firewalld_examples

Here's a practical reference of `firewall-cmd` examples, organized by category:

Status & Inspection

bash

```
firewall-cmd --state
firewall-cmd --list-all                          # active zone
details
firewall-cmd --list-all --zone=internal          # specific zone
firewall-cmd --list-all-zones
firewall-cmd --get-active-zones
firewall-cmd --get-default-zone
firewall-cmd --get-zones
firewall-cmd --get-services
```

Zones

bash

```
# Set default zone
firewall-cmd --set-default-zone=internal

# Bind interface to zone
firewall-cmd --permanent --zone=trusted --change-interface=eth1

# Add a source network to a zone
firewall-cmd --permanent --zone=trusted
--add-source=192.168.1.0/24

# Remove a source
```

```
firewall-cmd --permanent --zone=trusted
--remove-source=192.168.1.0/24
```

Services

bash

```
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --permanent --zone=public
--remove-service=dhcpv6-client
firewall-cmd --list-services
```

Ports

bash

```
firewall-cmd --permanent --zone=public --add-port=8443/tcp
firewall-cmd --permanent --zone=public --add-port=8080-8090/tcp
# range
firewall-cmd --permanent --zone=public --remove-port=8443/tcp
firewall-cmd --zone=public --list-ports
```

Rich Rules

bash

```
# Allow a subnet to reach a service
firewall-cmd --permanent --zone=public \
  --add-rich-rule='rule family=ipv4 source
address=192.168.1.0/24 service name="ssh" accept'

# Reject a specific IP
firewall-cmd --permanent --zone=public \
```

```
  --add-rich-rule='rule family=ipv4 source address=10.5.0.100
reject'

# Allow port range from specific subnet to specific destination
firewall-cmd --permanent --zone=public \
  --add-rich-rule='rule family=ipv4 source address=10.0.0.0/24
destination address=192.168.0.10/32 port port=8080-8090
protocol=tcp accept'

# Rate-limit SSH to 10 connections/minute
firewall-cmd --permanent \
  --add-rich-rule='rule service name=ssh limit value=10/m
accept'

# Log + accept SSH from a subnet (rate-limited logging)
firewall-cmd --permanent \
  --add-rich-rule='rule family="ipv4" source
address="192.168.0.0/24" service name="ssh" log prefix="ssh"
level="info" limit value="50/m" accept'

# Block a single IP from SSH only
firewall-cmd --permanent \
  --add-rich-rule='rule family="ipv4" source
address="192.168.1.100" service name="ssh" reject'

# List rich rules
firewall-cmd --list-rich-rules
firewall-cmd --permanent --zone=public --list-rich-rules

# Remove a rich rule
firewall-cmd --permanent --zone=public \
  --remove-rich-rule='rule family=ipv4 source address=10.5.0.100
reject'

# Query if a rich rule exists (returns 0/1)
```

```
firewall-cmd --permanent --zone=public \
  --query-rich-rule='rule family=ipv4 source address=10.5.0.100
reject'
```

NAT — Masquerading & Port Forwarding

bash

```
# Enable masquerading on a zone
firewall-cmd --permanent --zone=external --add-masquerade

# Masquerade only for a specific subnet (rich rule)
firewall-cmd --permanent --zone=external \
  --add-rich-rule='rule family=ipv4 source
address=192.168.1.0/24 masquerade'

# Forward port 12345/tcp to internal host port 22
firewall-cmd --permanent --zone=public \

--add-forward-port=port=12345:proto=tcp:toport=22:toaddr=10.20.3
0.40

# Forward port via rich rule
firewall-cmd --permanent --zone=public \
  --add-rich-rule='rule family=ipv4 source
address=192.168.1.0/24 forward-port port=22 protocol=tcp
to-port=2222 to-addr=10.0.0.10'
```

IP Sets

bash

```
# Create an IP set
```

```
firewall-cmd --permanent --new-ipset=blocklist --type=hash:ip

# Add IPs to the set
firewall-cmd --permanent --ipset=blocklist --add-entry=10.5.0.1
firewall-cmd --permanent --ipset=blocklist
--add-entries-from-file=/etc/fw-blocklist.txt

# Use IP set as zone source
firewall-cmd --permanent --zone=drop
--add-source=ipset:blocklist

# List IP sets
firewall-cmd --get-ipsets
firewall-cmd --permanent --ipset=blocklist --get-entries
```

Runtime vs. Permanent

bash

```
# Apply permanent config to runtime without restart
firewall-cmd --reload

# Save current runtime rules as permanent
firewall-cmd --runtime-to-permanent

# Temporary rule (expires after 5 minutes)
firewall-cmd --zone=public --add-service=http --timeout=300
```

Rule Processing Order (within a zone)

1. Port forwarding / masquerading
2. Logging rules
3. Allow rules
4. Deny rules

Direct rules (`--direct`) are evaluated before all of the above. The full rich language syntax is documented in `man 5 firewalld.richlanguage`.