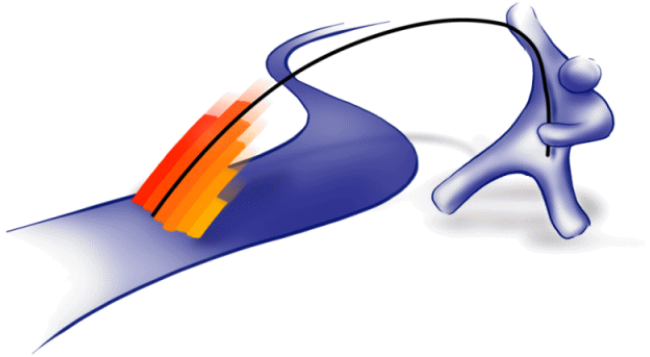
Flow Analysis in Heterogeneous Cloud Scenarios



{jochen.koegel,sebastian.meier,stefan.oettl}
@isarnet.de

vipnano

isarNet
Software Solutions GmbH

Outline

- IsarNet, IsarFlow and the VIPNANO project
- IsarFlow Overview and Monitoring Scenario
- AWS Flow Logs
- Design decisions for transcoding to IPFIX
- Summary

IsarNet Overview

- 1999: 5 founders (former System Engineers at Siemens) network consulting, workshops
- 2003: started **IsarFlow** as **software for flow analysis**
- 2025: 30 employees

- Located in Hallbergmoos (close to Munich Airport)

IsarFlow

IsarFlow: Official References

T Systems

DAIMLER

BT

MAN

ATRUVIA

MA14 Wir vernetzen Wien.

ÖBB

WIKA

APA AUSTRIAPRESSEAGENTUR

BITMARCK

VIPNANO Project

VIPNANO:
Monitoring of **Vi**rtual **P**rivate Cloud **N**etworks
for Automated **Ano**maly Detection
of Enterprise Applications in heterogeneous Networks

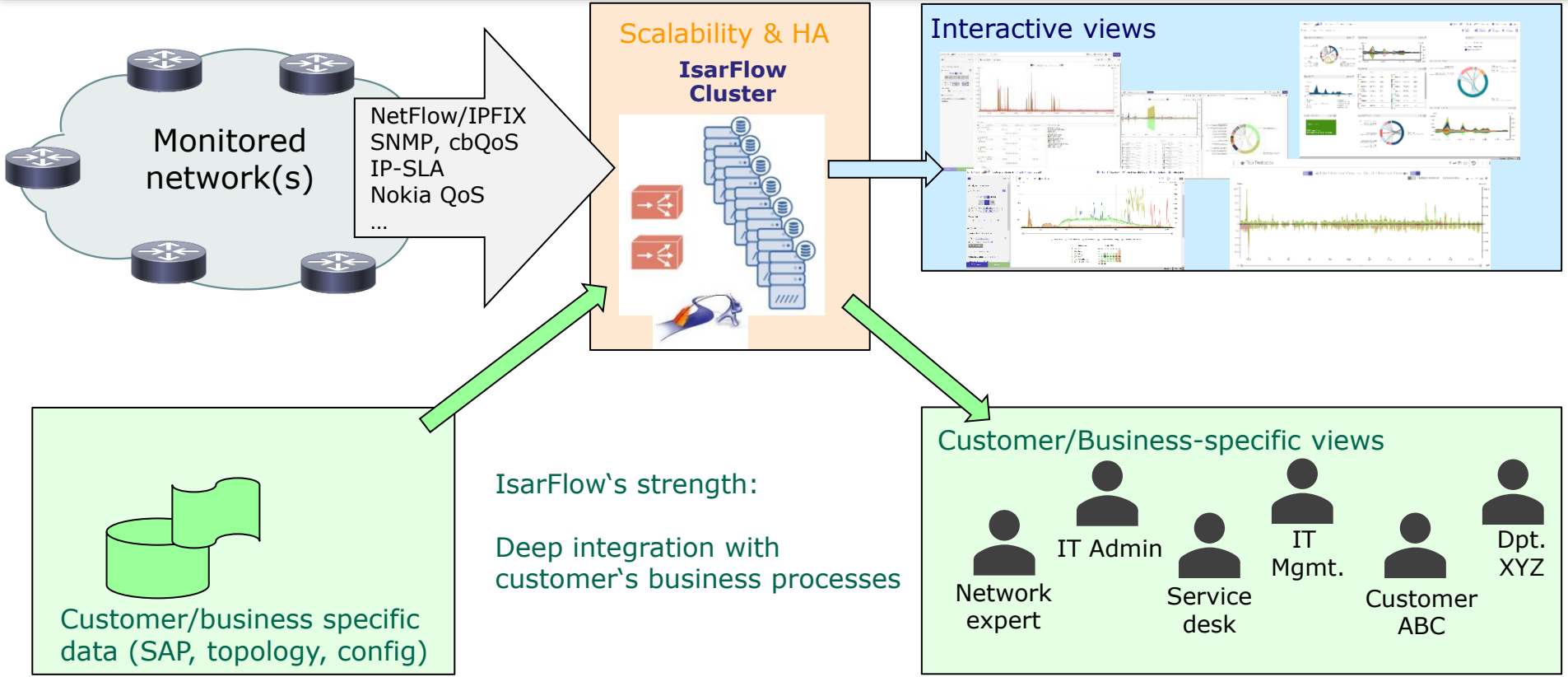
Partners

- IsarNet SWS GmbH, Munich
- Julius-Maximilians-Universität Würzburg (JMU)
  Chair of Communication Networks
- associated: DB Systel GmbH, Frankfurt

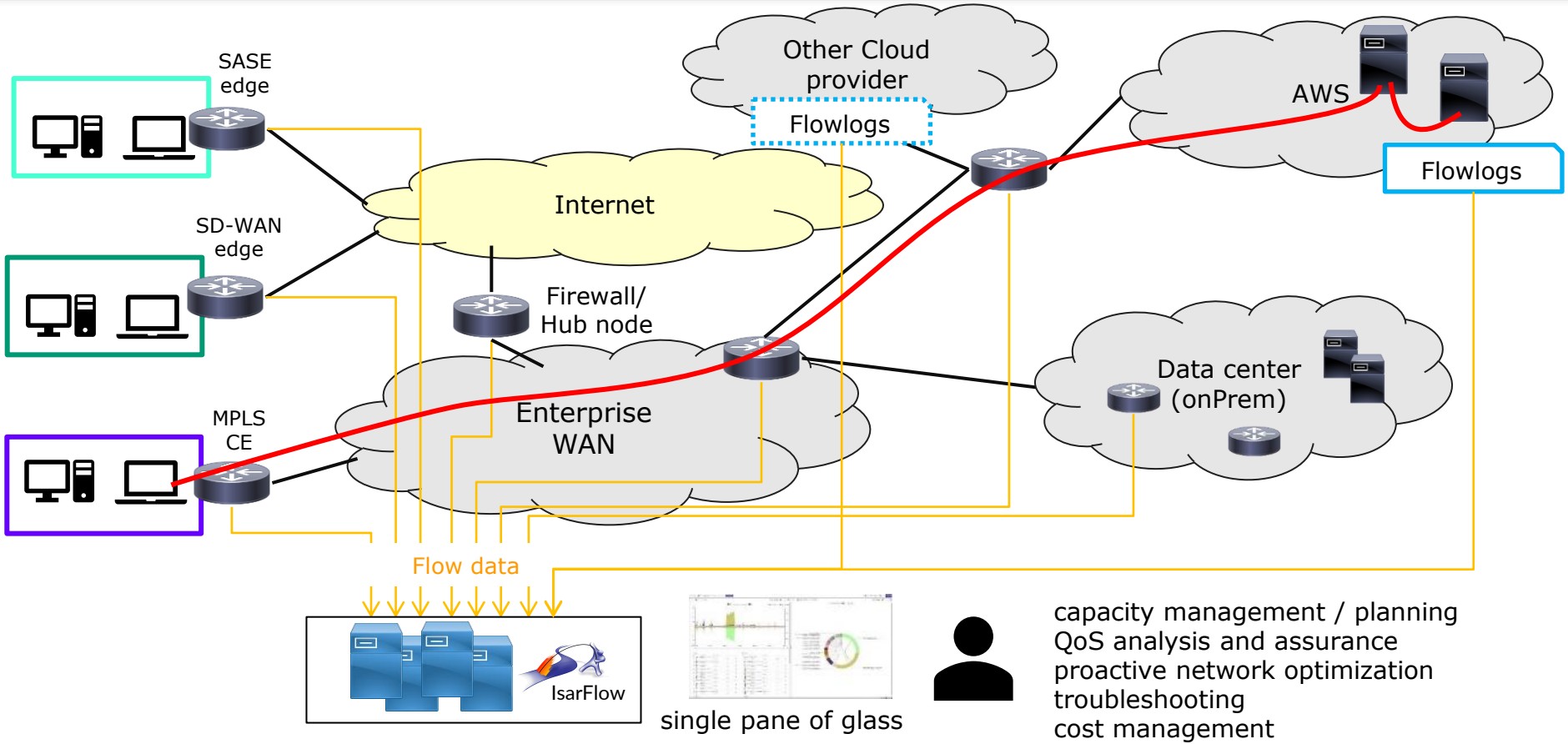
Funding

Bayerisches Staatsministerium für
Wirtschaft, Landesentwicklung und Energie

IsarFlow Overview

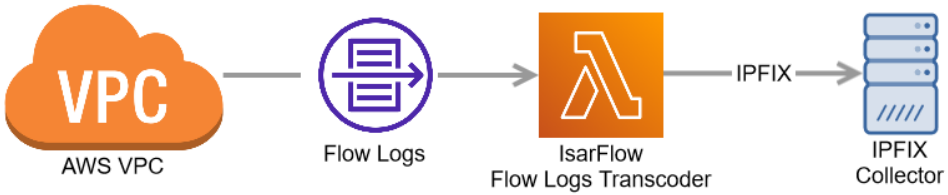


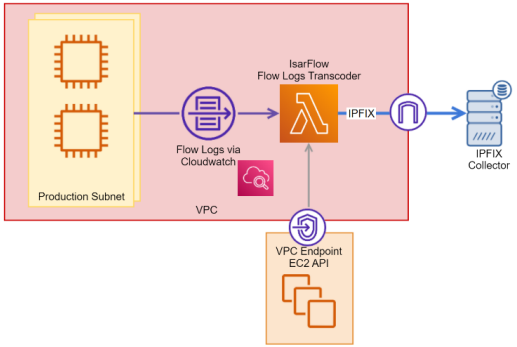
Monitoring Scenario



AWS Flowlogs

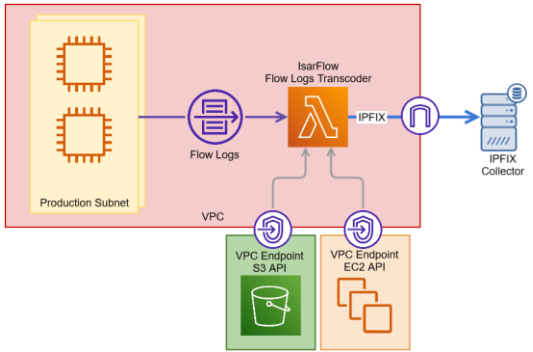
Integrating AWS Flowlogs via IPFIX





- Two applications available via
  AWS Serverless Application Repository
  - CloudWatch: FlowLogs-to-IPFIX-CWL
  - S3: FlowLogs-to-IPFIX-S3

- Unlocked on request for AWS accounts / organizations



AWS Flowlogs

IPFIX (IP Flow Information Export)

- standardized by IETF
- defines data model*, protocol, and architecture for flow information handling
- covers measurement data and related configuration data
- allows for vendor specific extensions (PEN concept)

AWS Flowlogs

- domain specific flow data (vpc, aws-account, …)
- allows for streaming & batch processing
- handling either via AWS SDK or export to standardized file format (csv, parquet)
- flow information / properties quite similar to IPFIX

→ How to map AWS Flowlog Data to IPFIX?

* https://www.iana.org/assignments/ipfix/ipfix.xhtml

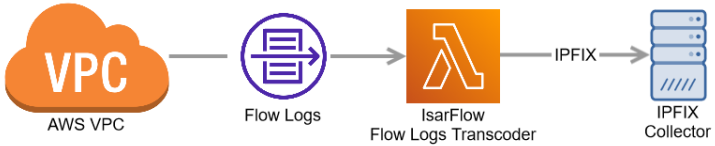
Flowlog Transcoding

Alternative 1: Proprietary Transcoding

- rely on IPFIX PEN concept for defining custom data model
- transfer Flowlog data „as is“
- modify IPFIX collector (+ Analysis Engine) to handle domain specific data

\+ simple (no) translation

\- vendor specific software modifications



Alternative 2: map to IETF/IANA Information Elements (IEs)

- translation: domain specific → standardized (if applicable/possible)

\- requires translation/transcoding

\+ no vendor specific software modifications (single pane of glass)

\+ enables 3rd parties to consume IPFIX stream without vendor specific knowledge

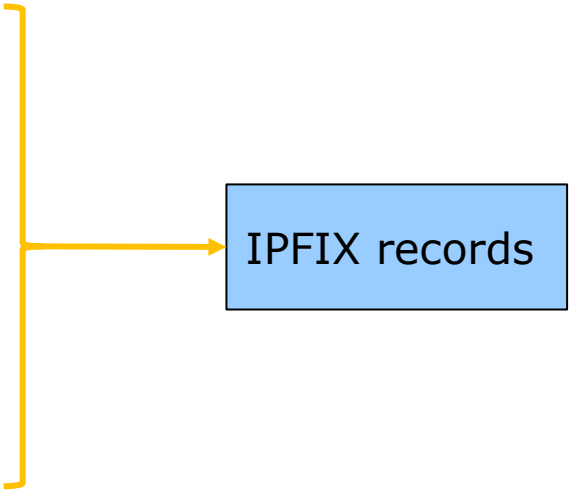
Flowlog Transcoding

Mapping of Flowlogs to IPFIX with default fields

```
version account-id     interface-id              srcaddr         dstaddr       srcport dstport protocol packets bytes start      end        action log-status
2       526716944320 eni-04787f938622c1ec2 89.248.165.109 172.31.43.65 57730   39713   6        1       40    1654234187 1654234243 ACCEPT OK
```

Flowlog field	IPFIX field	IPFIX IE No
version	-ignored-	
account-id	-ignored-	
log-status*	- ignore record, if not OK -	
action*	egressInterface (generated ID)	14
srcaddr*	sourceIPv4Address / sourceIPv6Address	8 / 27
dstaddr*	destinationIPv4Address / destinationIPv6Address	12 / 28
srcport*	sourceTransportPort	7
dstport*	destinationTransportPort	11
protocol*	protocolIdentifier	4
interface-id*	ingressInterface (generated ID)	10
packets*	packetDeltaCount	2
bytes*	octetDeltaCount	1
start*	flowStartSeconds	150
end*	flowEndSeconds	151
tcp-flags	tcpControlbits	6
flow-direction	flowDirection	61

*mandatory

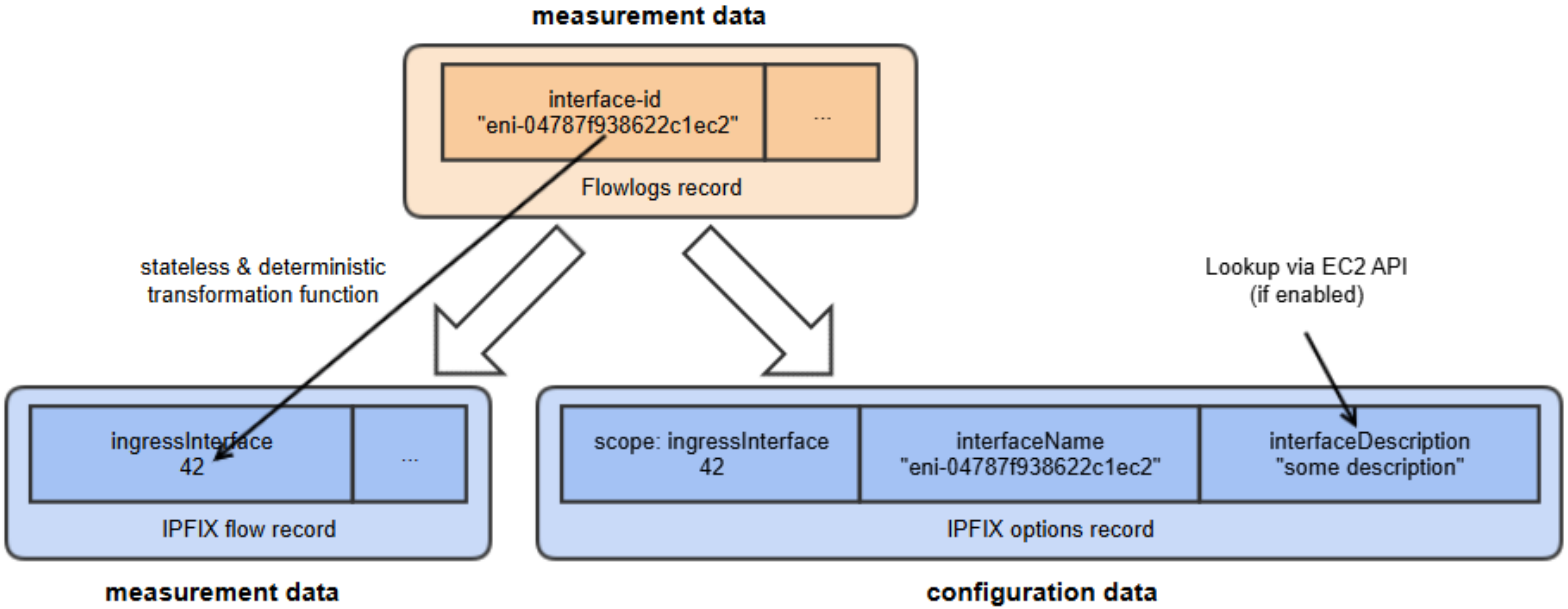


Flowlog Transcoding

Example: interface-id

Flowlogs Representation: String (e.g. „eni-04787f938622c1ec2”)

IPFIX Representation: uint32

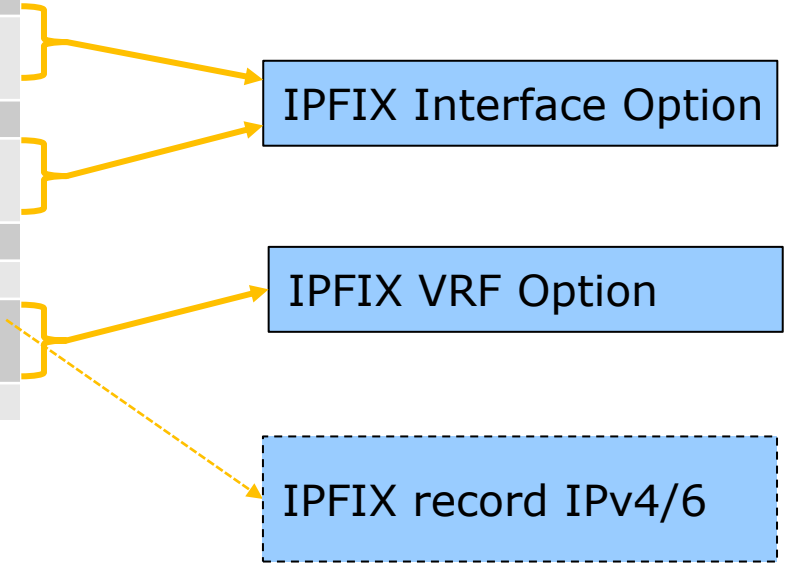


Flowlog Transcoding

Mapping of Flowlogs to IPFIX – extra fields and options handling

IPFIX Options provide configuration data, which is sent periodically and not per-flow

Flowlogs	IPFIX field	IPFIX IE No
action*	egressInterface (generated ID) interfaceName interfaceDescription	10 (14) 82 83
interface-id*	ingressInterface (generated ID) interfaceName interfaceDescription	10 82 83
vpc-id	ingressVRFID (generated ID) vrfName vrfDescription	234 236 21659:413



Summary

- Flowlogs → IPFIX transcoder
  - realized as AWS lambda function → cost scales with traffic, well-suited for PoCs and testbeds
  - PoC and tests show technical feasability
  - available via serverless application repository

- Transcoding design considerations
  - standard compliant, non-proprietary IPFIX data stream
  - translation of domain specific concepts

→ Homogeneous traffic view across cloud and on-prem infrastructure


isarNet
Software Solutions GmbH