Selected Aspects of Self-Driving Networks in the bwNET2020+ Project

3. KuVS Fachgespräch „Network Softwarization“

Philipp Wolter (KIT)

Research and innovative services for flexible networks in Baden-Württemberg

Partners, Funding and current Phase

universität ulm

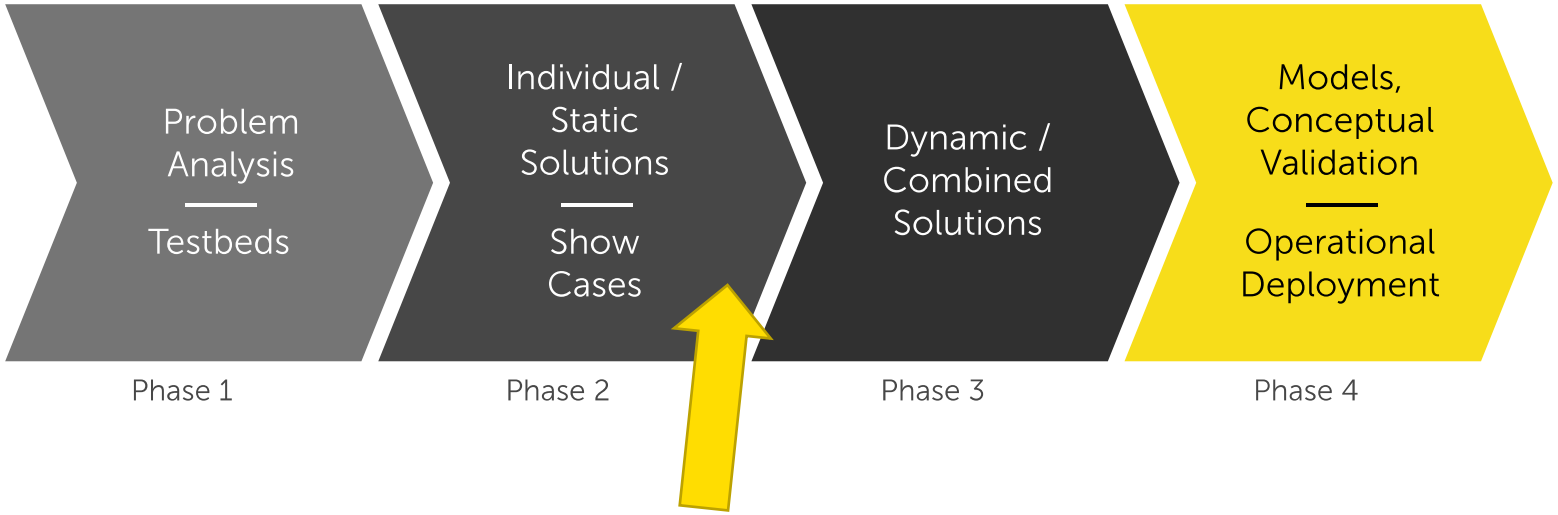
Karlsruher Institut für Technologie

EBERHARD KARLS UNIVERSITÄT TÜBINGEN

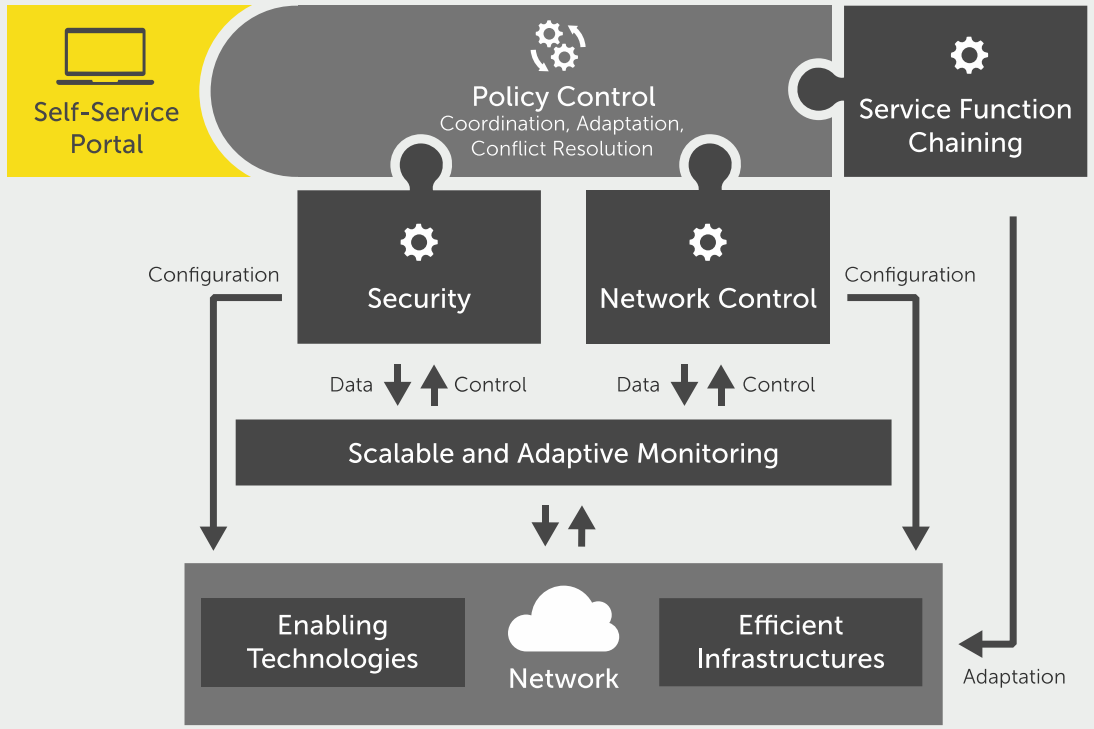
Hochschule Karlsruhe Technik und Wirtschaft
UNIVERSITY OF APPLIED SCIENCES

BelWü
Landeshochschulnetz Baden-Württemberg

Baden-Württemberg
MINISTERIUM FÜR WISSENSCHAFT, FORSCHUNG UND KUNST

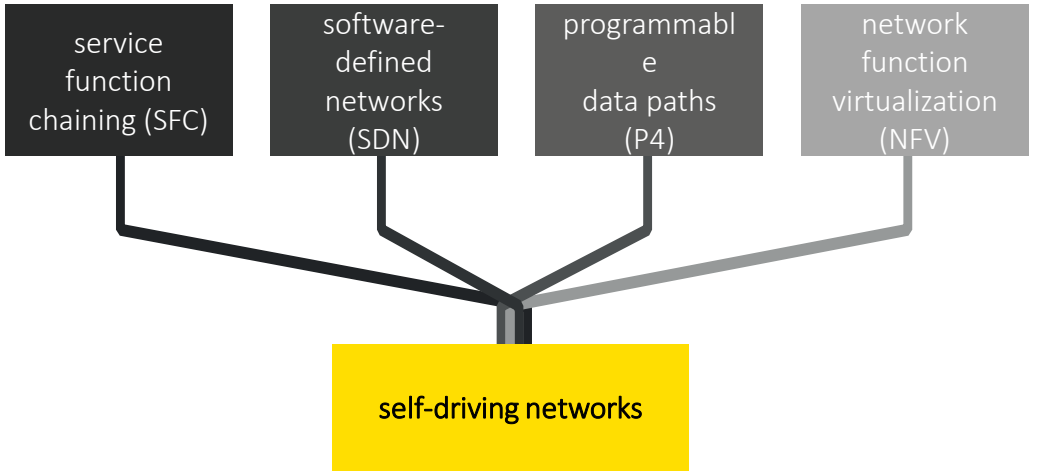


Vision of Self-driving Networks



- Policy Control is the core component responsible for compliance with SLAs and network policies derived from intents
- Users should be able to easily define network services via self-service portal.

Enabling Technologies:



Use Cases

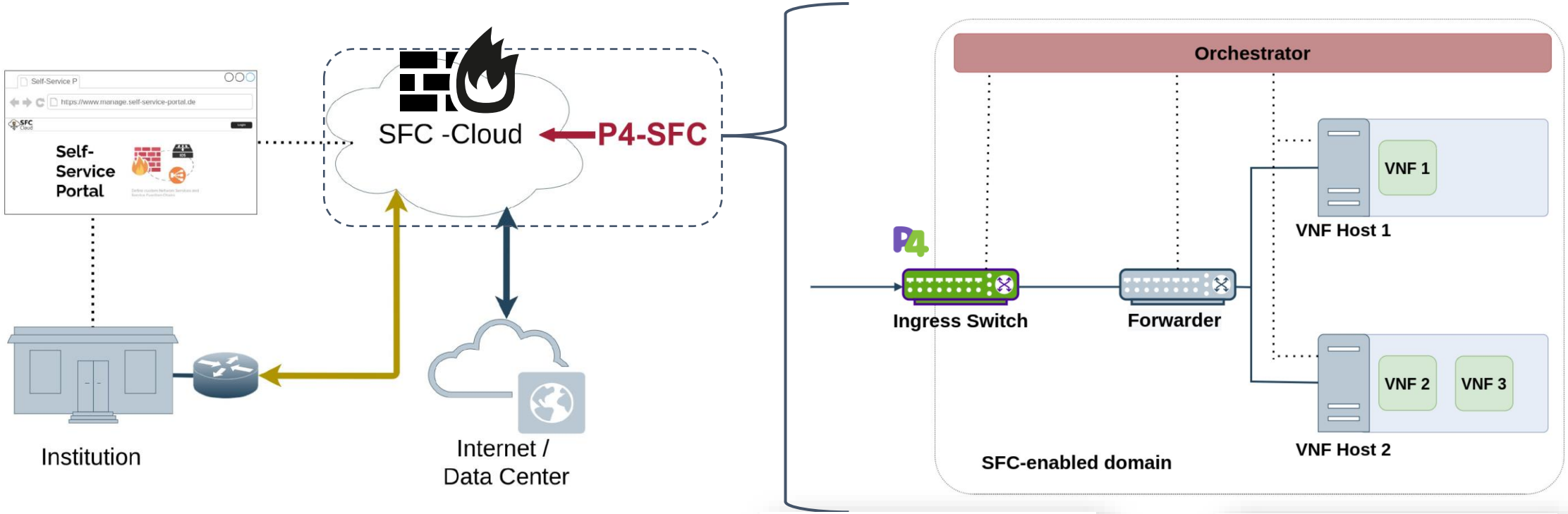
Firewall as a Service

Access via WIFI and 5G networks

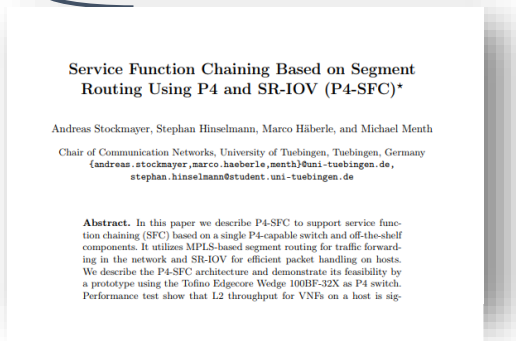
Transfer of large research datasets

Improved security in campus networks

Use-Case 1: Firewall as a Service based on P4-SFC



- Web-based management of Service Functions and Chains
- Automated deployment in SFC Cloud
- 100G ready



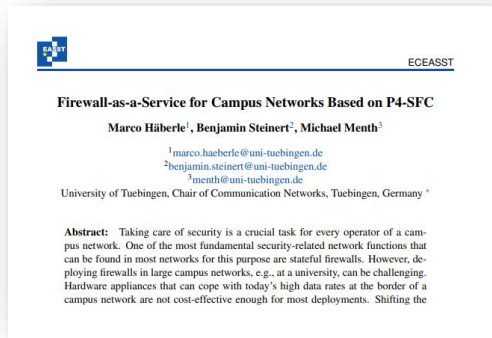
Service Function Chaining Based on Segment Routing Using P4 and SR-IOV (P4-SFC)*

Andreas Stockmayer, Stephan Hinselmann, Marco Häberle, and Michael Menth

Chair of Communication Networks, University of Tuebingen, Tuebingen, Germany
{andreas.stockmayer,marco.haeberle,menth}@uni-tuebingen.de,
stephan.hinselmann@student.uni-tuebingen.de

Abstract. In this paper we describe P4-SFC to support service function chaining (SFC) based on a single P4-capable switch and off-the-shelf components. It utilizes MPLS-based segment routing for traffic forwarding in the network and SR-IOV for efficient packet handling on hosts. We describe the P4-SFC architecture and demonstrate its feasibility by a prototype using the Tofino Edgecore Wedge 100BF-32X as P4 switch. Performance test show that L2 throughput for VNFs on a host is sig-

https://link.springer.com/chapter/10.1007/978-3-030-59851-8_19



ECEASST

Firewall-as-a-Service for Campus Networks Based on P4-SFC

Marco Häberle[1], Benjamin Steinert[2], Michael Menth[3]

[1]marco.haeberle@uni-tuebingen.de
[2]benjamin.steinert@uni-tuebingen.de
[3]menth@uni-tuebingen.de
University of Tuebingen, Chair of Communication Networks, Tuebingen, Germany

Abstract: Taking care of security is a crucial task for every operator of a campus network. One of the most fundamental security-related network functions that can be found in most networks for this purpose are stateful firewalls. However, deploying firewalls in large campus networks, e.g., at a university, can be challenging. Hardware appliances that can cope with today's high data rates at the border of a campus network are not cost-effective enough for most deployments. Shifting the

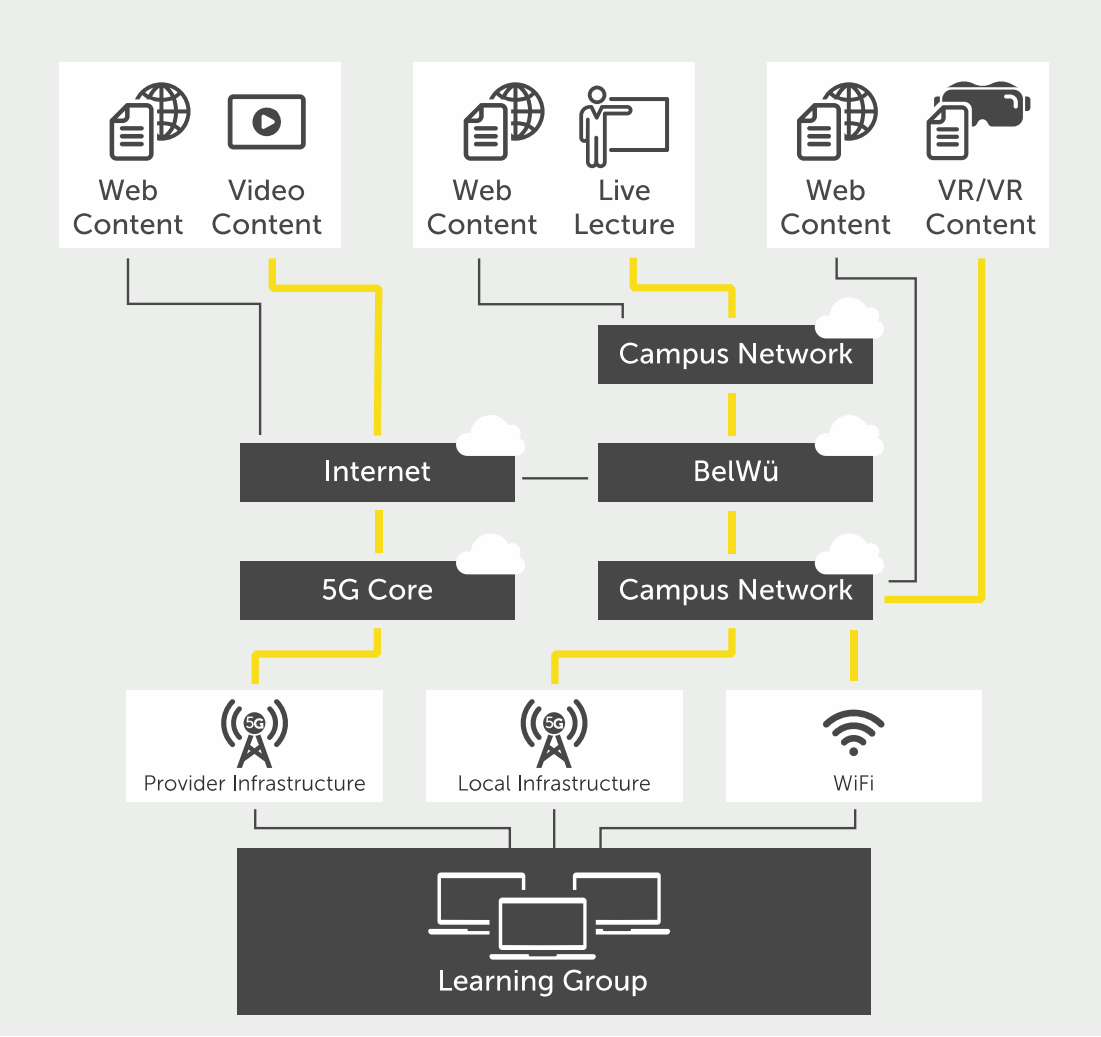
https://journal.ub.tu-berlin.de/eceasst/article/view/1185

Use Case 2

Access via WIFI and 5G networks

Approach

- MultiPath-TCP deployment in WiFi 5/6 and 5G networks
- Investingate and adapt MP-TCP to new wireless technologies
- Establish cross-technology control of mobile access by users or to content on campus to best utilize wireless technologies and increase QoE in learning groups.

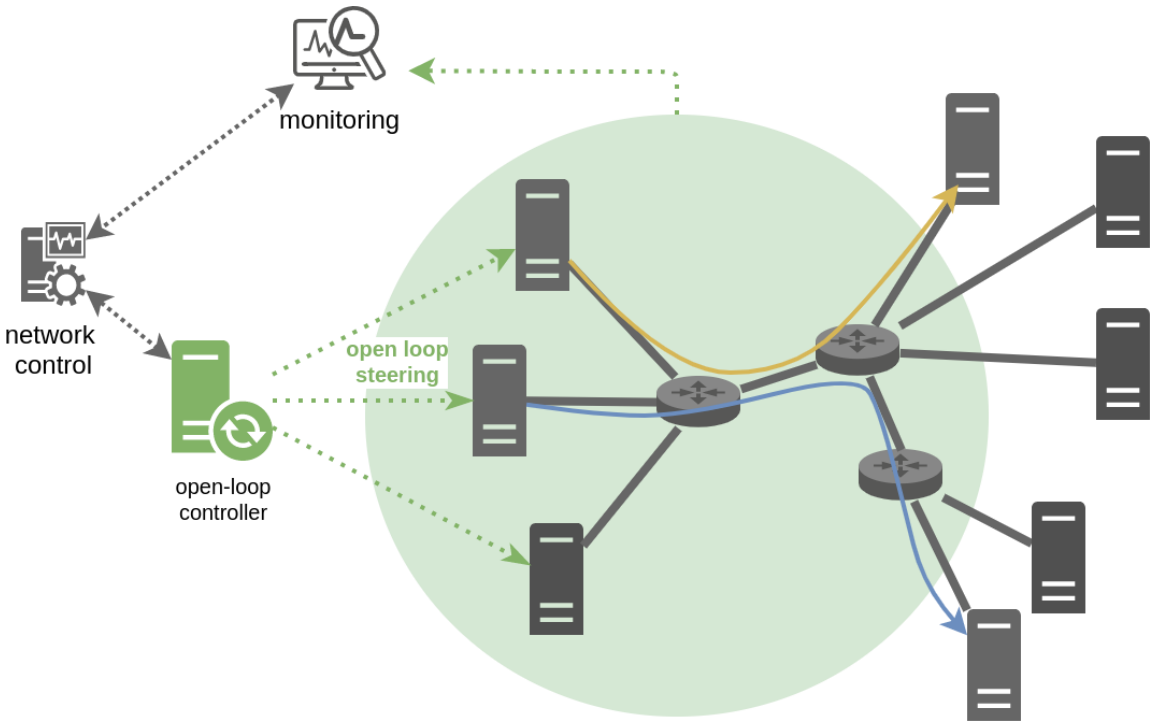


Use-Case 3: Open-Loop Congestion Control

Open-Loop Congestion Control

- Utilizes multiple inputs to determine state (Combined viewpoints of senders, network, receivers)
- Combination of explicit network state information over time & space (Consecutive & parallel flows)
- Steering of multiple senders based on combined knowledge

-> Faster and more efficient
congestion resolution (and prevention)

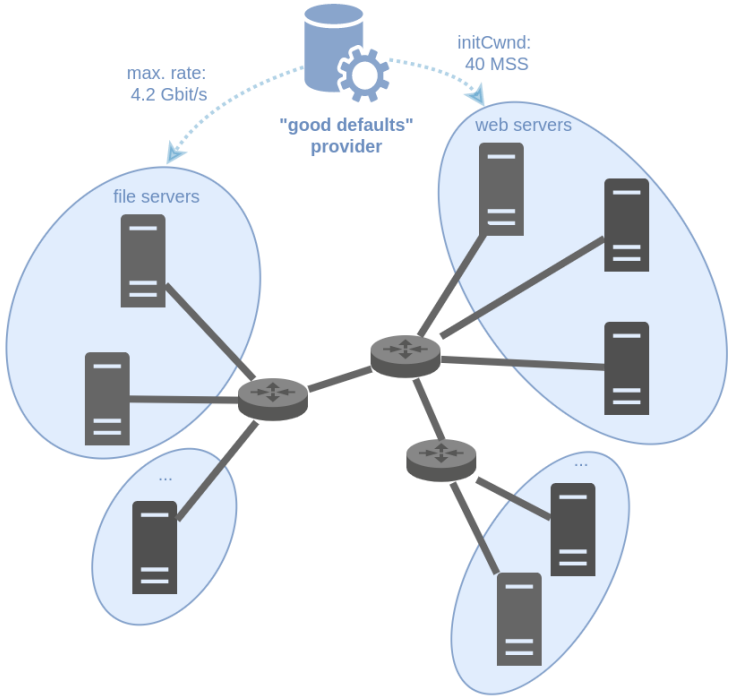


Congestion control: 2 flavors

Daily/Hourly “Good Defaults”

-> broad defaults for many (similar) services

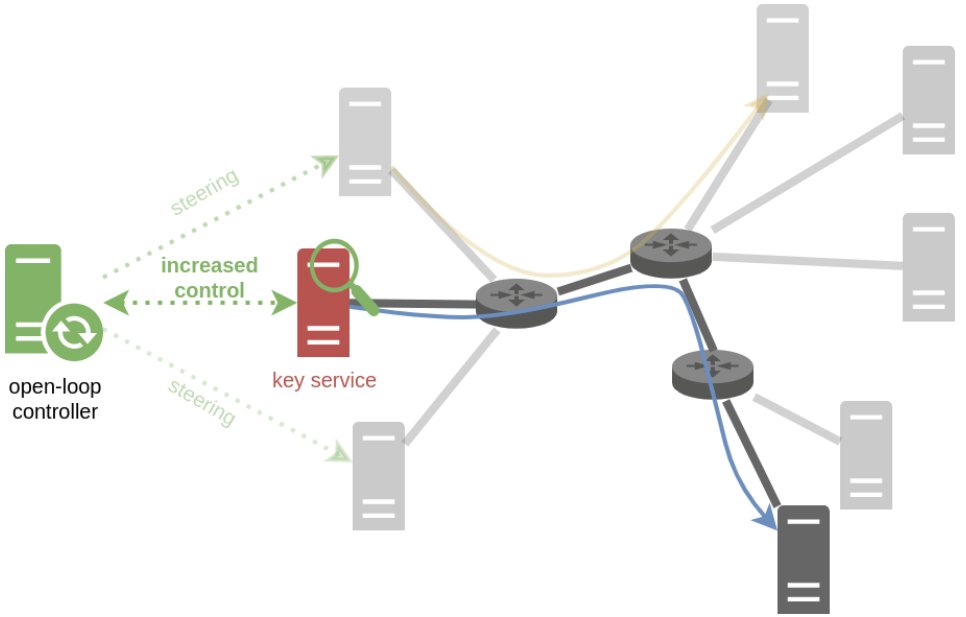
-> per-service default optimizations



Real-time Online Supervision

-> increased control (beyond steering)

-> per-flow detailed optimization



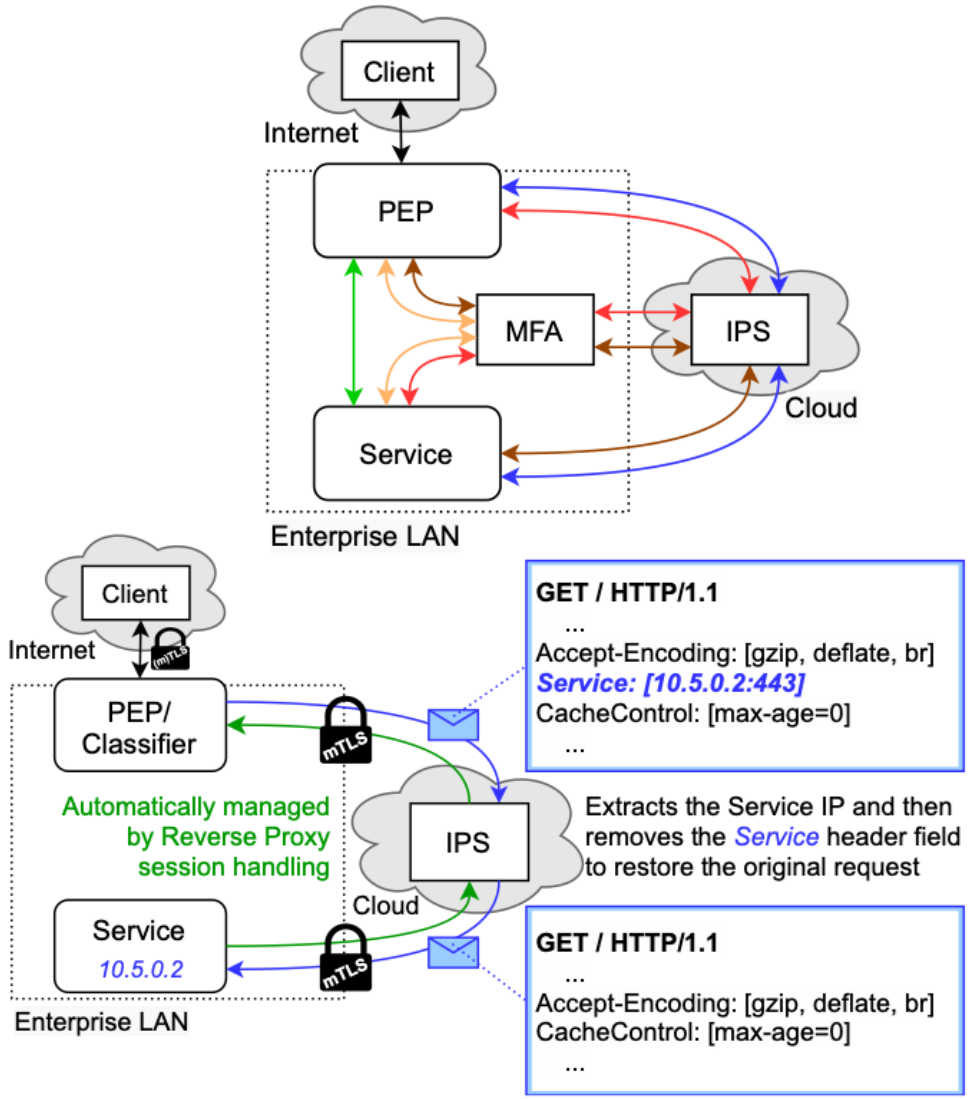
Use-Case 4:
Zero Trust Service Function Chaining (ZTSFC) in Campus Networks

- Motivation: Poor security of university services:
  - Perimeter-based security.
  - Authentication with password only.
  - Coarse-grained role-based authorisation (RBAC).
- With ZTSFC for Campus Networks we achieve:
  - Flexible integration of security components anywhere in the network.
  - Multi-factor authentication for all service access.
  - Fine-grained authorisation through trust score calculation.

Zero Trust Service Function Chaining (ZTSFC)

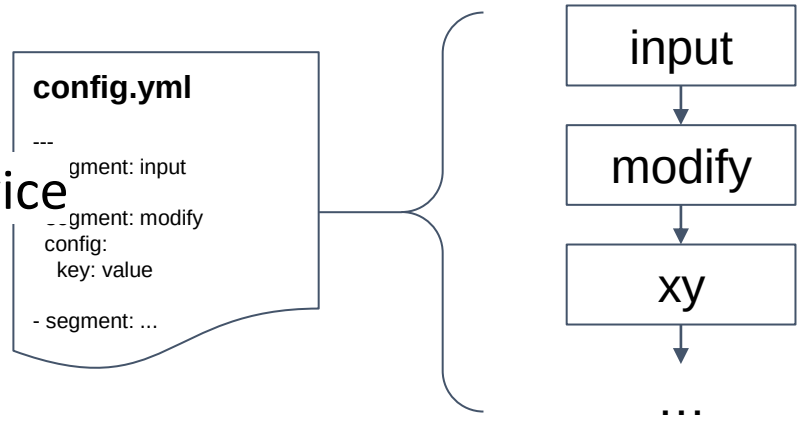
And how does it work (with HTTPS)?

- Policy Enforcement Points (PEP) act as entry points to the network:
  - Each access is authenticated and encrypted.
  - Least-Privilege authorisation of user, device and context
  - Trust-based application of security functions to the packets
  - SFC-based packet forwarding
  - Forwarding information can be embedded into the HTTP headers



Real-Time Flow Processing

Custom tooling: **flowpipeline**



- Receive, modify, export Flow streams as a pub/sub service
- Configuration-defined, easily deployed
  - single (static) binary, container, part of a SFC
- IPFIX, Netflow and sFlow supported, as well as eBPF
- Different segments available for output, dataset generation, export, anonymization, or enrichment:

Prometheus MAXMIND kafka json / csv

SQLite SNMP influxdb

- Available here: https://github.com/bwNetFlow/flowpipeline

Next steps

- Use-Cases
  - Finalize demonstrators, roll things out
  - Scale them up
  - not just resolve issues, also prevent (e.g with reinforcement learning)
  - preventive and automated responses to security events
- Monitoring
  - Improved data correlation and real-time analysis
- Overall Project
  - Proof solutions at scale
  - Knowledge transfer → datacentres
  - Conceptual evaluation
  - operational deployment

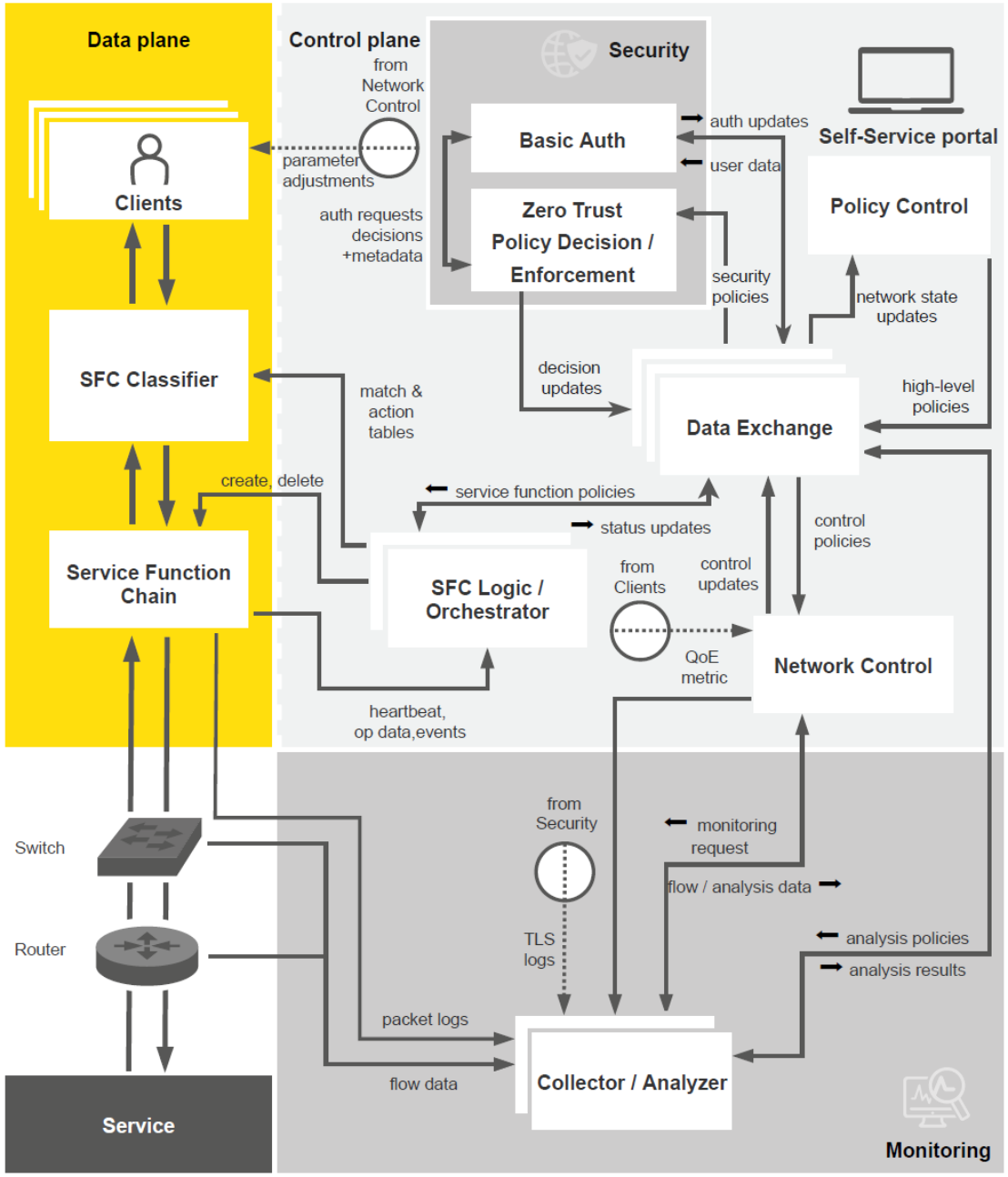
Thank you for your attention

Any questions?

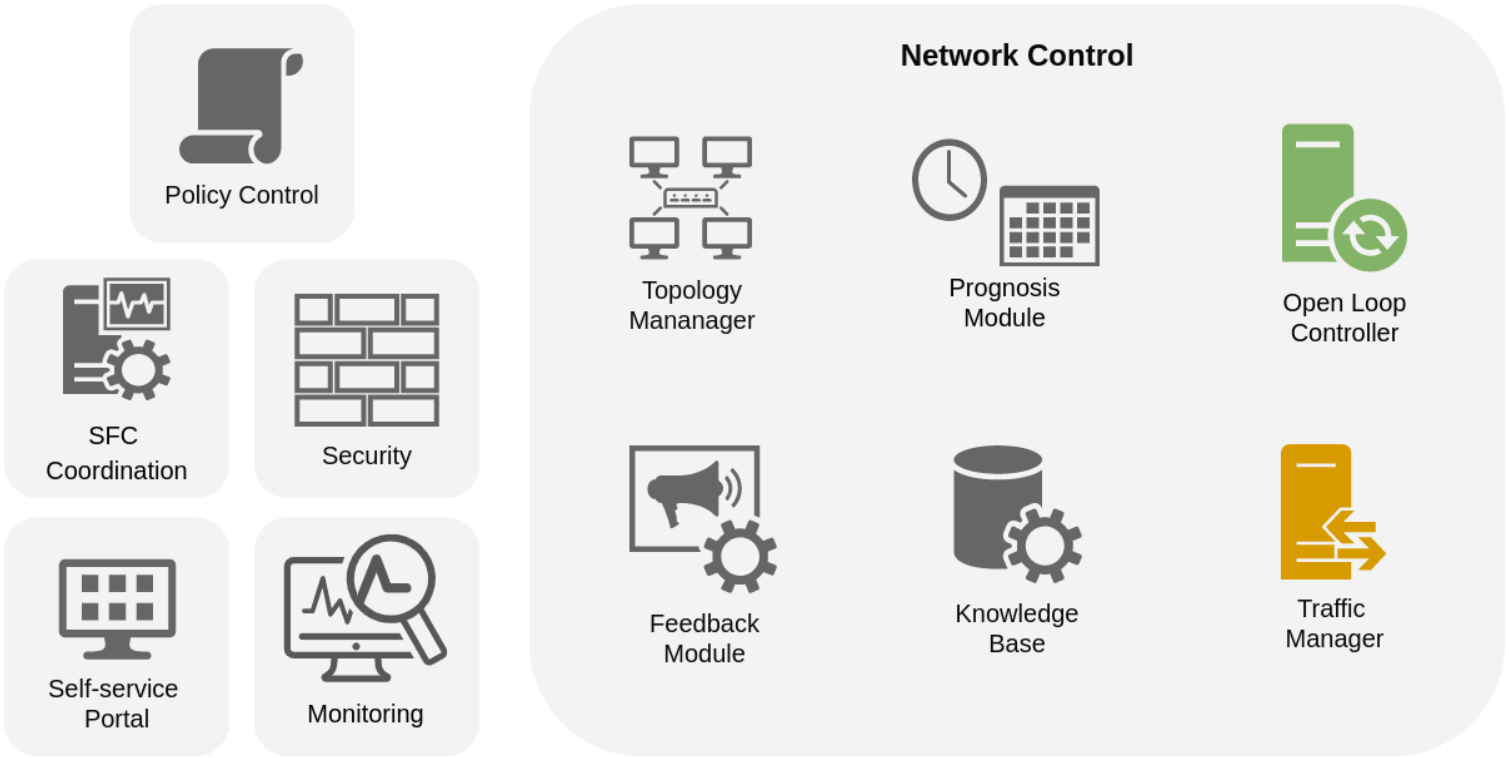
philipp.wolter@kit.edu

Extra Slides

Simplified Architecture



Planned Work: Network Control



- Open Loop Controller
  - **short-term** steering of flows

  -> resolve congestion

- Traffic Manager
  - **mid-/long-term** traffic scheduling
  - routing changes
  - placement of services
  - traffic engineering

  -> prevent congestion