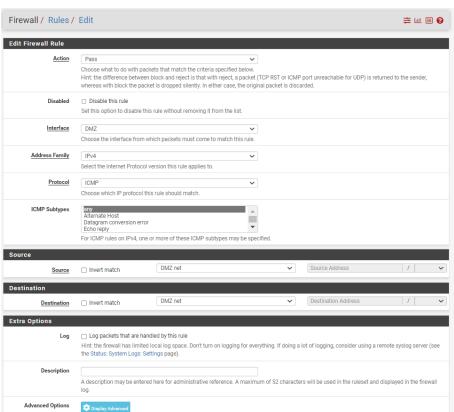
Add rule: allow all machines in DMZ can reach anywhere



Add rule: allow ICMP packets can reach DMZ



Firewall / Rules / Edit **⋣ Ш ⊞ 0** Edit Firewall Rule Action 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. IPv4 Address Family Select the Internet Protocol version this rule applies to. Protocol ~ Choose which IP protocol this rule should match. any Source Address Source ☐ Invert match 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 / 24 192.168.100.123 ☐ Invert match Network ~ Destination SSH (22) SSH (22) Destination Port Range Custom То 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 and displayed in the firewall Advanced Options Save