der Bundeswehr
Universität München

Towards a collaborative, flow-based, distributed inter-domain Intrusion Detection System

RC CODE Research Center Cyber Defence
Universität der Bundeswehr München

Frank Tietze

Institut für Technische Informatik
Fakultät für Informatik

frank.tietze@unibw.de

Structure

- Introduction
- Intrusion Detection on Flows
- Detectable attacks with knowledge-based IDS‘s on Flows
- Research approach
- Hoped-for improvements
- Impact / Issues on RFC 3917

Introduction

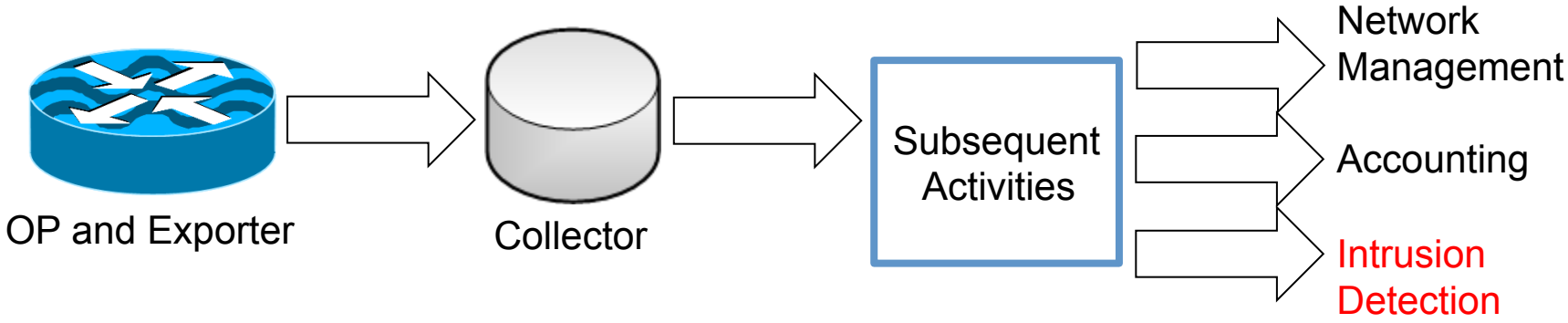
- **Definition of "Flow" within our approach:**
  - See RFC 3954: NetFlow V9

"An IP Flow, also called a Flow, is defined as a **set of IP packets** passing an Observation Point in the network during a certain time interval. **All packets that belong to a particular Flow have a set of common properties** derived from the data contained in the packet and from the packet treatment at the Observation Point.

Introduction

❑ Generation of "Flow" (classical architecture):

- See RFC 3917 / 5101: IPFIX and RFC 3954: NetFlow V9
- Aspects important for ID:
  - Reliability
  - Overload Behavior
  - Security (transfer)
  - Sampling
  - Time (stamps & sync)
  - Anonymization / Pseudonymization



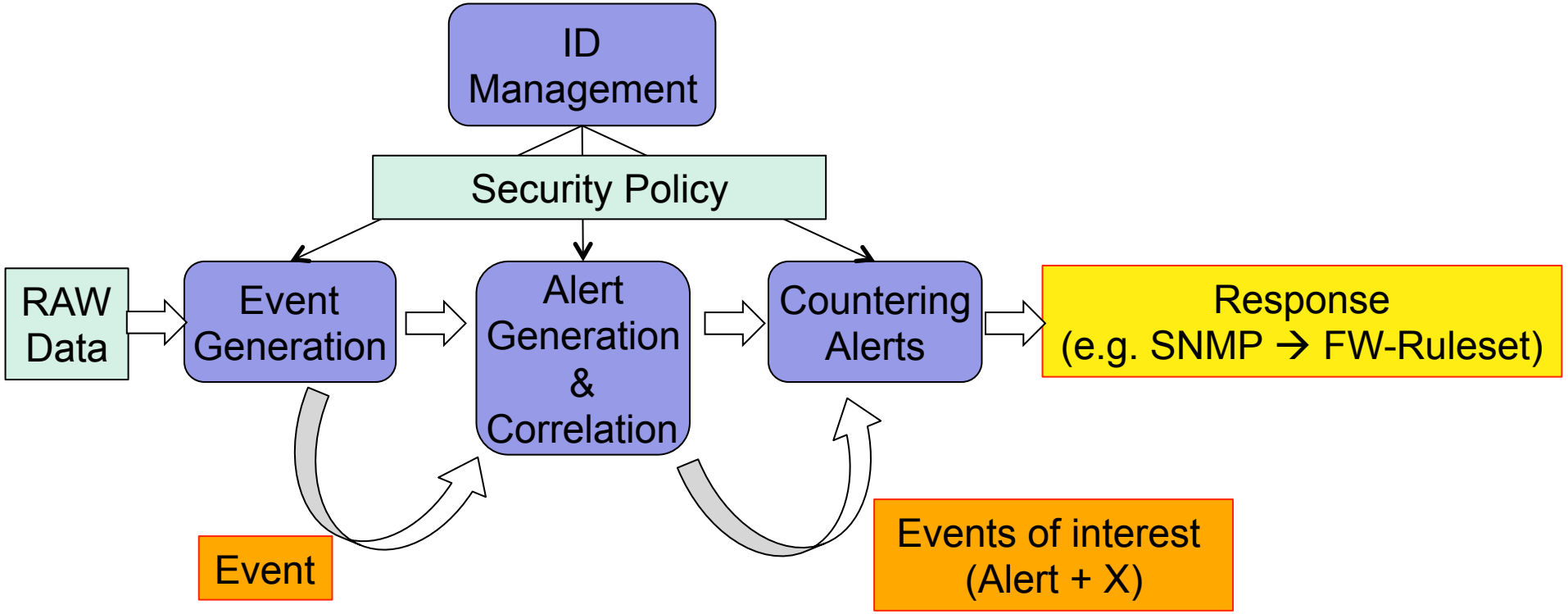
❑ Why Intrusion Detection on Flows?

- Encrypted Traffic ⇧ (Processability)
- Bandwidth ⇧ (Scalability)
- Complexity of attacks ⇧ (Detectability)

Intrusion Detection on Flows (I)

❑ What is Intrusion Detection? (NIST SP800-94)

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible *incidents*, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.



Intrusion Detection on Flows (II)

Intrusion Detection	Flow-based	Payload-based
Knowledge-based	+ Good at known threats + Simple to configure - High false negative rate - Bad on multi-event attacks - Reactive method + Privacy due to no payload + "easy" to process - Loss of data (less information?)	+ Good at known threats + Simple to configure - High false negative rate - Bad on multi-event attacks - Reactive method + No data is lost (more information) - Processing / performance - Complex algorithms
Behavior-based	+ Good at unknown / new threats + more sensitive in detection + Proactive method - High false positive rate - Hard to define "normal"-state + Privacy due to no payload + "easy" to process - Loss of data (less information?)	+ Good at unknown / new threats + more sensitive in detection + Proactive method - High false positive rate - Hard to define "normal"-state + No data is lost (more information) - Processing in learning phase - Complex algorithms

IDS in approach

Detectable attacks with knowledge-based IDS's on Flows

- DoS / DDoS
- Scans
- Worms
- Botnet-based Attacks
- data extraction via bots in internal network

Research Approach (I)

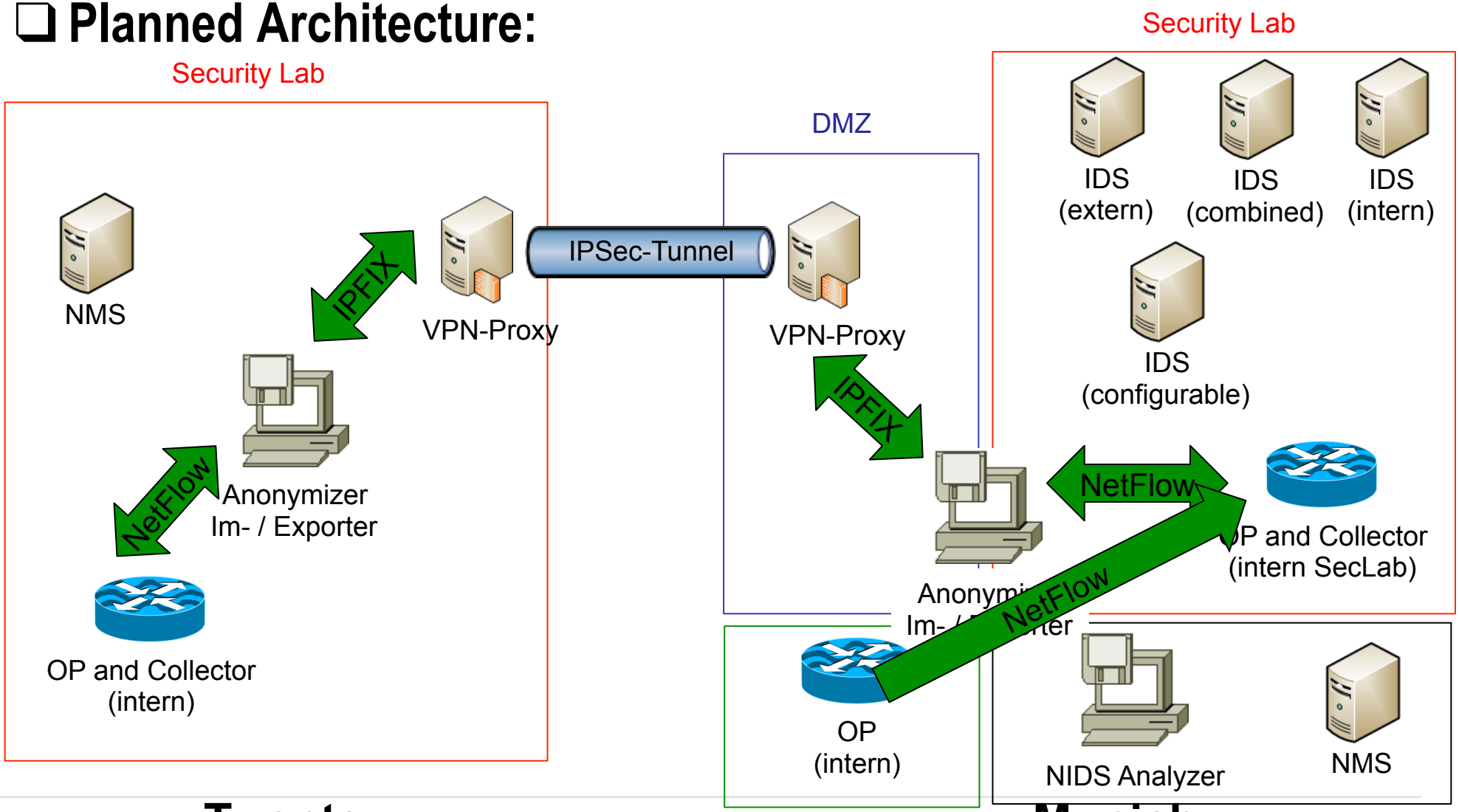
Universität der Bundeswehr München

- Inter-domain IDS between University of Twente (UT) and Universität der Bundeswehr München
- Exchange of domain-knowledge and Flows between partners (with comparable infrastructure / services)
- Integration of IDS in Joint Security Labs (Flamingo + X)
- Combination of NetFlow- and IPFIX-components addressing shortcomings of RFC 3917 / 5101 IPFIX

Research Approach (II)

der Bundeswehr Universität München

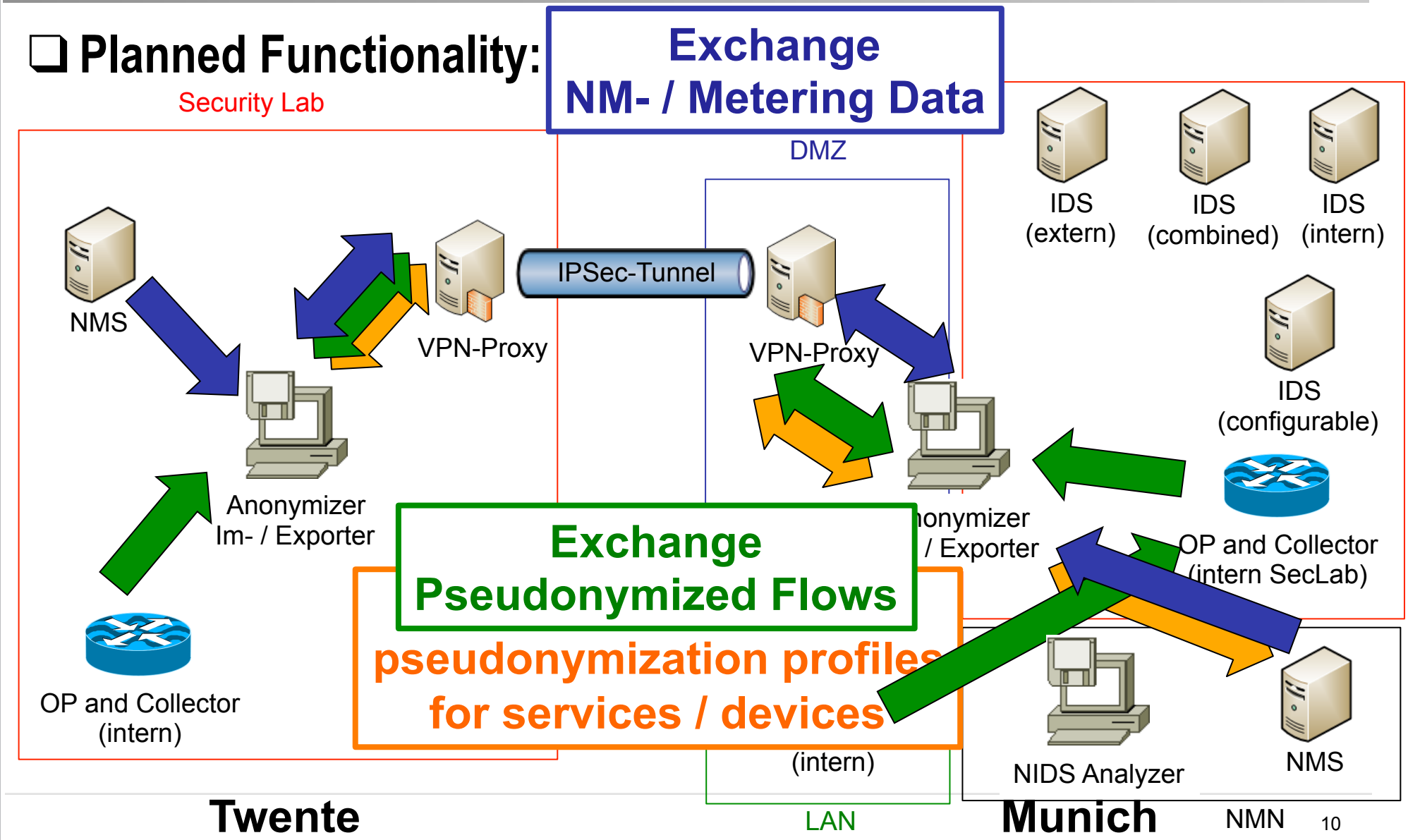
❑ Planned Architecture:



Research Approach (III)

der Bundeswehr Universität München

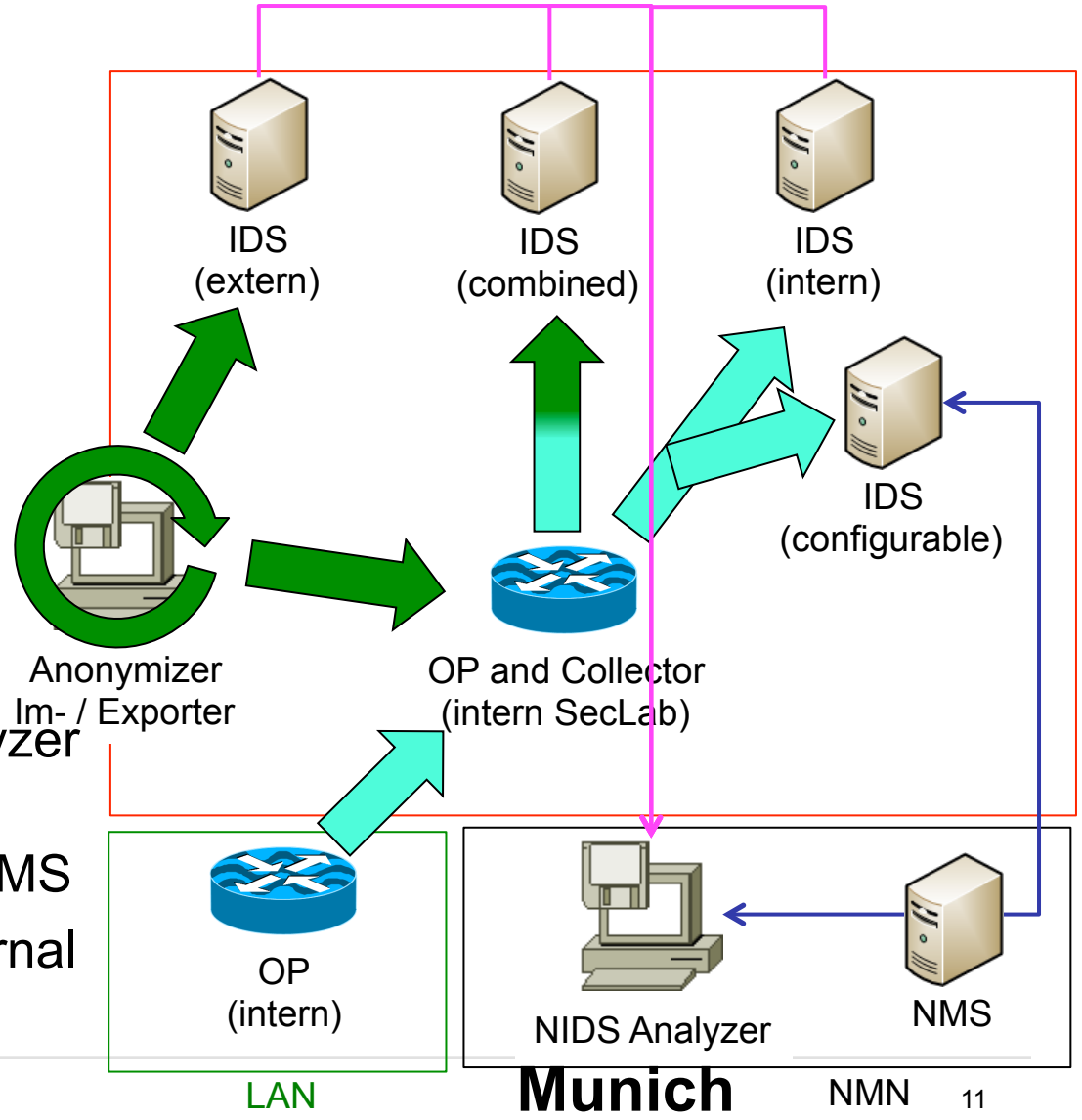
❑ Planned Functionality:



Research Approach (IV)

❑ Planned Functionality:

- Importer rewrites and filters external Flow - IPFIX
- Importer redirects external Flow to IDS (extern) and Collector
- Collector redirects internal Flow to IDS (intern) - NetFlow
- Collector combines internal and external Flow and redirects to IDS (combined) - NetFlow
- IDS‘s report alerts to NIDS Analyzer
- NIDS Analyzer reconfigures IDS (configurable)- ruleset via NMS
- IDS (configurable) analyzes internal Flow and alerts NIDS Analyzer (Verfification of new ruleset)

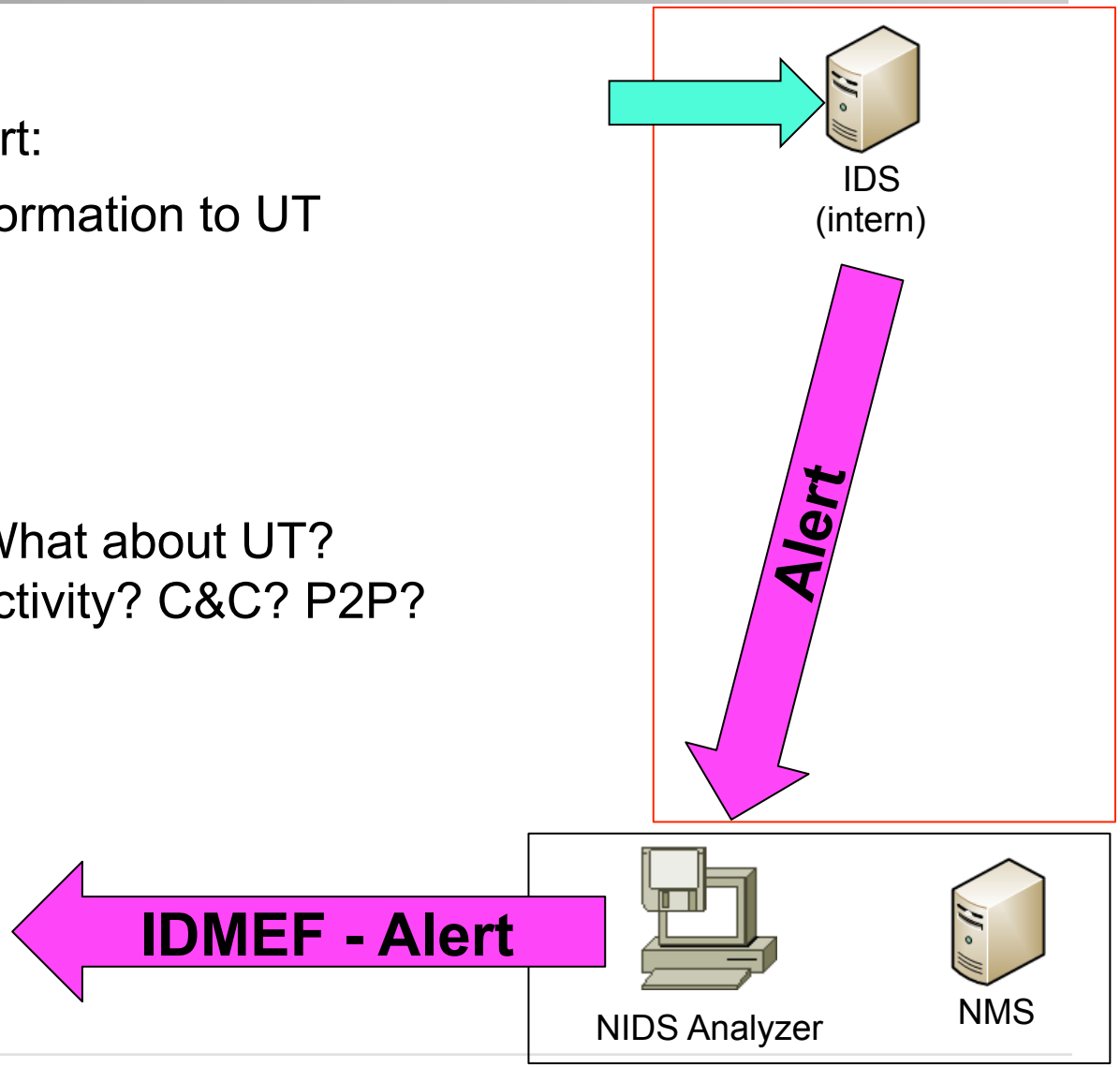


Research Approach (V)

❑ Possible results:

- Only internal IDS reports alert:
  - ➢ Report alert with further information to UT

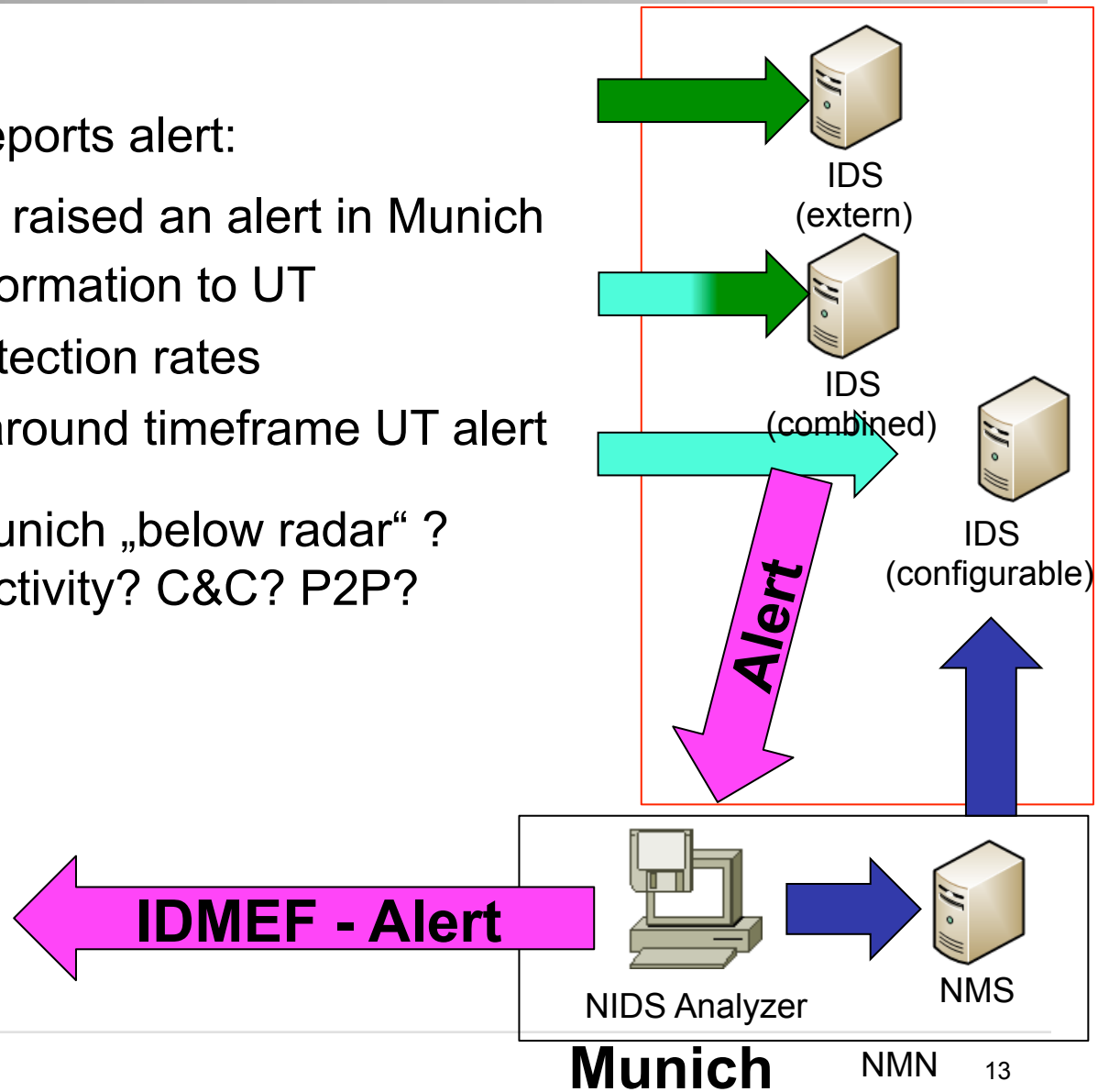
- Inbound: Attack in Munich! What about UT?
  Outbound: internal BotNet activity? C&C? P2P?



Research Approach (VI)

❑ Possible results:

- Combined and extern IDS reports alert:
  - ➢ Traffic from UT would have raised an alert in Munich
  - ➢ Report alert with further information to UT
  - ➢ Lower configurable IDS detection rates
  - ➢ Analyze internal Flow at / around timeframe UT alert
- Inbound: Similar attack in Munich „below radar“ ?
  Outbound: internal BotNet activity? C&C? P2P?

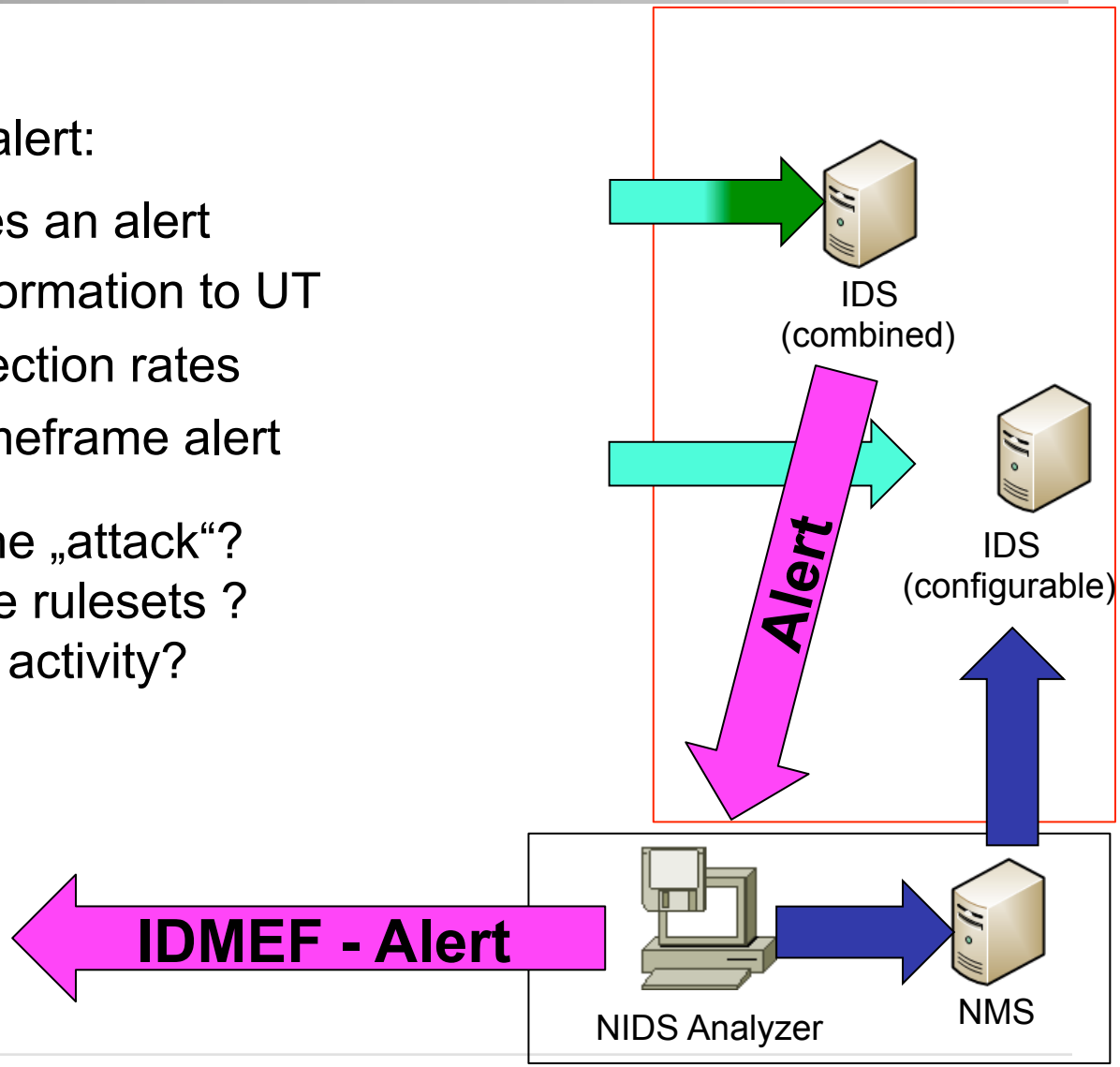


Research Approach (VII)

❑ Possible results:

- Only combined IDS reports alert:
  - ➢ Only combined Traffic raises an alert
  - ➢ Report alert with further information to UT
  - ➢ Tune configurable IDS detection rates
  - ➢ Analyze internal Flow at timeframe alert

- Inbound: Verfication of the „attack“?
  Validation of the rulesets ?
  Outbound: internal BotNet activity?
  (C&C? P2P?)



Hoped-for Improvements

- Lower false negative rates in knowledge-/flow-based IDS concerning outbound-analysis while maintaining false positive rates
- Lower false negative rates in knowledge-/flow-based IDS concerning inbound-analysis (!!! false positive rates !!!)
- Better Identification of Bots / Botnets (intern & extern)
- First step towards automated IDS configuration over domain-boundaries
- Better detection of Worm- and Botnet-Activity in European networks

Impact / Issues on RFC 3917 / 5101

❑ Metering (5):

- 5.2. Sampling → Verification of output / Validation of input (Flow)
- 5.3. Overload Behavior → Due to NM- / Metering-data-Exchange for Infra
- 5.4. Timestamps → important for correlation frames (UTC)
- 5.5. Timesynchronization → important for correlation frames (UTC)

❑ Data Export (6):

- 6.1. Timestamps for first / last packet – ICMP type & code – IP / TCP header flags
- 6.3.3. + 6.3.4. Confidentiality and Integrity
- 6.7. Anonymization / Pseudonomization

❑ Further Further Research:

- Verification / Validation of correlated inbound-Flows
- Automated, loop-free, fail-save IDS configuration (across domain-boundaries)
- Behavior-based inter-domain ID on Flows

Thank you for your attentiveness
Any questions?