In this talk

- What is SURFs usecase for NFV?
- Our experiences building a NFV infrastructure
- What does our NFV infrastructure look like
**SURFfirewall**

Built upon several building blocks in SURF Network Orchestrator:
- SURFinternet
- L2VPN
- L3VPN
- FW

Usable in any configuration
Physical firewalls in central location
What about other services?

Use cases:
- Routers
- VPN concentrators
- Wireless controllers
- Switches
- EduVPN
- .. etc

"Give me a fully licensed 1Gbit UTM capable firewall with such-and-such ruleset in Amsterdam between 9:00AM and 4:00PM on September 22nd"
Goals for NFV

• Provide additional network services for connected institutes
• On-demand
• Pay as you grow
• High throughput – low latency

"Give me a fully licensed 1Gbit UTM capable firewall with such-and-such ruleset in Amsterdam between 9:00AM and 4:00PM on September 22nd"
PoCs

- Juniper Contrail
  Not the right fit
  Better for datacenters

- Vanilla Openstack with VPP dataplane
  Openstack is complex (!)
  No QinQ success story
What do we need for NFV at SURF?

- Virtualization engine
- Shared storage solution
- High speed dataplane
- Workflow engine

https://github.com/ansible/awx
https://ceph.io
https://fd.io
NFV technology domain

- Handles compute stuff
- In-house developed
- Based on ETSI NFV-MANO & NFVi
Payload from orchestrator

- Service version
- Availability zone
- State
- Identifier
Customer information
Update project ticket
Create circuits for impact/monitoring
Reserve p2p prefixes

- Create IP-gateways
- Create circuits
- Request license
- Configure connectivity
- Prepare Fortimanager

Validate everything
Put in sync