# Handling IPsec with Foomuuri

Foomuuri is a multizone bidirectional nftables firewall

Muuri is Finnish word for brick or stone wall

# Foomuuri features

- Zone-based firewall
- Bidirectional firewalling for inbound, outbound and forwarding
- From laptop to corporate firewall
- Rule language supports macros and templates
- IPv4 and IPv6 support
- SNAT, DNAT and maquerading
- IPsec policy matching

# How foomuuri came to be

- I had discussion with Pablo about firewall software on linux at London IPsec workshop 2022
- After workshop Kim Heino and I had a discussion and we decided to create a completely new firewall product
- Kim wrote simple nftables firewall manually to test the idea
- At the beginning of the 2023 he started to write firewall generator with python
- In one month product was good enough and I replaced our corporate firewall software with foomuuri
- Two weeks after that software was released on https://github.com/FoobarOy/foomuuri
- Today foomuuri is available on multiple distros

# IPsec setup on foomuuri

- Traffic with source IPsec, you use sipsec
- Traffic with destination IPsec, you use dipsec
- Nftables equivalents:

```
sipsec == “meta ipsec exists”
-sipsec == “meta ipsec missing”

dipsec == “rt ipsec exists”
-dipsec == “rt ipsec missing”
```

# Server with IPsec

```
zone {
  localhost     # firewall itself
  public eth0
}

public-localhost {
  ping  saddr_rate "5/second burst 20"
  dhcp-client
  dhcpv6-client
  sipsec  ssh   # IPsec secured ssh
  ipsec
  drop log
}
```

```
localhost-public {
  dhcp-server
  dhcpv6-server
  domain
  domain-s
  dipsec  mysql  daddr 10.58.30.5
  ping
  http
  https
  ipsec
  ssh
  reject log
}
```

# Netfilter packet flow (simplified)

- Prerouting → filter → postrouting
- DNAT (destination nat) handles in prerouting
- firewall happens in filter
- SNAT/MASQUERADE (source nat) handles in postrouting

# NAT to IPsec tunnel

```
# IPsec tunnel between 198.51.100.0/24 <==> 192.0.2.5/32
iplist {
  @lan_net 192.168.5.0/24
  @remote_net 198.51.100.0/24
}
macro {
  default-ip 192.0.2.4
  secondary-ip 192.0.2.5
}
snat {
  oifname eth1  saddr @lan_net  daddr @remote_net  -dipsec  snat to secondary-ip
  oifname eth1  saddr @lan_net                     -dipsec  snat to default-ip
}
```

# DNAT from IPsec to lan server

```
# IPsec tunnel between 198.51.100.0/24 <==> 192.0.2.5/32
iplist {
  @lan_net 192.168.5.0/24
  @remote_net 198.51.100.0/24
}
macro {
  web-server 192.168.5.6
}
dnat {
  sipsec  iifname eth1  saddr @remote_net \
    daddr external-ip  dnat to web-server
}
public-internal {
  sipsec  https  saddr @remote_net  daddr web-server
  Sipsec  ping  saddr @remote_net  daddr web-server
}
```

# Map roadarriors to internal zone

```
zone {
  localhost
  public eth1
  internal eth0
}

macro {
  roadwarrior 192.168.4.0/24
}

zonemap {
  sipsec  szone public  saddr roadwarrior  new_szone internal
  dipsec  dzone public  daddr roadwarrior  new_dzone internal
}
```

# Map IPsec from public to vpn zone

```
zone {
  localhost
  public eth1
  internal eth0
  vpn   # empty zone
}

zonemap {
  sipsec  szone public  new_szone vpn
  dipsec  dzone public  new_dzone vpn
}
```

# How to handle special cases

- How to handle special nft features foomuuri doesn’t support?

  nft "<your-nft-command>"

# Questions?

- Answers: Foomuuri documentation
  https://github.com/FoobarOy/foomuuri/wiki