Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

Descartes
research

Performance and Security Influence of Augmenting IDS using SDN and NFV

SSP 2017

Lukas Iffländer & Jonathan Stoll

2017/11/9

http://se.informatik.uni-wuerzburg.de/

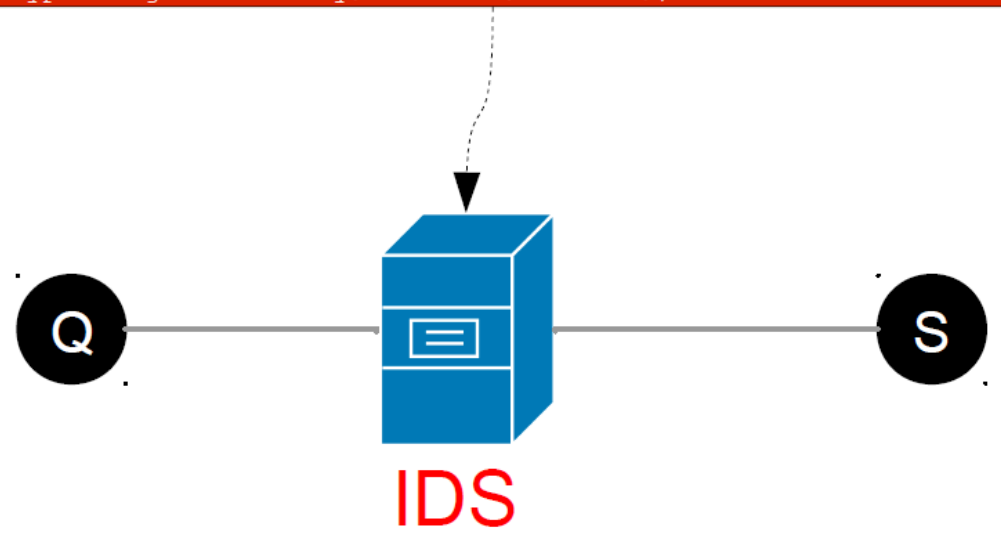
Content

- Motivation
- Background
- Approach
- Evaluation
- Conclusion

MOTIVATION

Motivation

```
Signatur:
alert tcp $EXTERNAL_NET any -> $HOME_NET 12345:12346
(msg:"MALWARE-BACKDOOR netbus getinfo"; flow:to_server, established;
content:"GetInfo|0D|"; metadata:ruleset community;
classtype:trojan-activity; sid:110; rev:10;)
```



- Attack detection requires DPI
- In inline mode IDS presend an active and potentially limiting component.

PIBA

Problem

- Active in-line IDS are a bottleneck
- IDS detect false-positives in overload scenarios

Idea

- Route only relevant traffic over the IDS

(Expected) Benefit

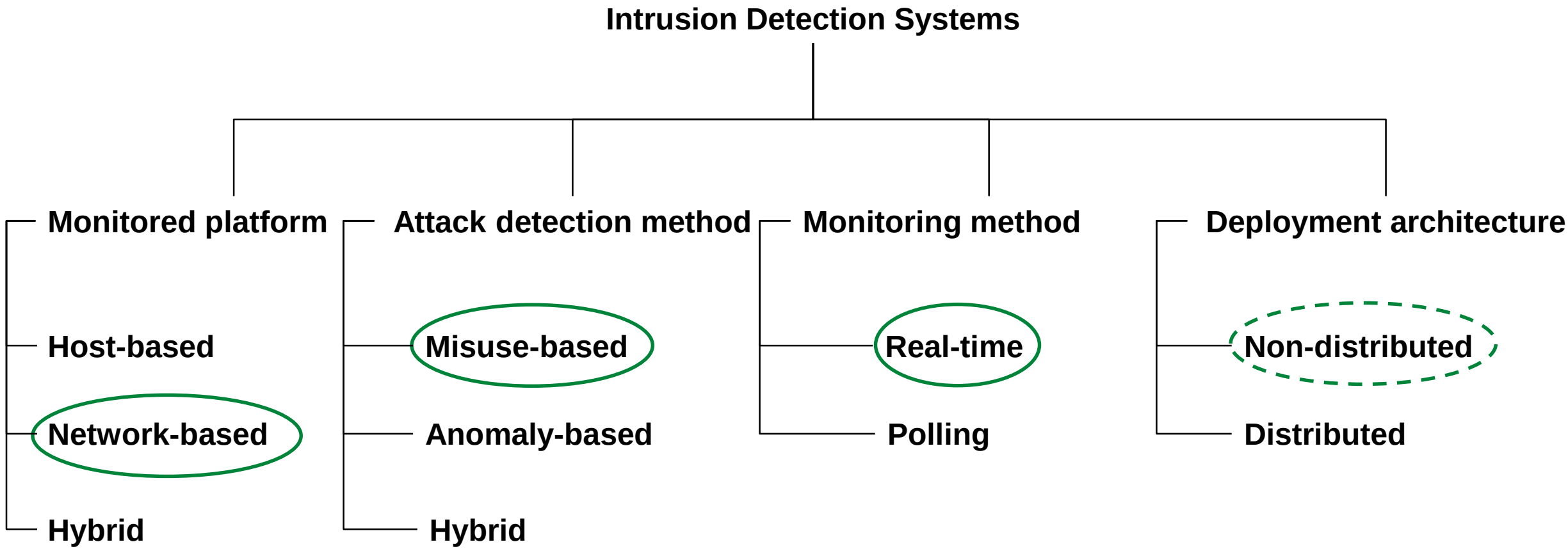
- Load removal from the IDS
  - Improves network performance
  - Improves attack detection
- Allows global reaction to attacks in the network

Action

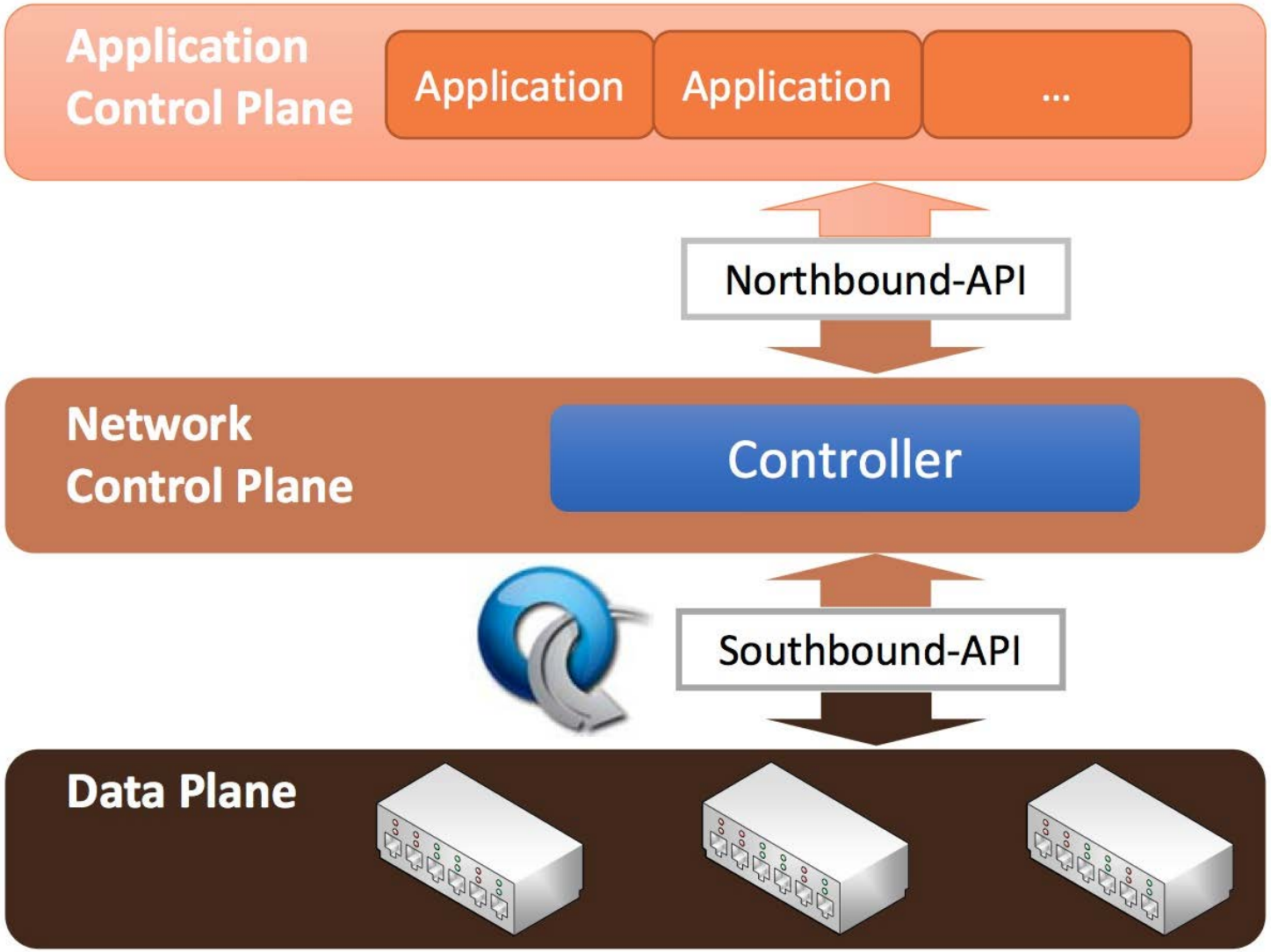
- Develop SDN based algorithms to route only relevant traffic over the IDS

BACKGROUND

IDS Categories



SDN


Application Control Plane
Application
Application
...
Northbound-API
Network Control Plane
Controller
Southbound-API
Data Plane

Related Work

- [CKR+14] Po Wen Chi, Chien Ting Kuo, He Ming Ruan, Shih Jen Chen und Chin Laung Lei: **An AMI Threat Detection Mechanism Based on SDN Networks.** In: Eighth International Conference on Emerging Security Information, Systems and Technologies(SECUWARE 2014). IARIA, Nov 2014.
- [XXHM14] Tianyi Xing, Zhengyang Xiong, Dijiang Huang und Deep Medhi: **SDNIPS: Enabling Software-Defined Networking Based Intrusion Prevention System** in Clouds. In: 10th CNSM and Workshop. IFIP, Nov 2014.
- [YPL+15] Changhoon Yoon, Taejune Park, Seungsoo Lee, Heedo Kang, Seungwon Shin und Zonghua Zhang: **Enabling security functions with SDN: A feasibility study.** In: Computer Networks, Band 85, Seite 19–35. Elsevier B.V., May 2015.

APPROACH

Assumptions

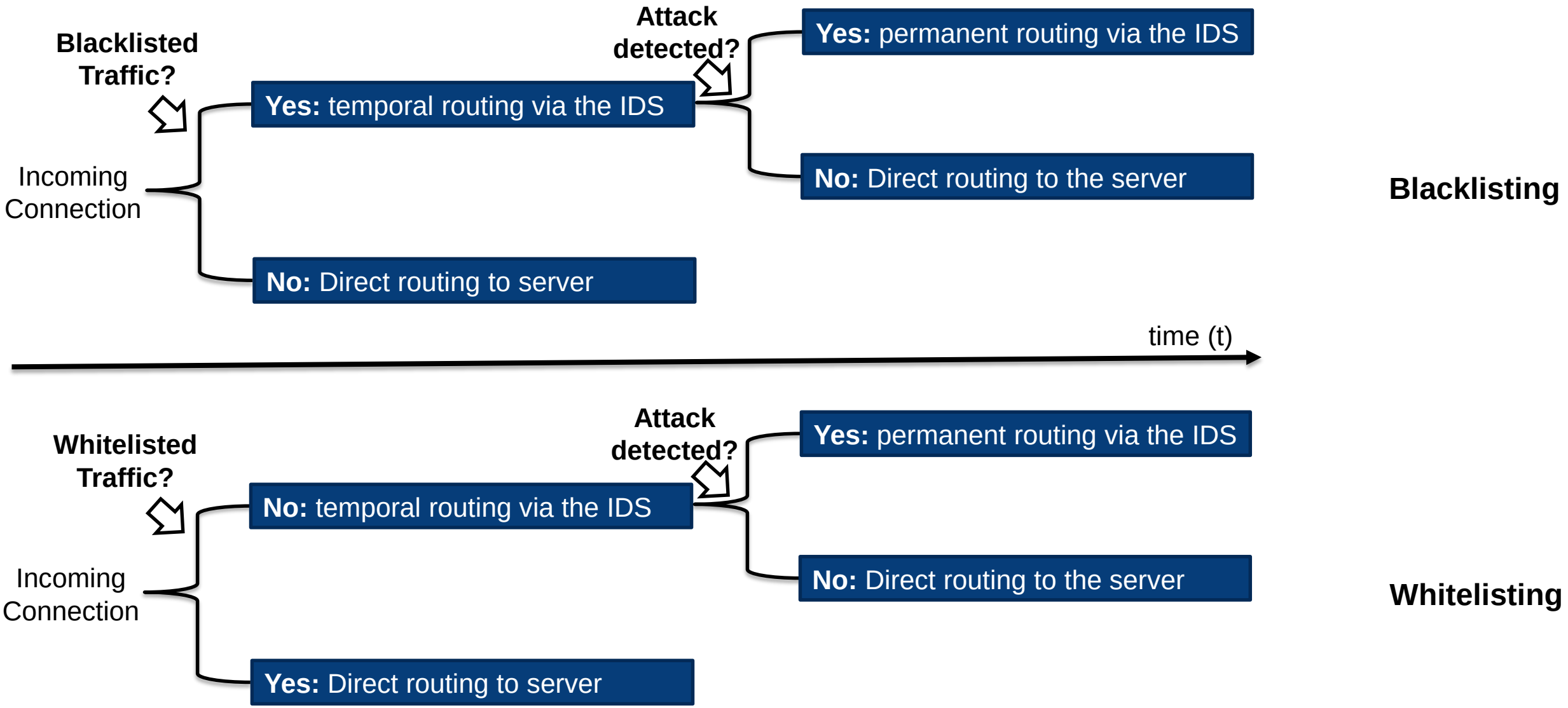
- Attacks only from the outside
  - ➔only incoming traffic to be monitored
  - ➔outgoing traffic is benign
- Only applications the IDS has signatures for are relevant
- Only the first packets of a connection contain attacks (e.g. HTTP-Requests)

Routing Concepts

Development of three SDN-based algorithms for routing traffic via the IDS

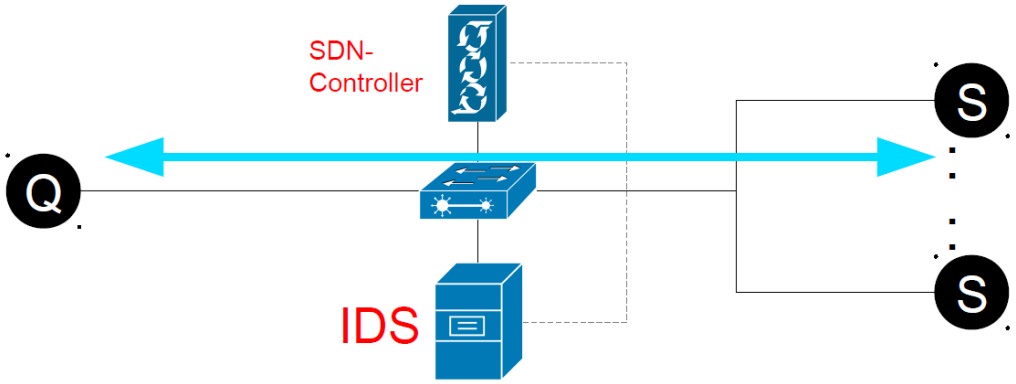
- **Adaptive Blacklisting**
  - Permanent blacklists for some services
  - Temporal blacklists for selected connections
- **Adaptive Whitelisting**
  - Permanent whitelists for some services
  - Temporal whitelists for selected connections
- **Selective Filtering**
  - Permanent routing of selected services over the IDS

New Connection



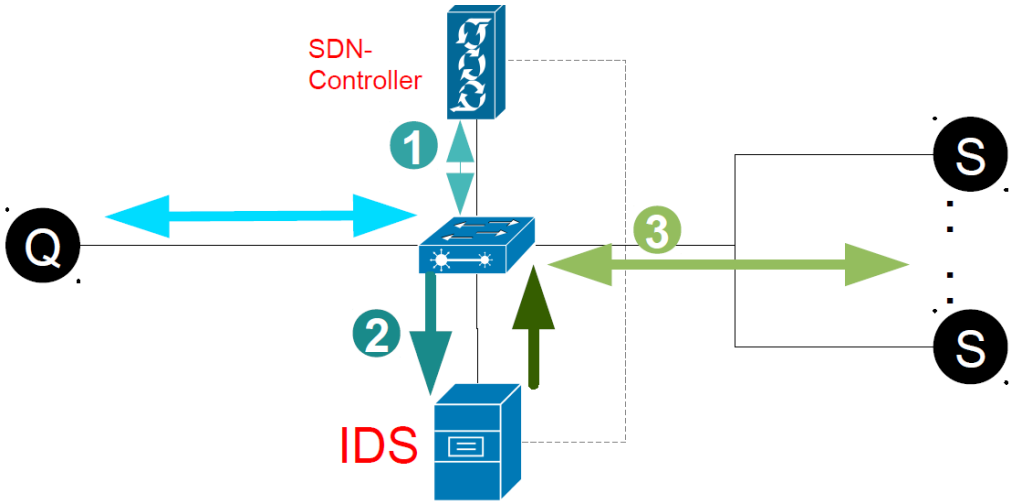
Blacklisting

Non-blacklisted traffic:



Direct routing between Q and S

Blacklisted traffic:



(1) New connection

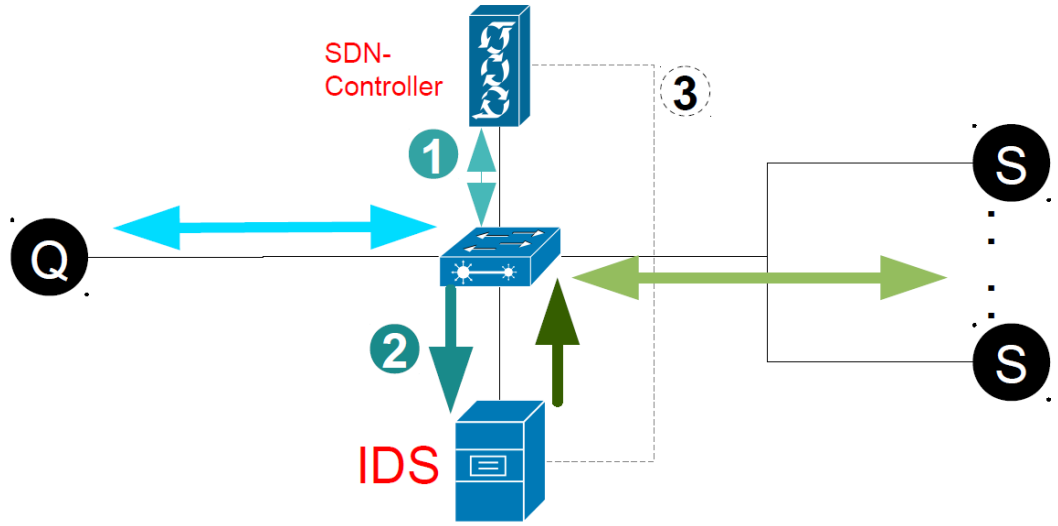
(2) Route via IDS for X seconds

(3) No attack detected:
Direct routing after X seconds for Y seconds

Attack detected:
Permanent routing via IDS

Whitelisting

Normal traffic:



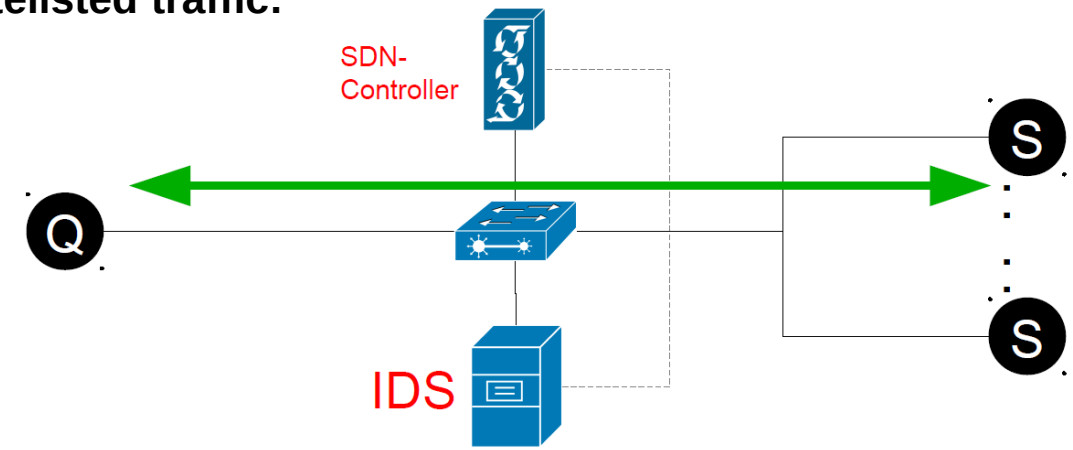
(1) New connection

(2) Route via IDS

(3) Require information weather attack occured within X packets

If not permanent routing from Q to S

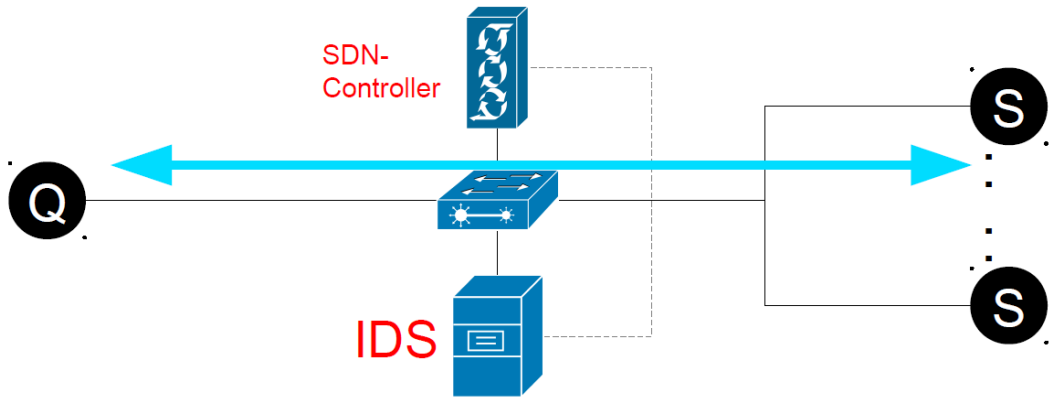
Whitelisted traffic:



Direct routing between Q and S

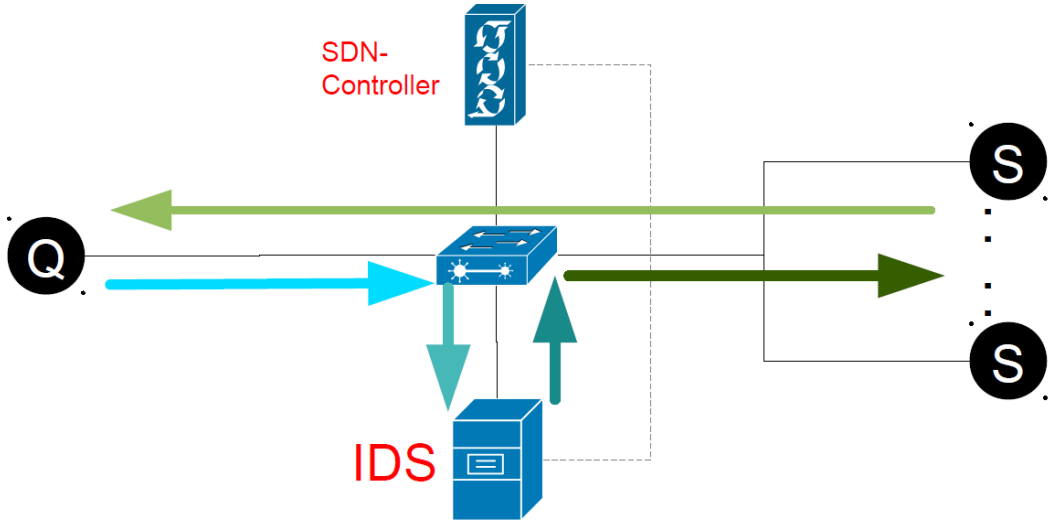
Selective Filtering

Normal traffic:



Direct routing between Q and S

Selected traffic:

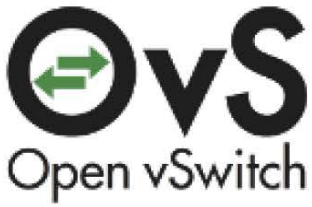


Routing of incoming traffic via the IDS

Direct routing of outgoing traffic

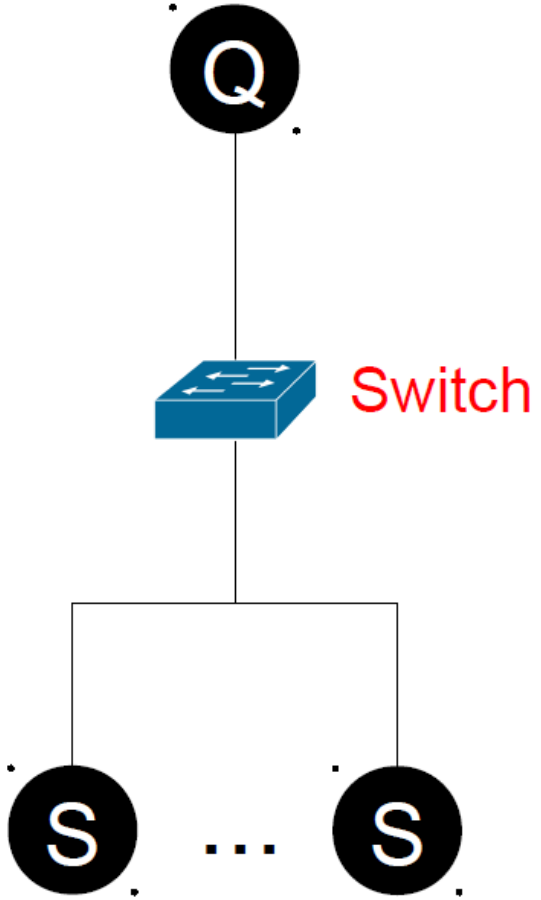
Used technologies

- SDN: OpenFlow + Ryu Controller
- IDS Snort with barnyard2
- Application: Apache Webserver
- Virtual Switch: Open vSwitch
- SDN Controll: L7sdntest

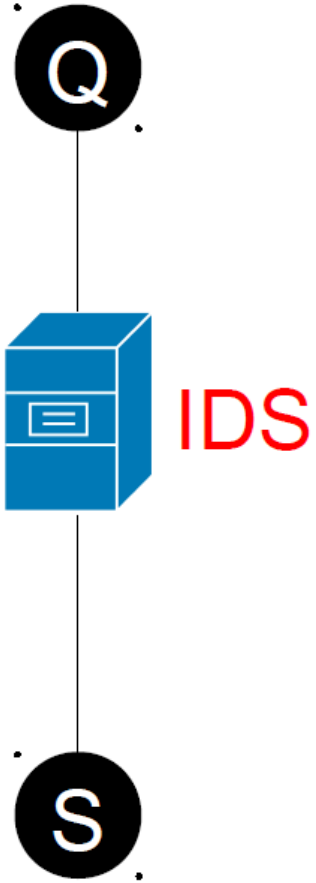


Reference Scenarios

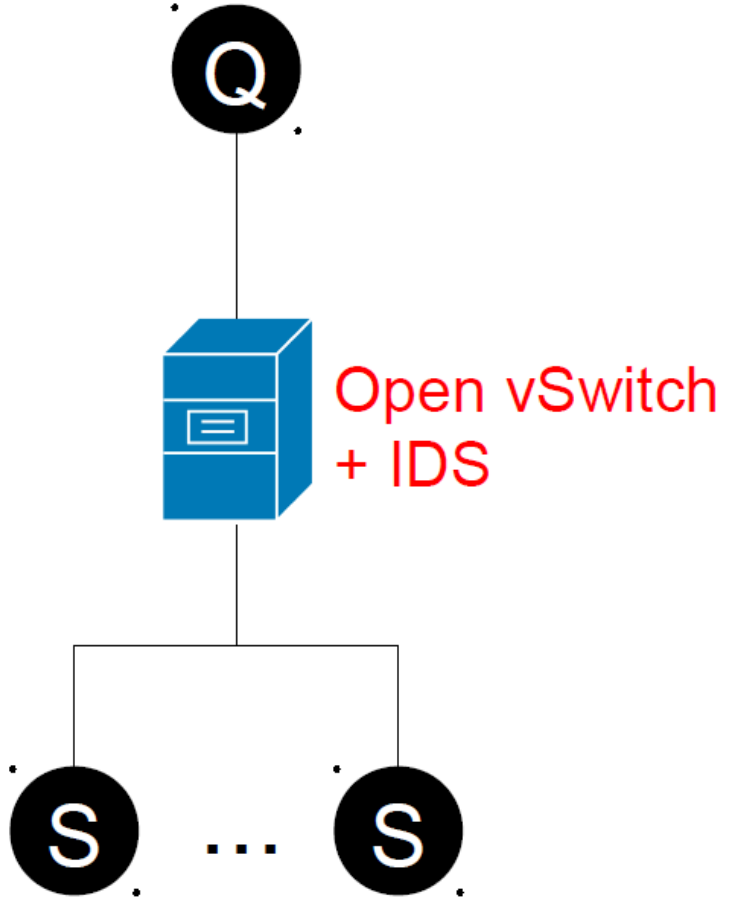
1a
(optimum reference)



1b
(minimum reference)

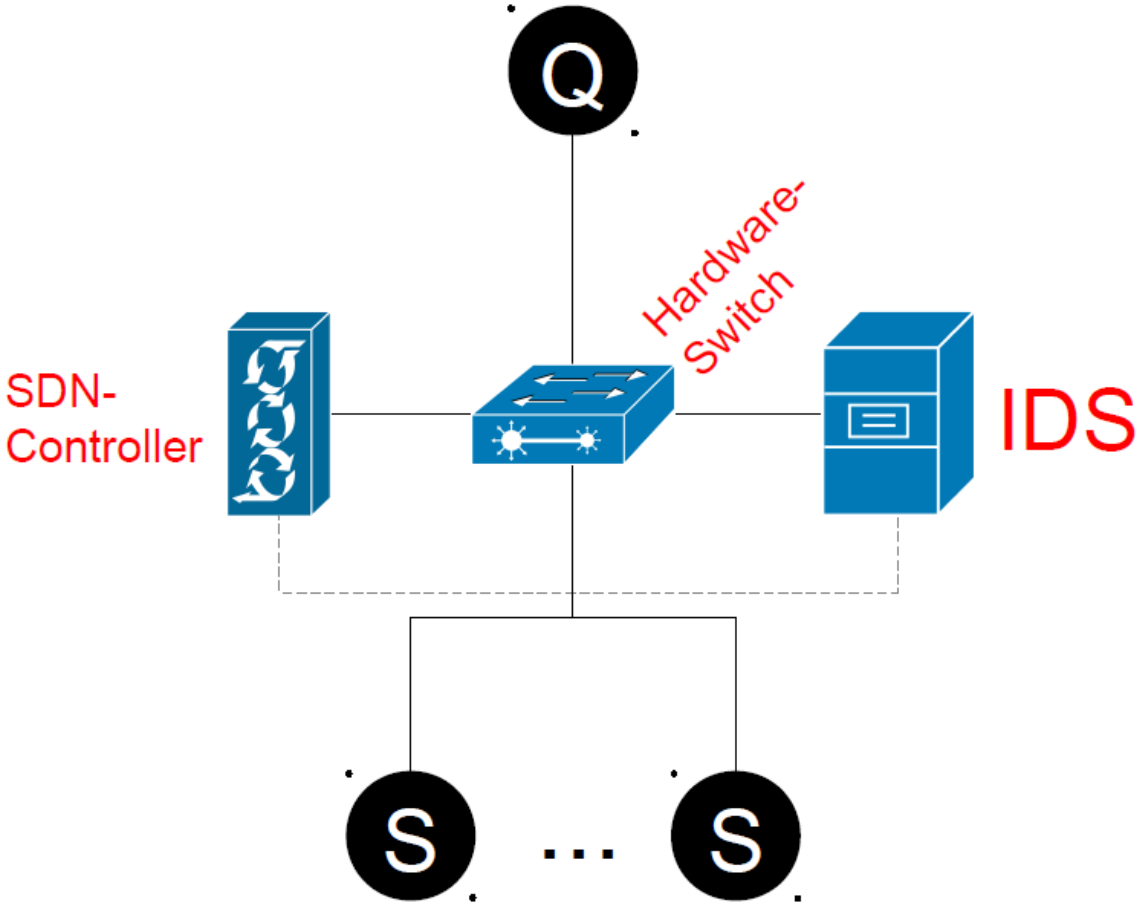


2
(Switch VNF + IDS)

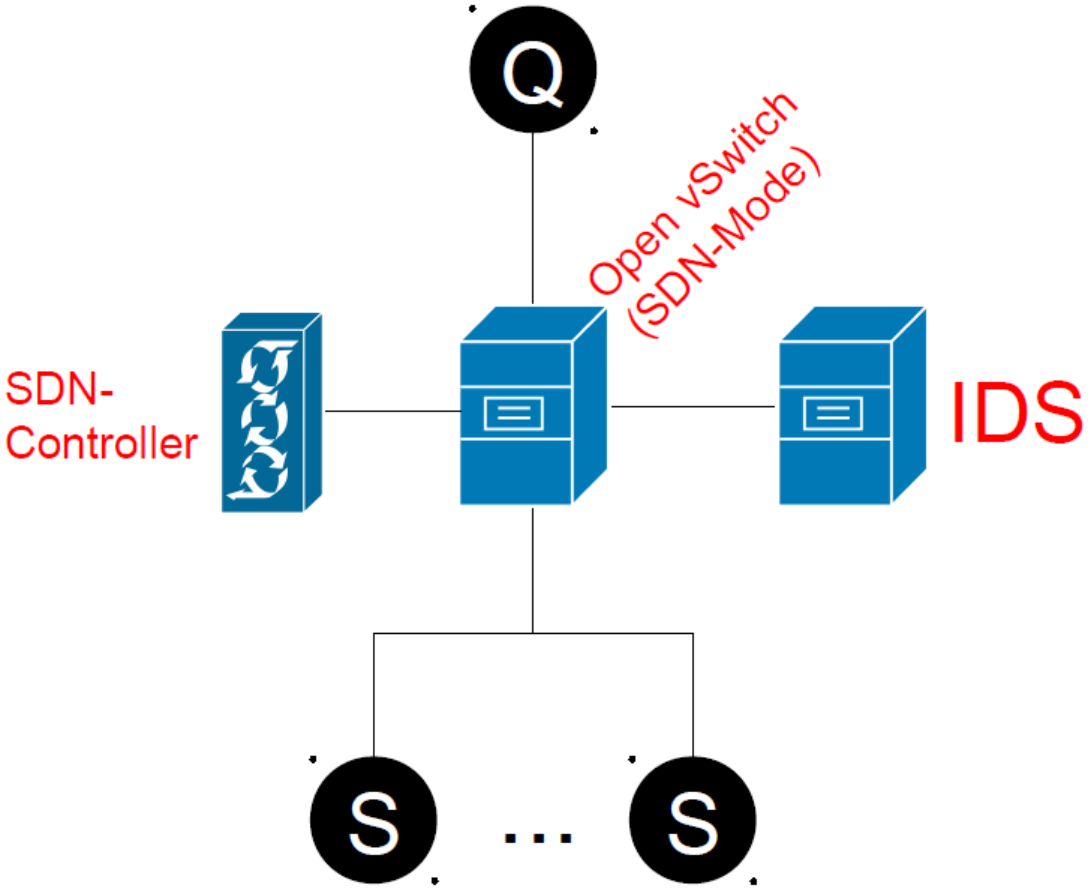


Intelligent Routing Scenarios

3
IDS + SDN Switch



5
IDS + SDN Switch VNF



Metrics and Workloads

- Throughput [Mbit/s]
- Delay [ms]
- Alarm-Rate
  - False positives
  - False negatives
- HTTP Requests

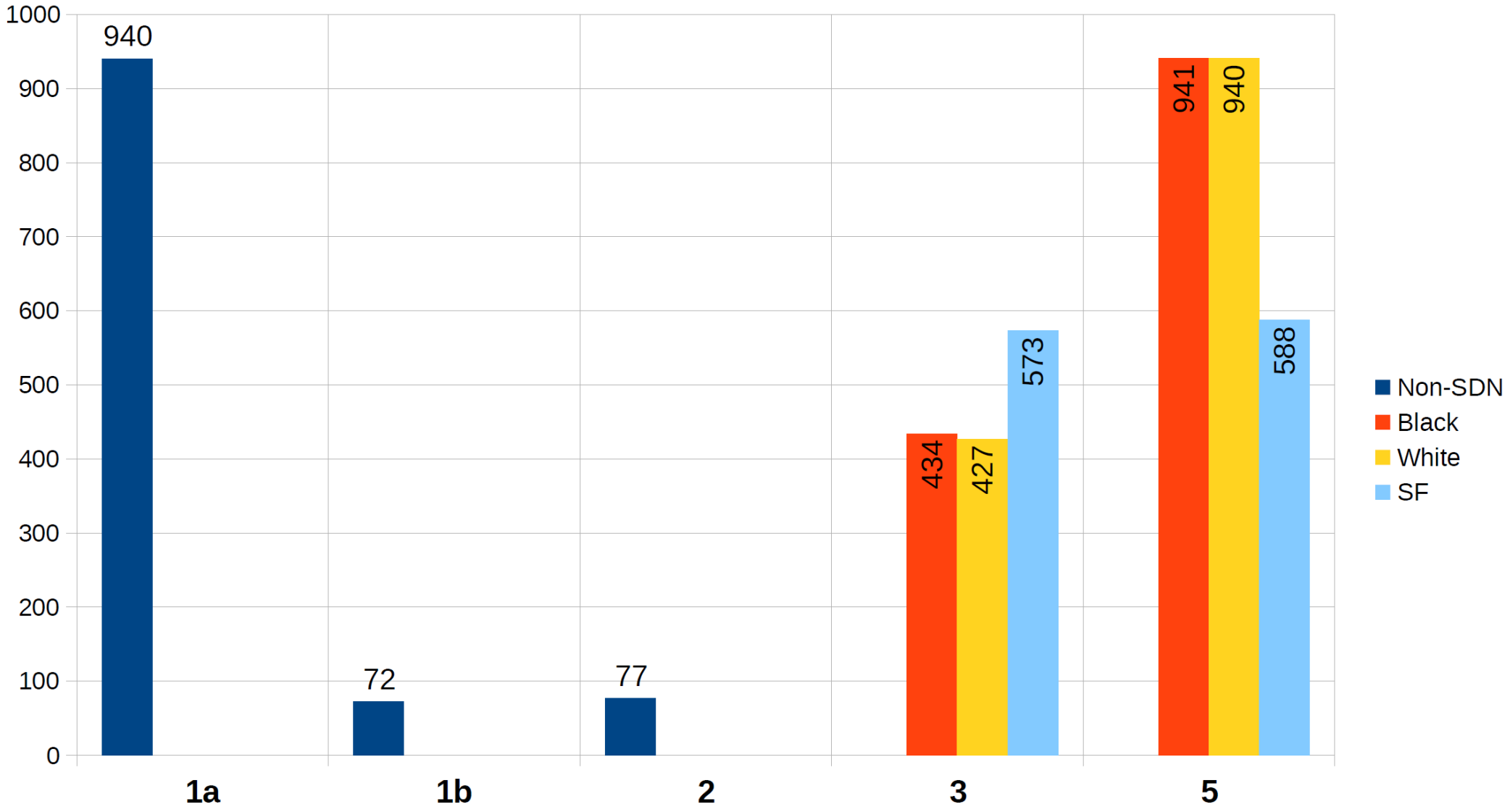
Workload 1: Constant Load

$$a = \frac{\lambda}{\mu} = 1$$

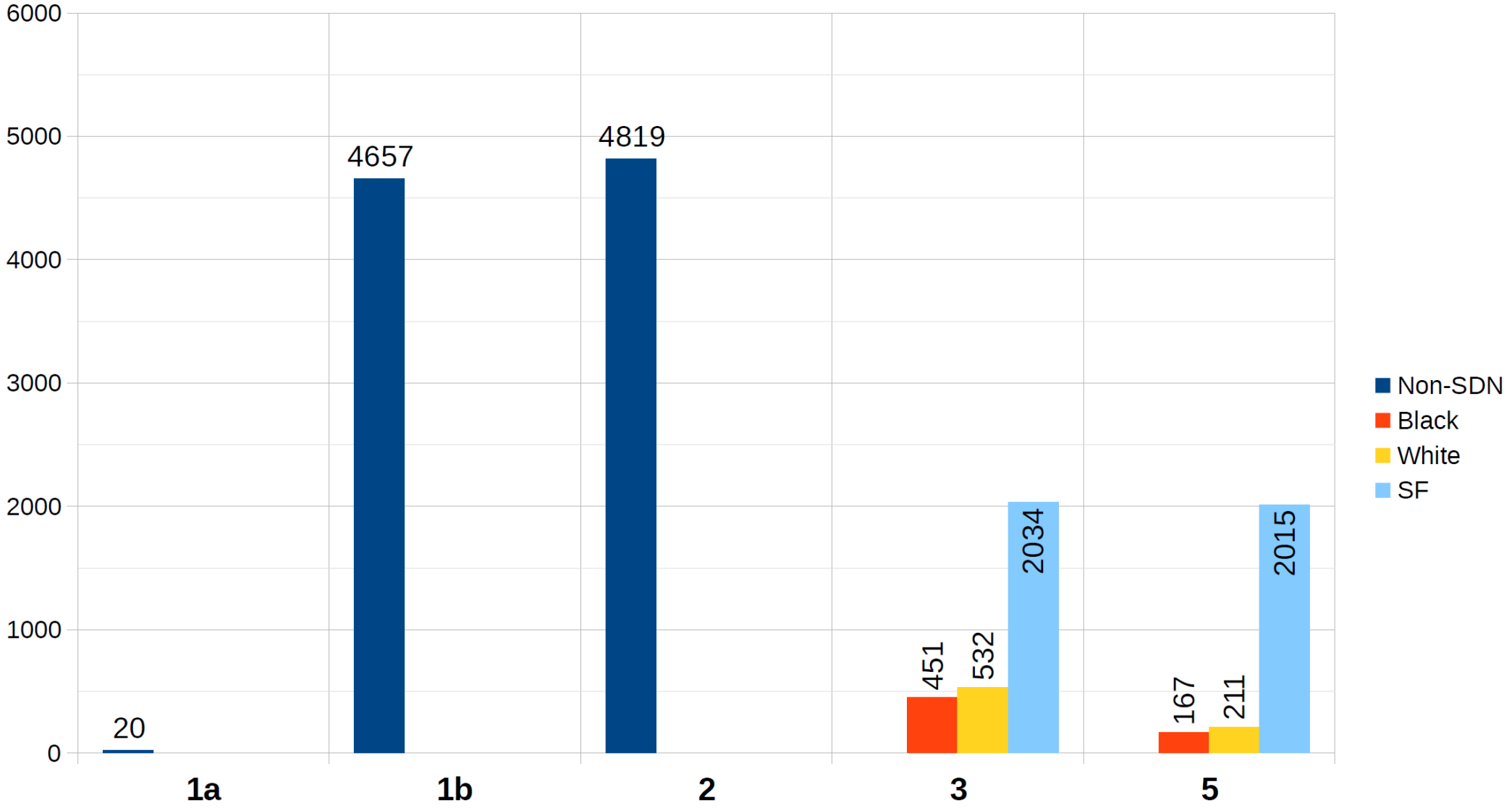
Workload 2: Overload

$$a = \frac{\lambda}{\mu} > 1$$

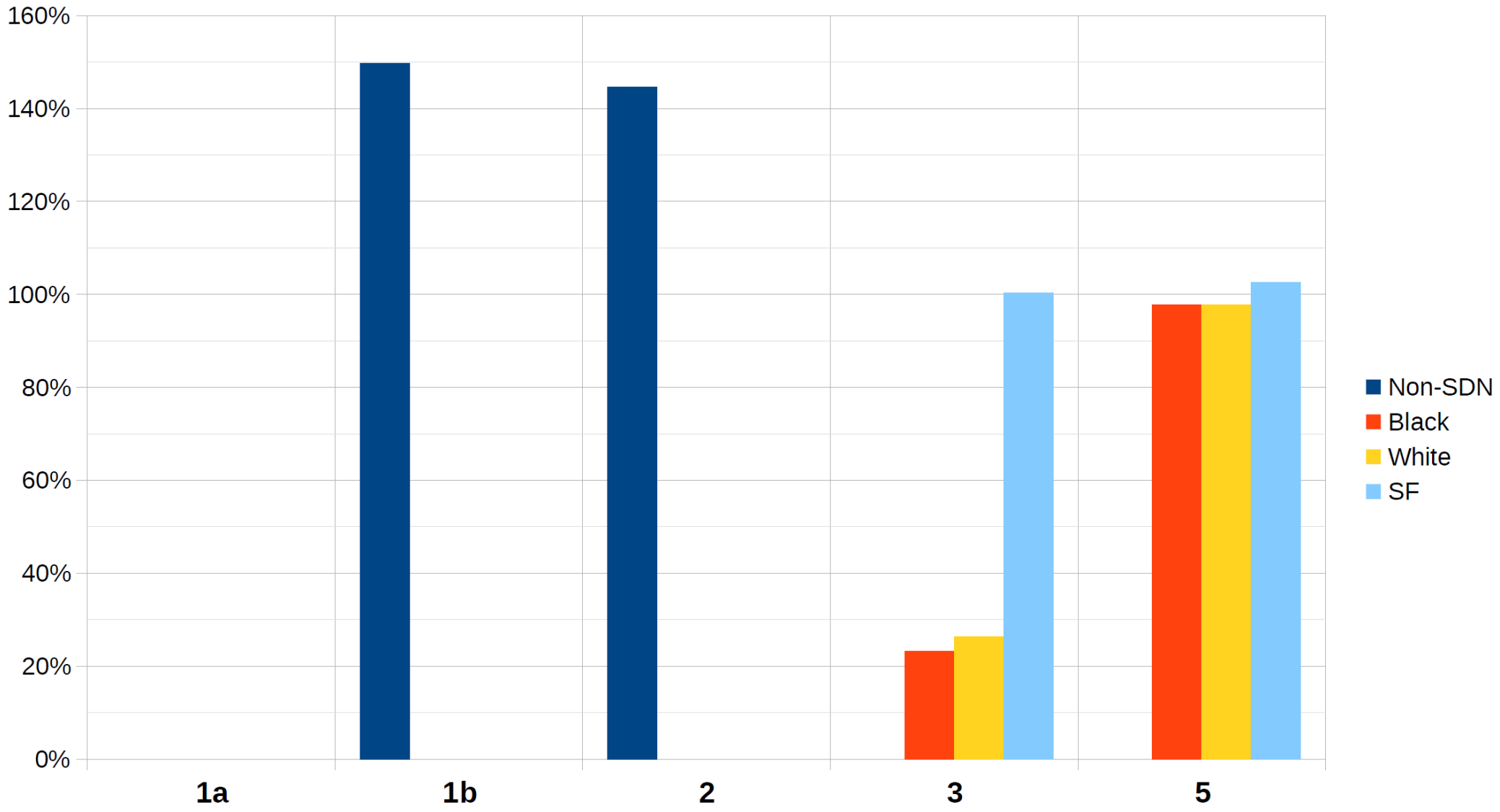
Workload 1: Througput [Mbit/s]



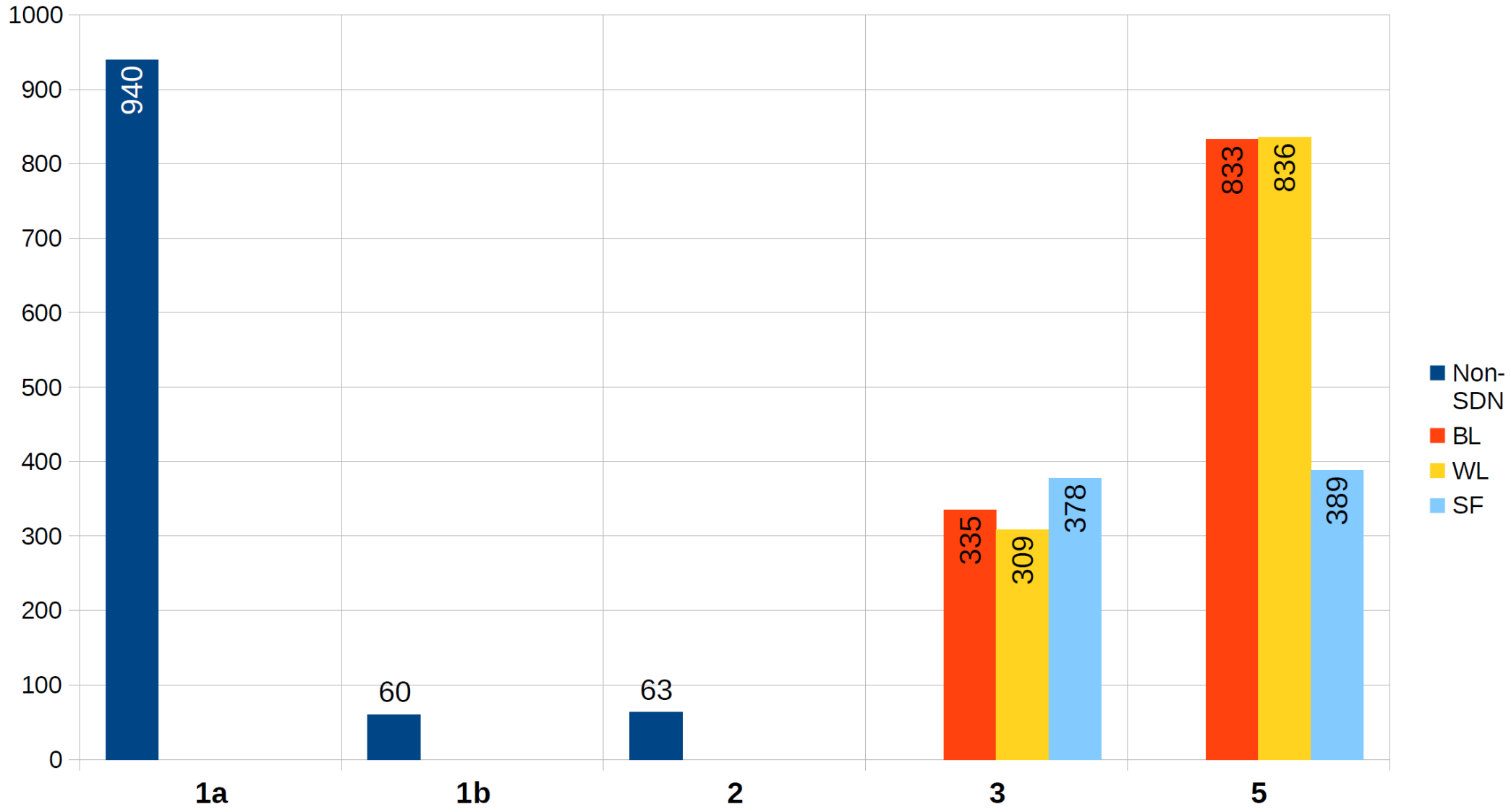
Workload 1: Delay [ms]



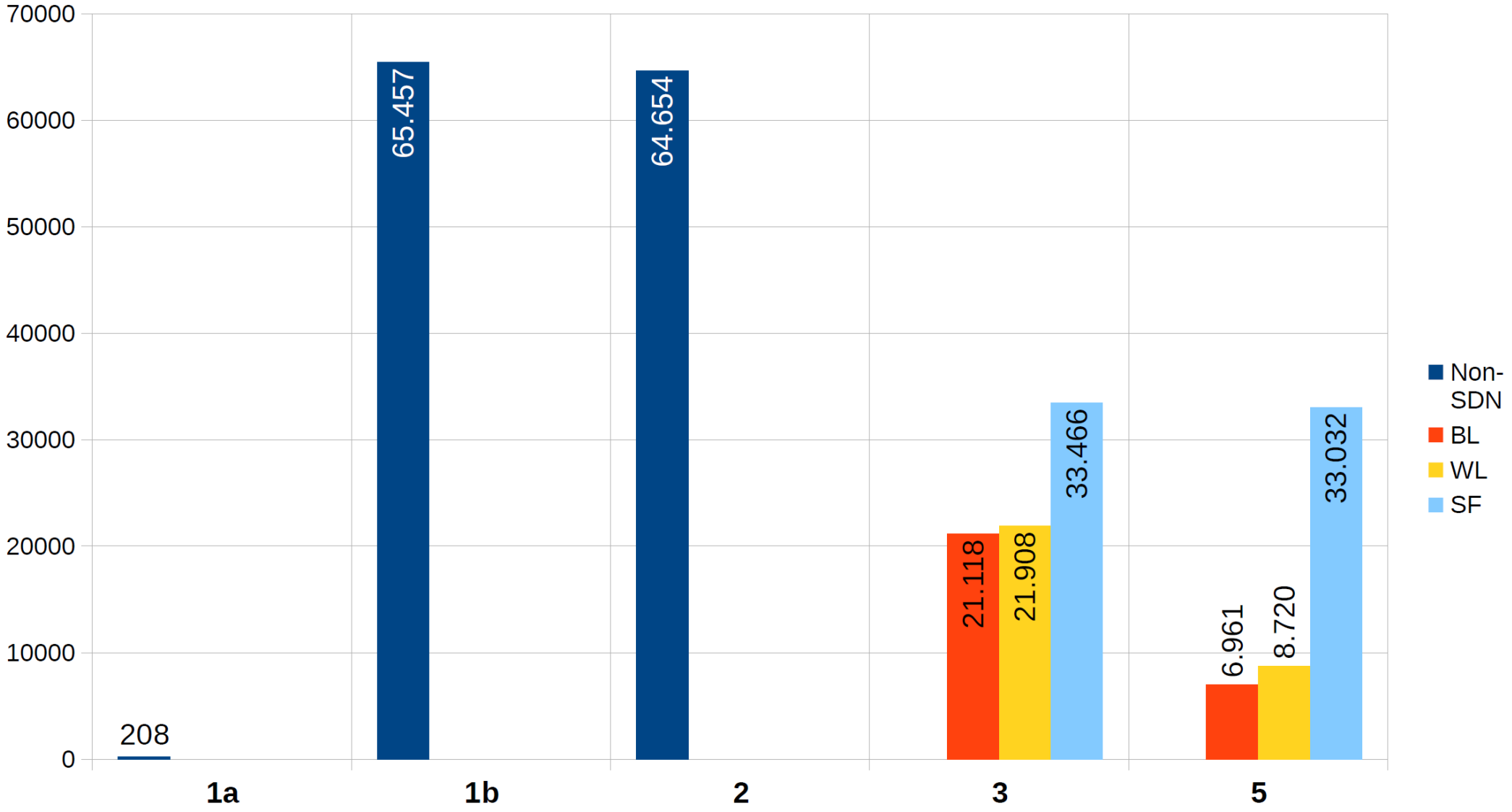
Workload 1: Alerts



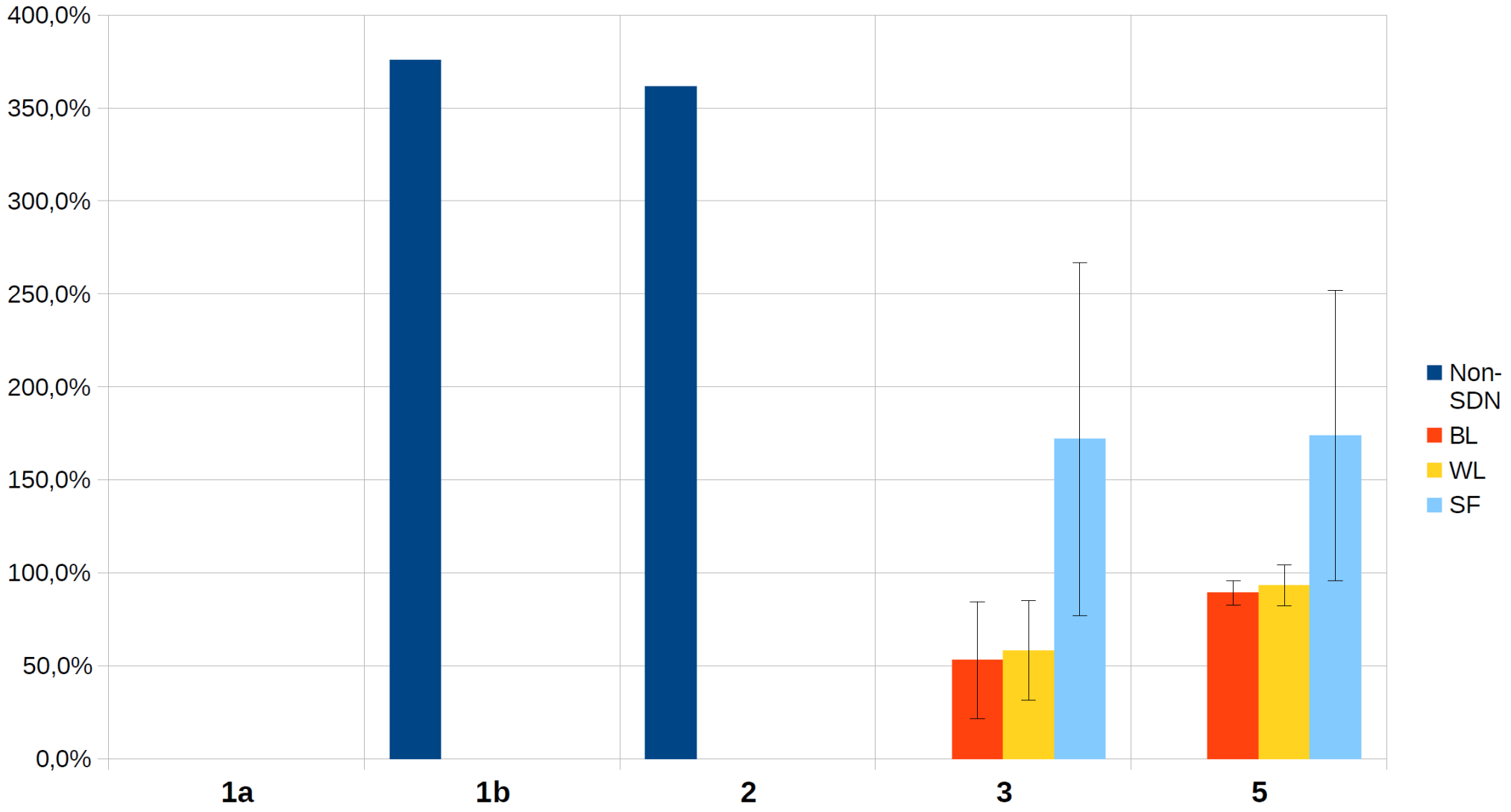
Workload 2: Througput [Mbit/s]



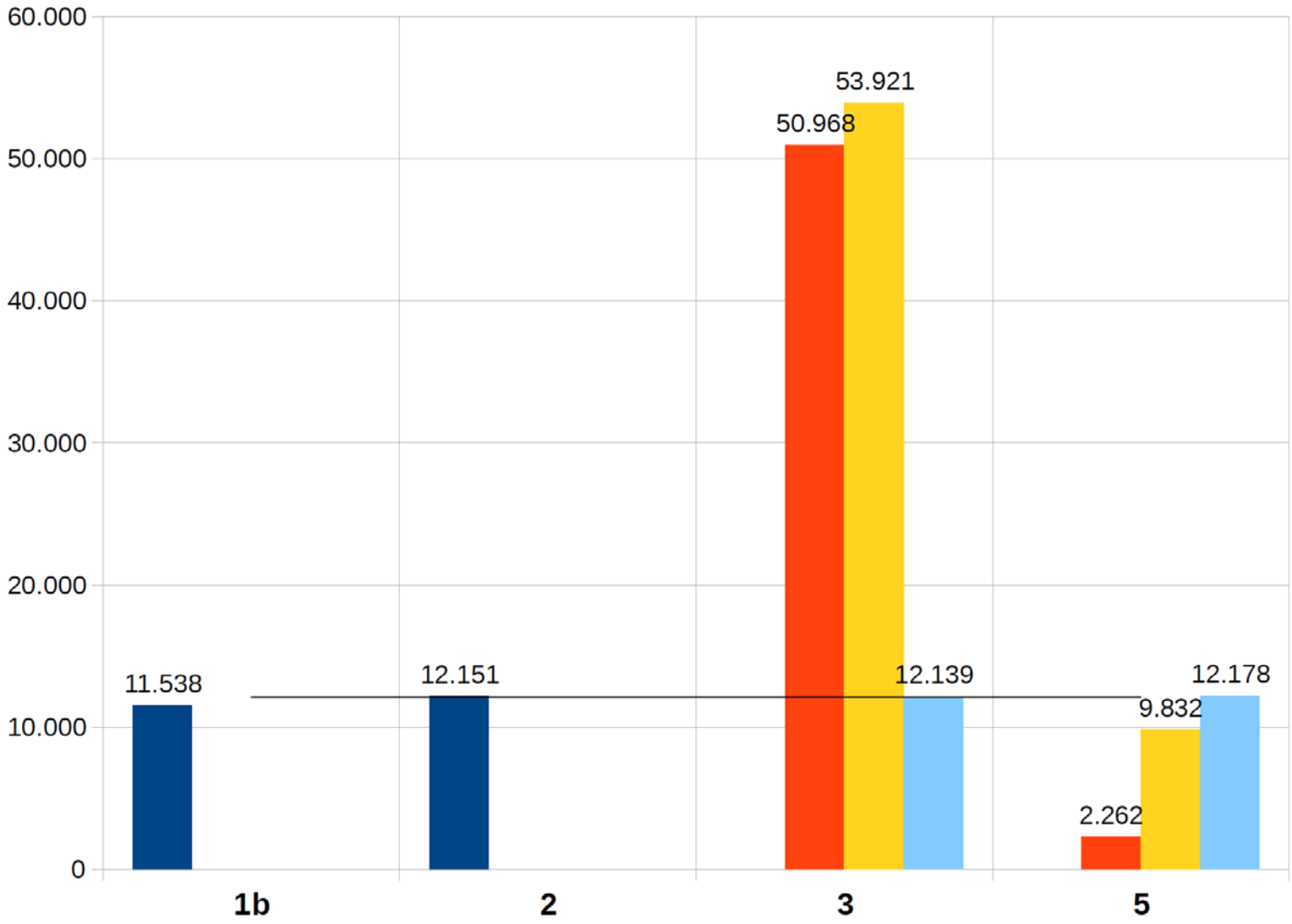
Workload 2: Delay [ms]



Workload 2: Alerts



Workload 2: Packets via IDS per Second



Summary

- Throughput was increased
- Delay was decreased
- Improved attack detection
  [further work needed for more precise statemens]
- Large differences between native and virtual switches
- Packet throughput at IDS indicator for system performance

Future Work

- Evaluation with other Hardware Switches
- Extension by load balancing solutions for IDS
- Evaluation of other IDSes (Bro, Suricata, Snort2, …)
- More detailed inspection of attack detection results
- Application of learned knowledge for function chaining of security VNFs

Thank you for your attention!

lukas.ifflaender@uni-wuerzburg.de

https://twitter.com/bladewing678