

# Other nice features

- Glob matching interface names with `iifname`; (that may not exist when the rule set is first loaded) that are matched later (potentially slow, but useful for compatibility)
- `iif` uses the interface index ID and is resolved by interface name when the rules are loaded so the interface must already exist
- Can declare concatenated selectors as constraints for sets; useful for metering
- Queuing packets to user space (`libnetfilter_queue`)

```
nft insert rule inet firewall input iifname "wlp*" counter
```

```
nft insert rule inet firewall input iif enp0s1 counter
```

```
nft add set inet firewall concat_type '{ type ipv4_addr . inet_service; size 64; flags timeout, dynamic; }'
```

```
pip3 install --user NetfilterQueue
```

```
nft add rule inet firewall output tcp dport 80 queue num 2
```

```
python3 -c 'from netfilterqueue import NetfilterQueue; import sys; (lambda q: (q.bind(2, lambda pkt: (print(pkt), pkt.accept()))), q.run(block = True)))( NetfilterQueue())'
```

```
TCP packet, 60 bytes
```

```
TCP packet, 52 bytes
```

```
TCP packet, 126 bytes
```

```
TCP packet, 52 bytes
```

```
TCP packet, 52 bytes
```

```
TCP packet, 52 bytes
```

# What's left to be desired

- Chain priority docs? (I'm not sure if I understand how chain priorities are supposed to work or if they work at all; unsuccessful in tests)
- eBPF; using IMA; and does IMA solve any of the known sandboxing problems of eBPF? <https://lwn.net/Articles/886575/> | TPM 2.0 is supported for EC2 instances now: <https://aws.amazon.com/blogs/aws/amazon-ec2-now-supports-nitrotpm-and-uefi-secure-boot/>