Networking
Firewall Worksheet

Configure a firewall in VyOS.

Apply a firewall to the outward-facing network interface. This firewall contains one rule for packets being routed, and four rules for packets destined for your LAN. (There are no rules for packets outbound from your LAN, although there could be.)

1. Start the configuration:

```
configure
```

2. Enter these commands:

```
#-----------------------------------------------------------
# Set firewall on gateway router.
# Two sets of rules: world-inbound-to-LAN,
# and world-to-router.
# No rules for packets outbound from LAN (let the fur fly).
# 2016-10-22
#-----------------------------------------------------------

set firewall name 'World-to-LAN' default-action 'drop'
# allow established and related packets,
# but no inbound connection requests except pings
set firewall name 'World-to-LAN' rule 10 action 'accept'
set firewall name 'World-to-LAN' rule 10 state established 'enable'
set firewall name 'World-to-LAN' rule 10 state related 'enable'
set firewall name 'World-to-LAN' rule 10 description 'Allow established and related'
# allow inbound pings to LAN:
set firewall name 'World-to-LAN' rule 20 action 'accept'
set firewall name 'World-to-LAN' rule 20 icmp type-name 'echo-request'
set firewall name 'World-to-LAN' rule 20 protocol 'icmp'
set firewall name 'World-to-LAN' rule 20 state new 'enable'
set firewall name 'World-to-LAN' rule 20 description 'Allow inbound pings'

set firewall name 'World-to-Router' default-action 'drop'
# allow established and related packets
set firewall name 'World-to-Router' rule 10 action 'accept'
set firewall name 'World-to-Router' rule 10 state established 'enable'
set firewall name 'World-to-Router' rule 10 state related 'enable'
set firewall name 'World-to-Router' rule 10 description 'Allow established and related'
# allow inbound pings to router:
set firewall name 'World-to-Router' rule 20 action 'accept'
set firewall name 'World-to-Router' rule 20 icmp type-name 'echo-request'
set firewall name 'World-to-Router' rule 20 protocol 'icmp'
set firewall name 'World-to-Router' rule 20 state new 'enable'
set firewall name 'World-to-LAN' rule 20 description 'Allow pings to router'


# These ssh rules actually control inbound sessions
# to the gateway routers or to the LAN.

# kill ssh attempts after 4 failed tries
set firewall name 'World-to-Router' rule 30 action 'drop'
set firewall name 'World-to-Router' rule 30 destination port '22'
set firewall name 'World-to-Router' rule 30 protocol 'tcp'
set firewall name 'World-to-Router' rule 30 recent count '4'
set firewall name 'World-to-Router' rule 30 recent time '60'
set firewall name 'World-to-Router' rule 30 state new 'enable'
# allow ssh sessions to router
set firewall name 'World-to-Router' rule 40 action 'accept'
set firewall name 'World-to-Router' rule 40 destination port '22'
set firewall name 'World-to-Router' rule 40 protocol 'tcp'
set firewall name 'World-to-Router' rule 40 state new 'enable'
# allow ssh sessions to LAN
set firewall name 'World-to-LAN' rule 40 action 'accept'
set firewall name 'World-to-LAN' rule 40 destination port '22'
set firewall name 'World-to-LAN' rule 40 protocol 'tcp'
set firewall name 'World-to-LAN' rule 40 state new 'enable'


# bind firewall rulesets to an interface
set interfaces ethernet eth0 firewall in name 'World-to-LAN'
set interfaces ethernet eth0 firewall local name 'World-to-Router'
#-----------------------------------------------------------
```

Check your firewall with the command:

```
show firewall
```

Finish up.

1. Apply the configuration:

   ```
   commit
   ```

2. Save the configuration for future reboots:

   ```
   save
   ```

3. ... and quit:

   ```
   exit
   ```

Congratulations! You've configured a firewall on your router.
