Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

Institute of Computer Science
Chair of Communication Networks
Prof. Dr. Tobias Hoßfeld

VIPNANO: Monitoring of Virtual Private Cloud Networks for Automated Anomaly Detection

Marleen Sichermann, Katharina Dietz, Jochen Kögel, Sebastian Meier,
Stefan Geißler, Tobias Hoßfeld

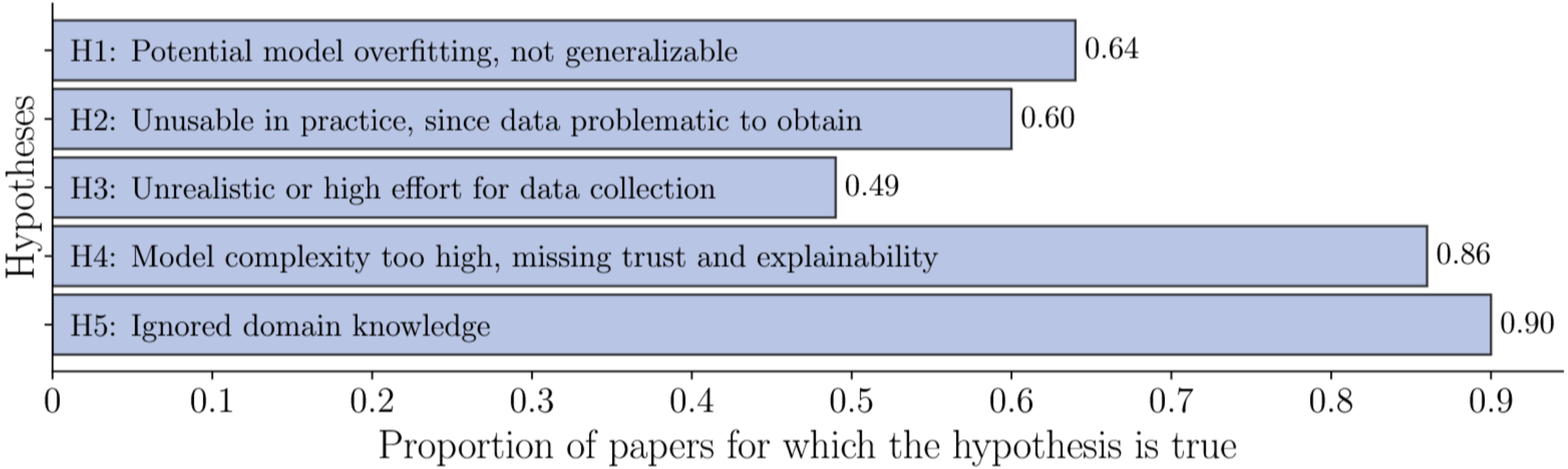
info3.org

Monitoring in Heterogenous Virtual Private Clouds Deployments

- Shift from on-premise solution towards heterogenous cloud environments
  → Increasingly complex network management

- Challenges
  - Connecting infrastructure segments across cloud provider boundaries
  - Integrating legacy on-premise services
  - Monitoring and representing the state of such heterogenous deployments
    - Necessary to detect anomalies, outages, or malicious attacks
    - Established approaches often fall short in applicability, scalability, or adaptability
      - Reliance on unrealistic input, e.g., full-packet resolution
      - Impractical computational overhead → not suited for large-scale networks
      - Lack of real-world validation

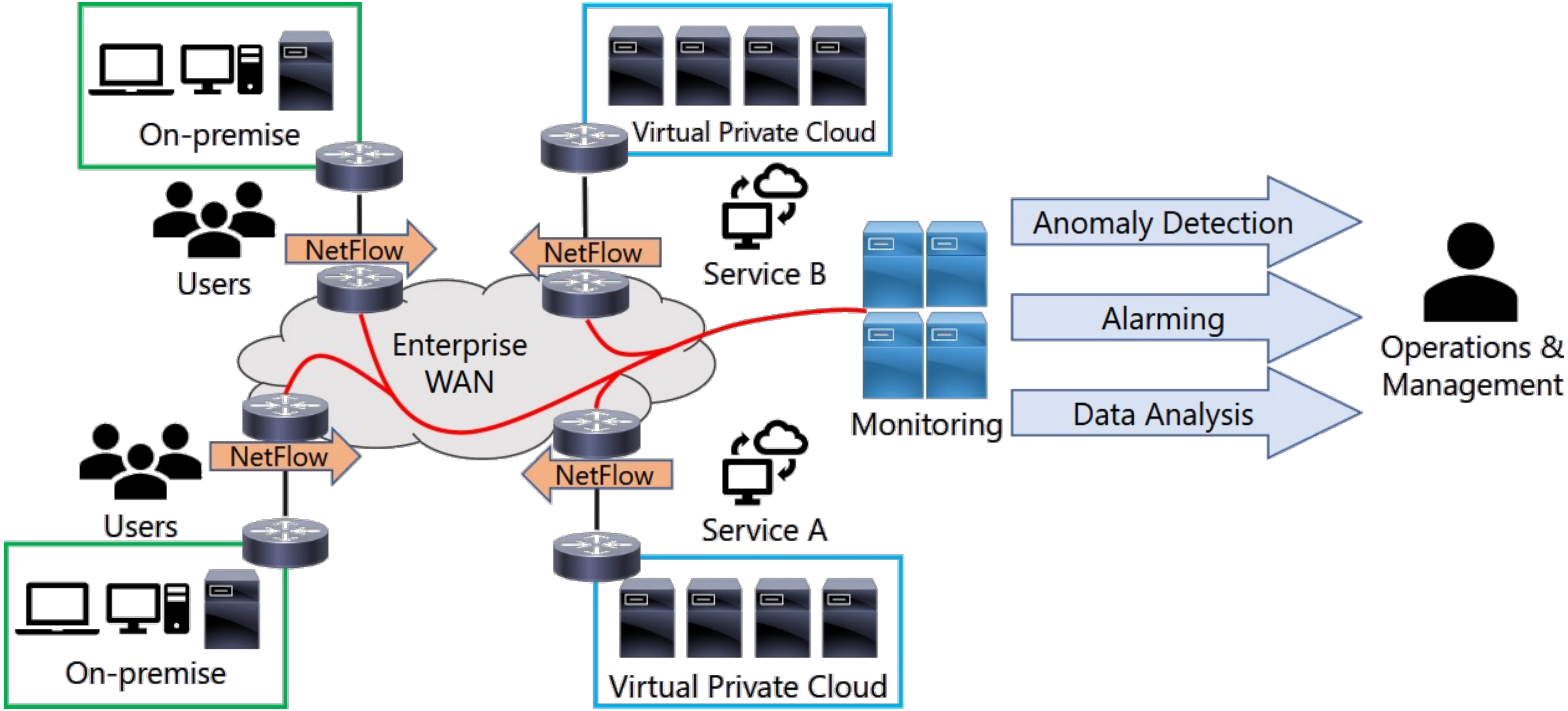
Gap in Literature



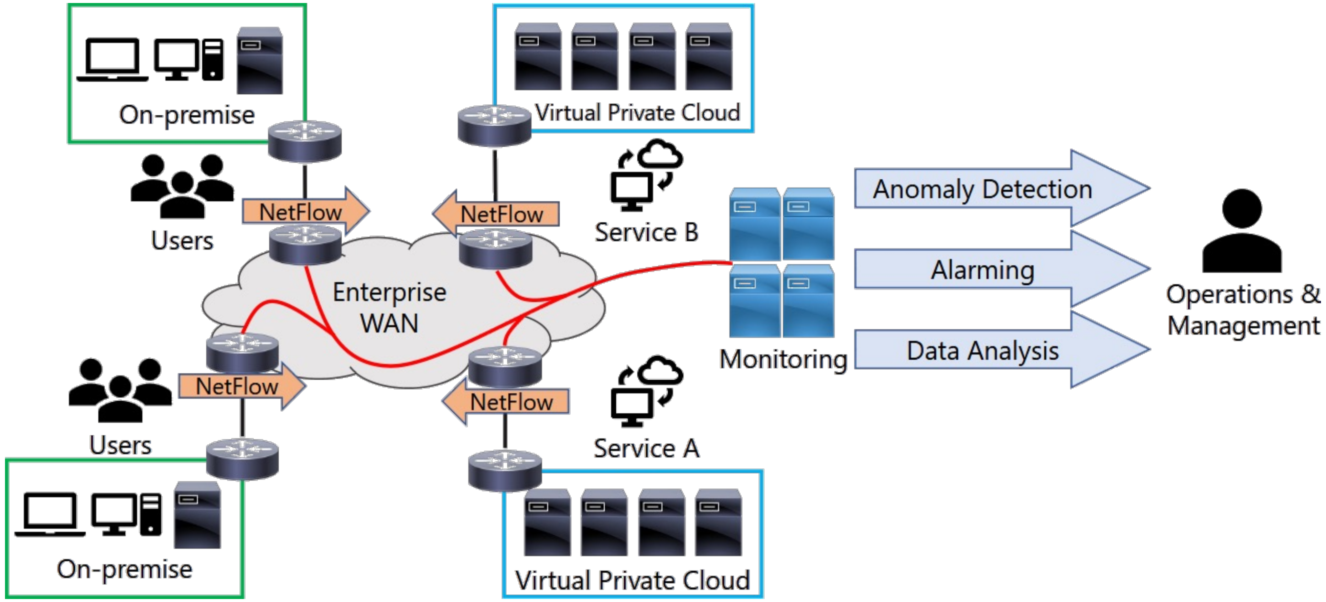
- Result of our comprehensive literature survey on intrusion and anomaly detection
- Establishment of 17 hypotheses, why academic research lacks practical adoption

Dietz, Katharina, et al. "The missing link in network intrusion detection: Taking AI/ML research efforts to users." *IEEE Access* (2024)

Heterogenous Cloud Scenarios

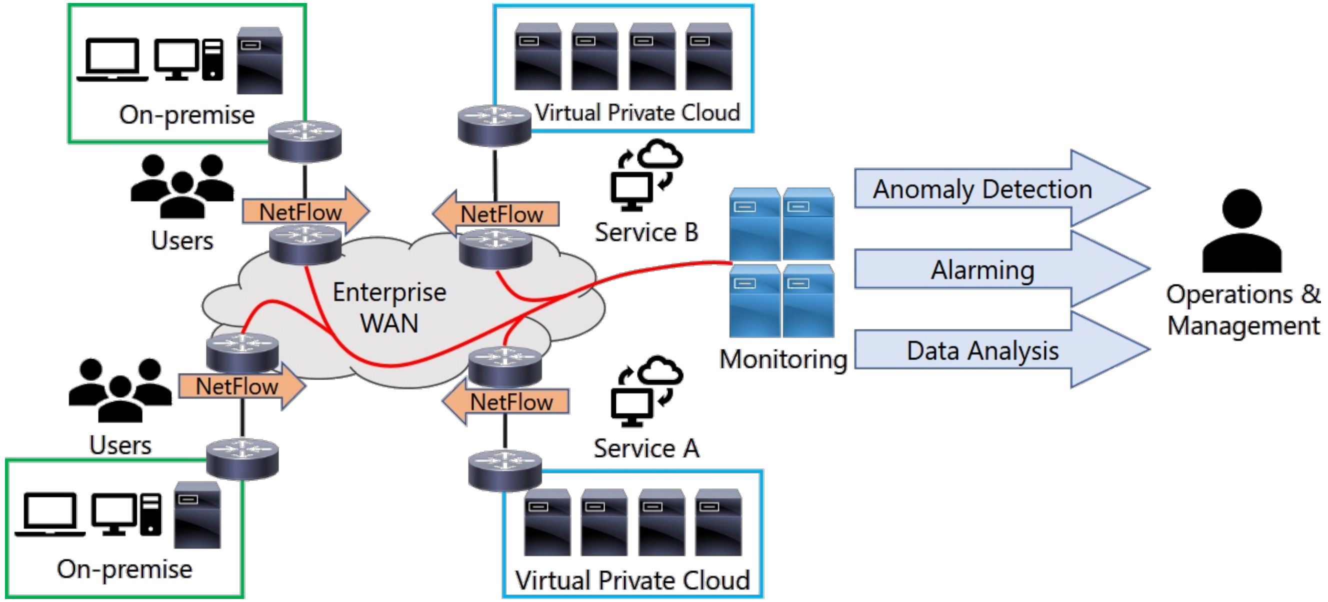


Heterogenous Cloud Scenarios



- Creation of a unified monitoring framework remains challenging
  - Variations in data formats, logging standards
  - Dynamic nature of these environments
    → Fluctuating workloads, frequent configuration changes
  - Scale of large enterprise systems

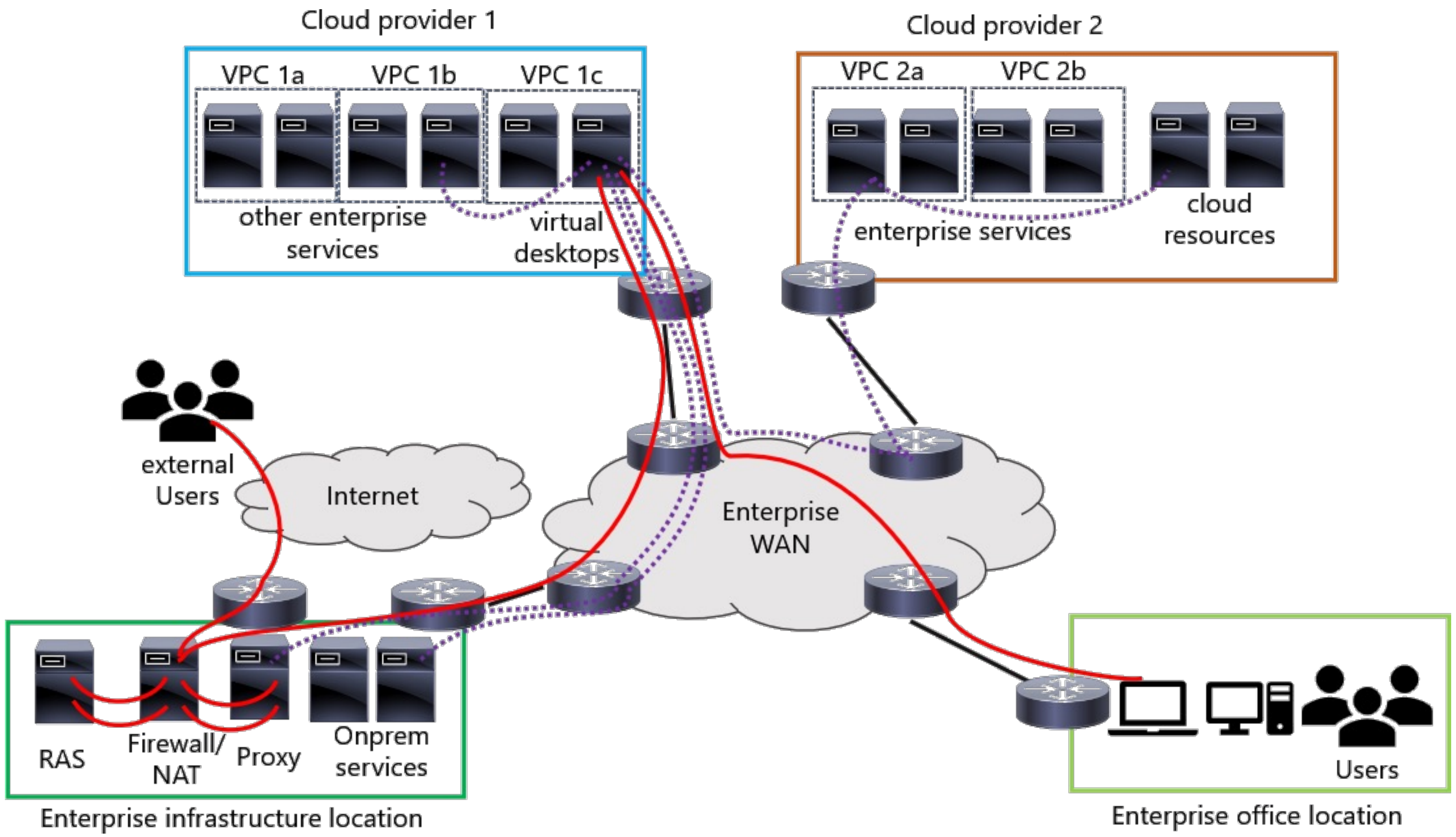
Heterogenous Cloud Scenarios



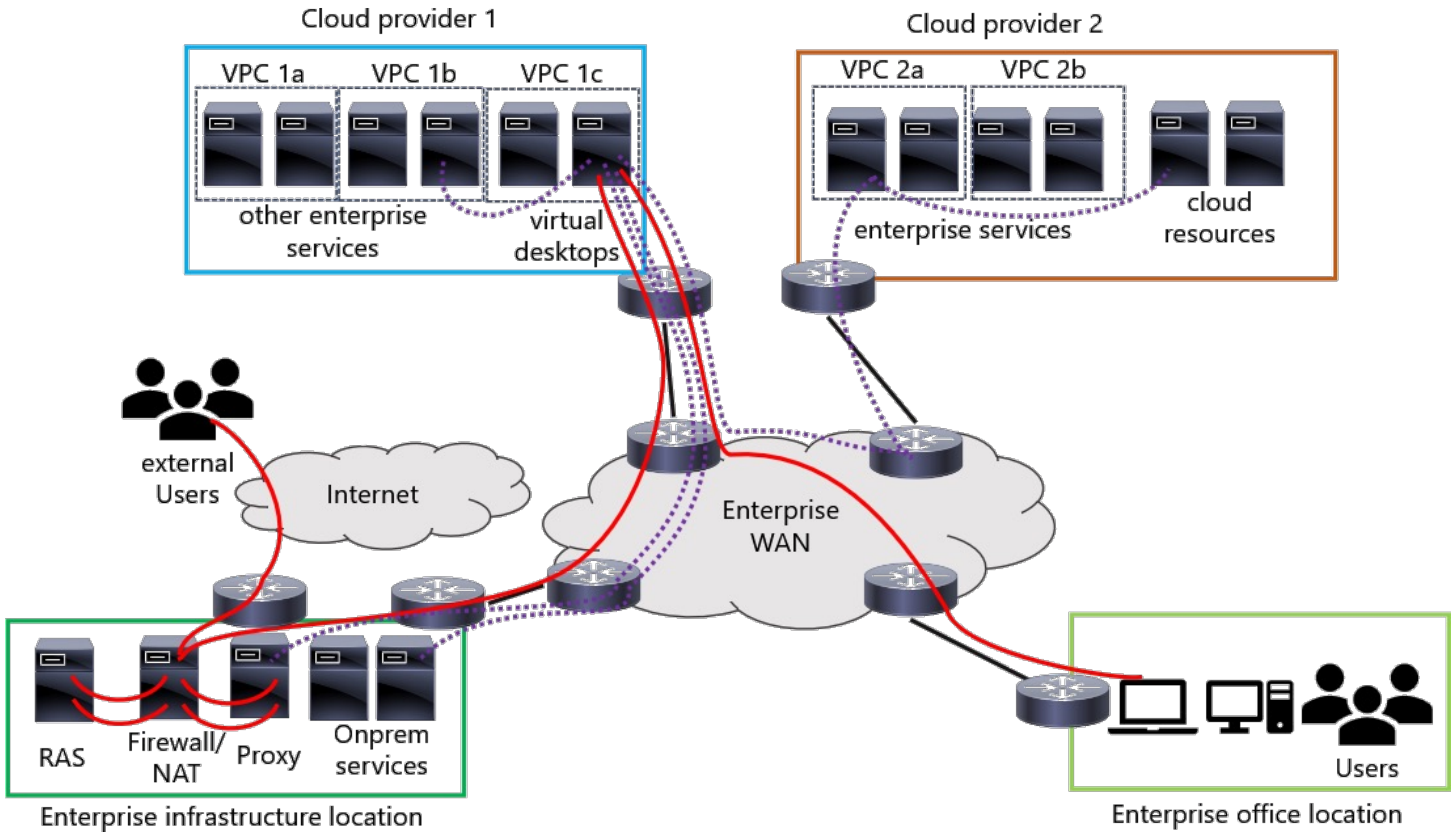
- Monitoring with NetFlow
  - Only available at specific points
  - Aggregated by flows instead of packet-level information
  - In extremely large-scale deployment may only be available for a short time
  - Potentially masking or distorting the signature of an anomaly through aggregation

Exemplary Multicloud Application

- Real-world application running in a multi-cloud environment at a large German transportation company
- Virtual desktop service via Citrix
- Valuable insights through NetFlow data and contact with network operation and application team



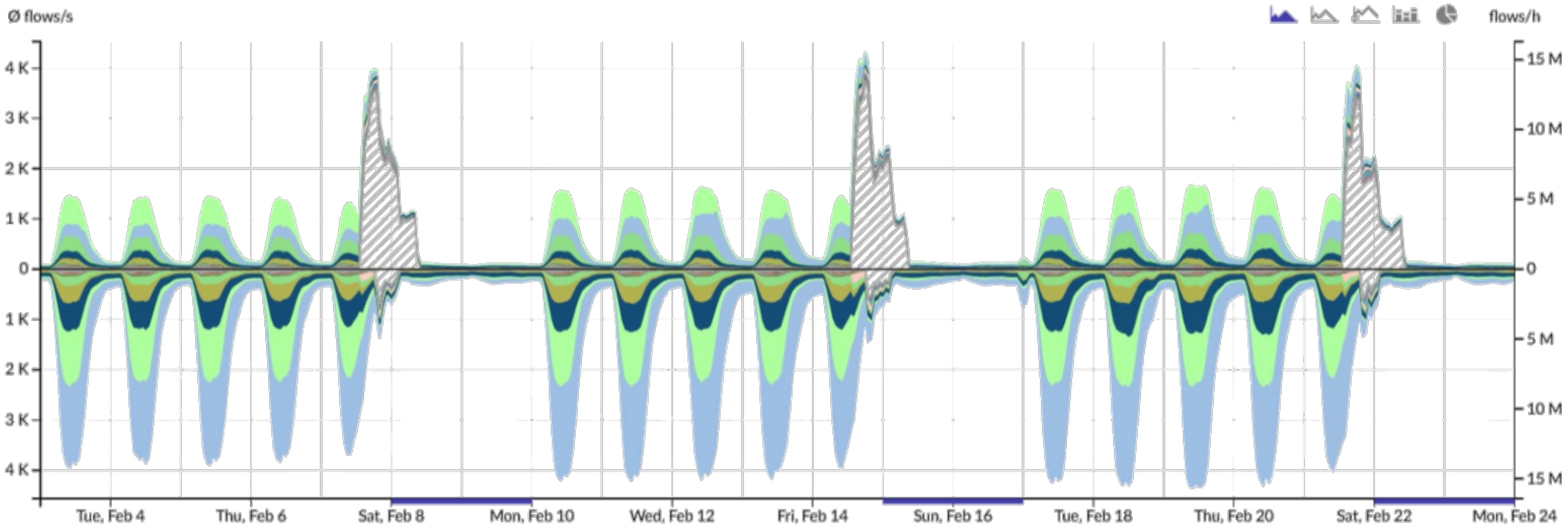
Exemplary Multicloud Application



- Characteristics
  - Asymmetric traffic pattern
  - Downstream video requires high bandwidth
  - Delay sensitive in both directions

- Dataset
  - NetFlow monitored at the enterprise WAN edge routers
  - Contains various (unlabelled) anomalies
  - 45.7 Billion flows recorded over 9 months

Anomaly Detection under Real World Constraints



- Absence of labelled data excludes supervised methods
- Current focus on baseline approaches due to seasonal nature of underling data
  - Weekly pattern (weekend/working days)
  - Scan traffic on Friday
  - Necessary differentiation between expected scheduled events and anomalies

Road Map

- Development of anomaly and network intrusion detection mechanism under real-world conditions
- Requirements
  - Acceptable computational overhead
  - Real-world validation
  - Working with highly aggregated NetFlow features
  - Overcome absence of labels
  - Follow data protection laws

- Future Work
  - Enhancing NetFlow monitoring and aggregation by investigation of extractable features
  - Development of a human-in-the-loop mechanism to address missing labels
  - Pragmatic survey on applicability of academic approaches to our dataset