Table of Contents

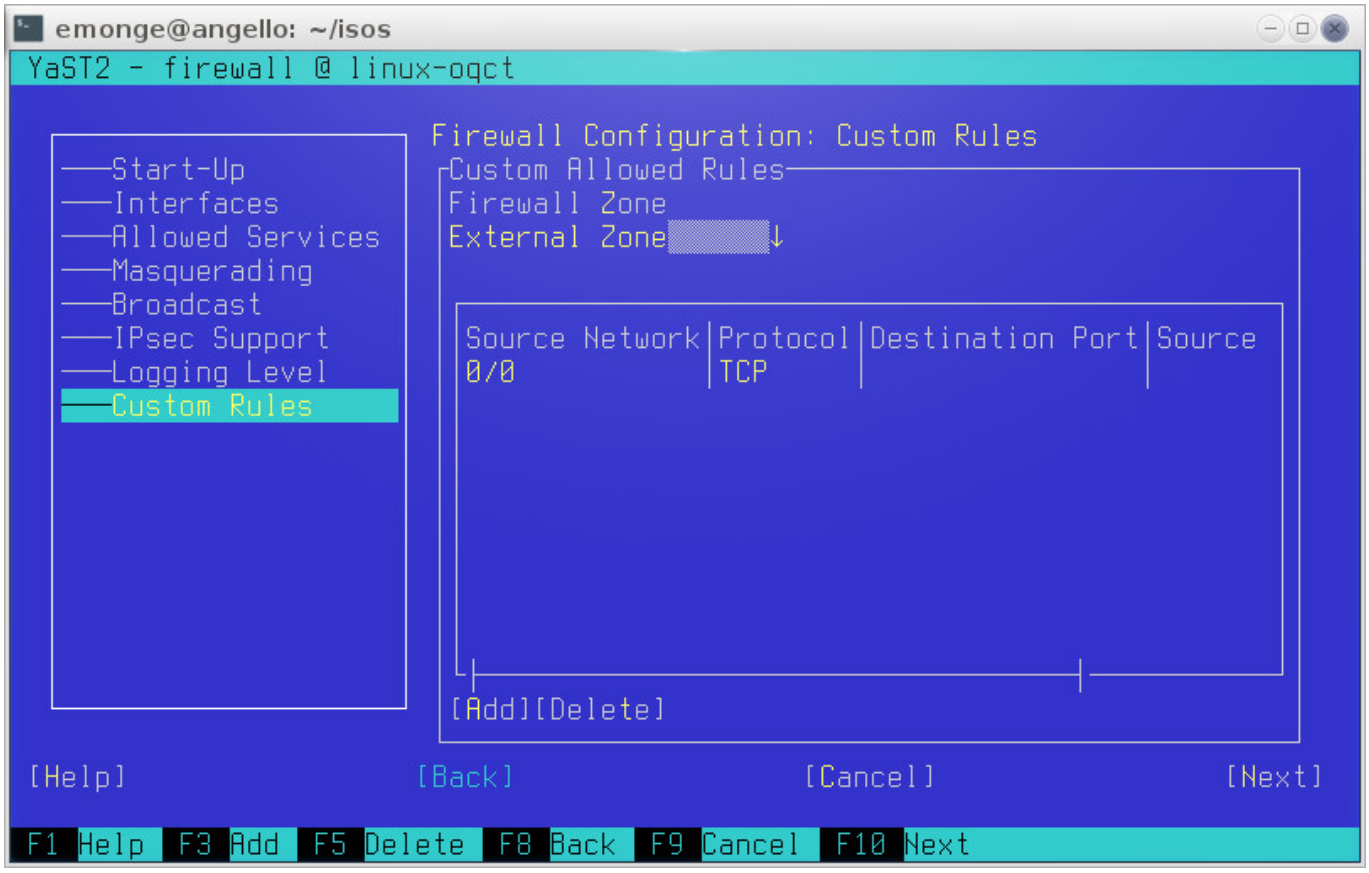
Playing with SuSE firewall

The organization have one requerimient, access to SSH must be allowed only from specific IP range.

The firewall must be up but only block SSH ports.

I know that you can down the SuSE Firewall and make a script with iptables... but I want make it in SuSE way. You need have basic knowledge about SuSE Firewall

Enable the firewall and configure a custom rule to allow all connections:



Now configure SuSE Firewall to accept custom rules. Please edit /etc/sysconfig/SuSEfirewall2 change the line:

```
FW_CUSTOMRULES="/etc/sysconfig/scripts/SuSEfirewall2-custom"
```

Edit the file /etc/sysconfig/scripts/SuSEfirewall2-custom change the lines:

```
fw_custom_before_port_handling() {
    # these rules will be loaded after the anti-spoofing and icmp handling
    # and after the input has been redirected to the input_XXX and
    # forward_XXX chains and some basic chain-specific anti-circumvention
    # rules have been set,
    # but before any IP protocol or TCP/UDP port allow/protection rules
    # will be set.
    # You can use this hook to allow/deny certain IP protocols or TCP/UDP
    # ports before the SuSEfirewall2 generated rules are hit.
```

```
    iptables -A INPUT -p tcp --dport 22 -s 192.168.122.0/24 -j ACCEPT
    iptables -A INPUT -p tcp --dport 22 -j DROP

    true
}
```

This block SSH to all IPs but 192.168.122.0/24 subnet.

Restart SuSE Firewall.

References

- https://www.suse.com/documentation/sles11/book_security/data/sec_fire_suse.html
- https://stackoverflow.com/questions/7423309/iptables-block-access-to-port-8000-except-from-ip-address