WIRESHARK

User Group Switzerland

Capture Options: From Host-Capturing to TAPs

You‘ll never find what you didn‘t captured before

Vorstellung

- Benjamin Pfister
- Leiter Netzwerk & Telekommunikation
- IT-Consultant
- Trainer
- Freier Autor

Überblick Capture-Optionen

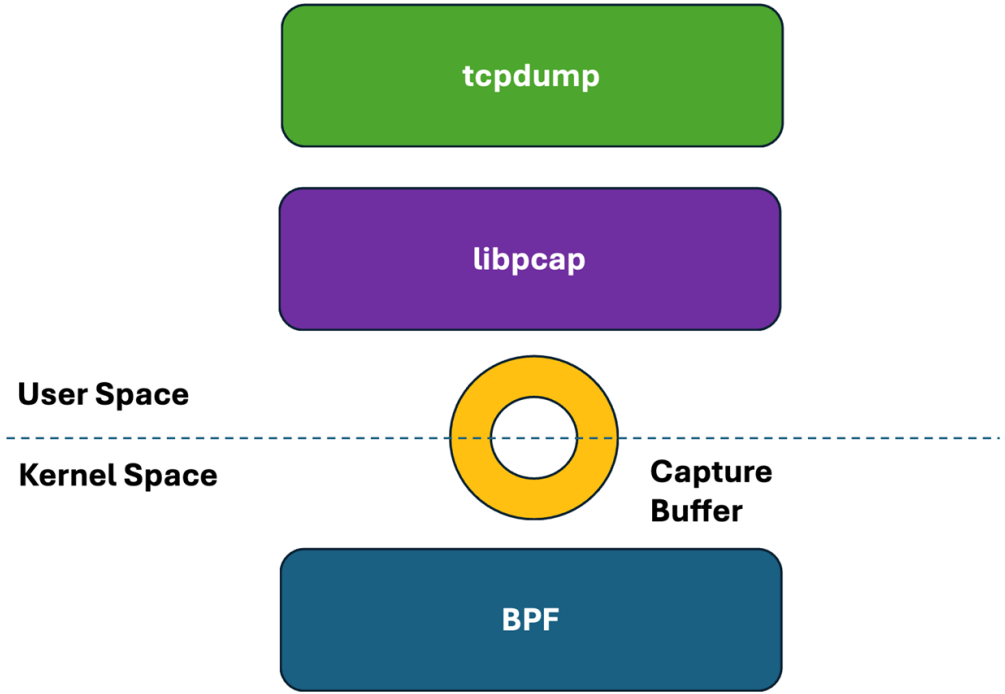
- Host-basierte Aufzeichnung
- Capture auf Netzwerkkomponenten
- Hubs
- SPAN / RSPAN / ERSPAN
- TAPs

Host-basierte Aufzeichnung

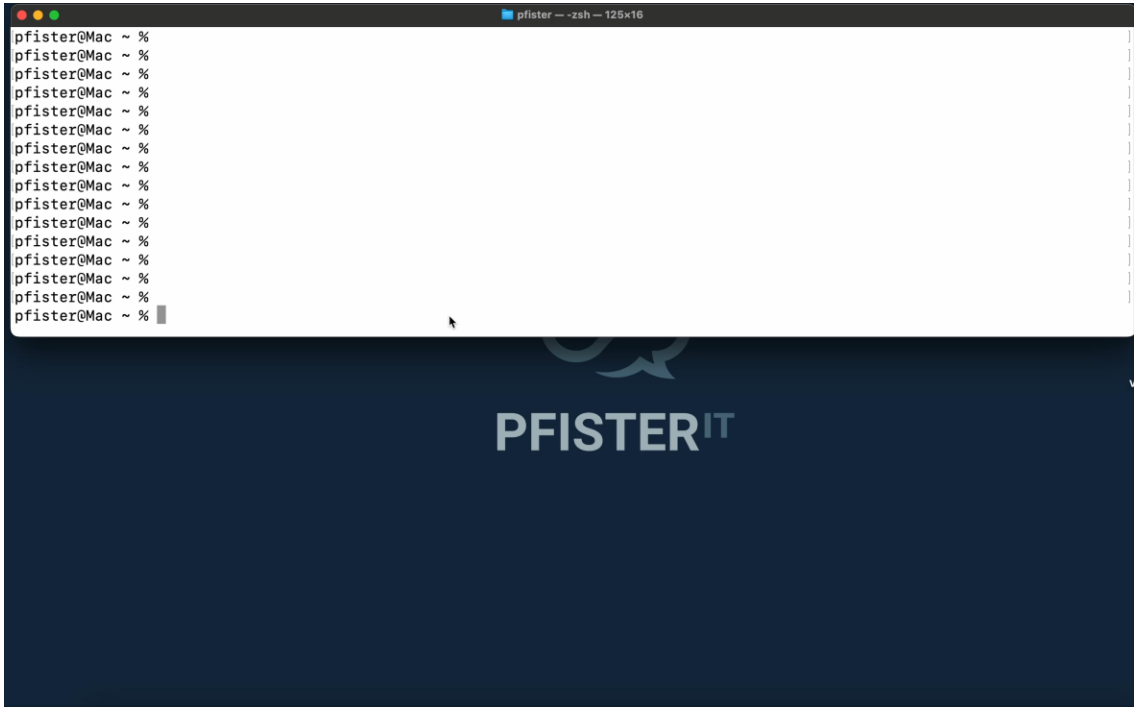
- Differenzierung unixoid vs. Windows
- Integriert oder Third Party?

Host-basierte Aufzeichnung | tcpdump

- Kommandozeilentool
- unixoide Systeme
- Mitschneiden
- BPF-Filter

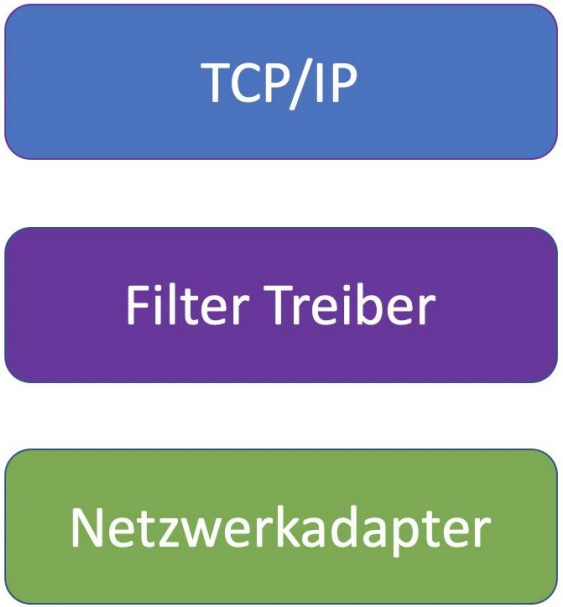


Host-basierte Aufzeichnung | tcpdump

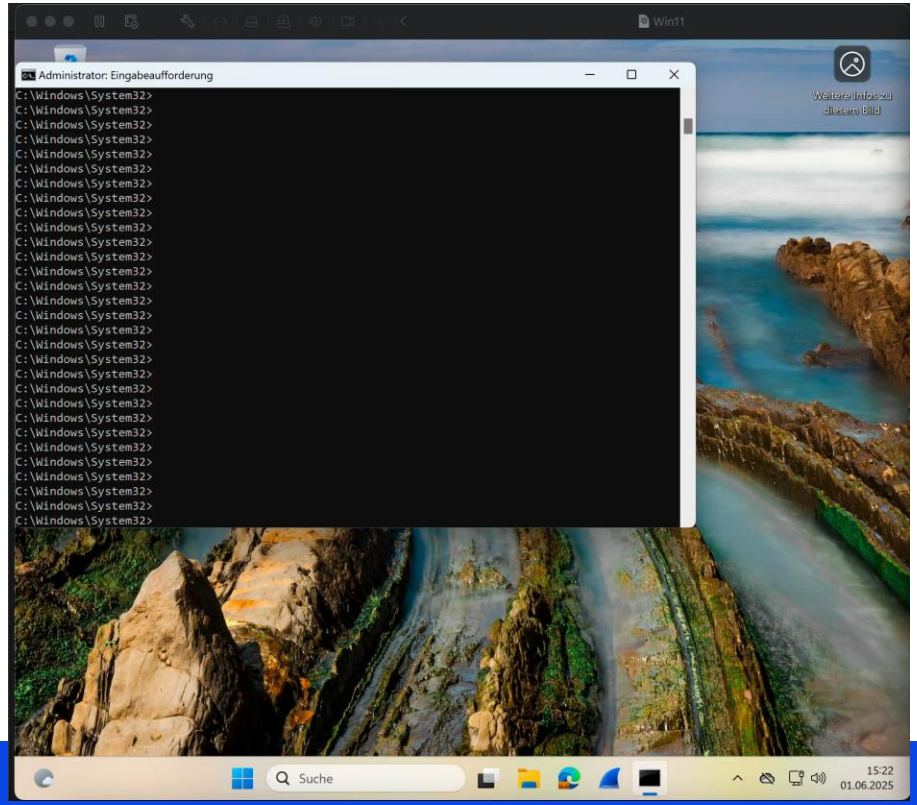


Host-basierte Aufzeichnung | pktmon

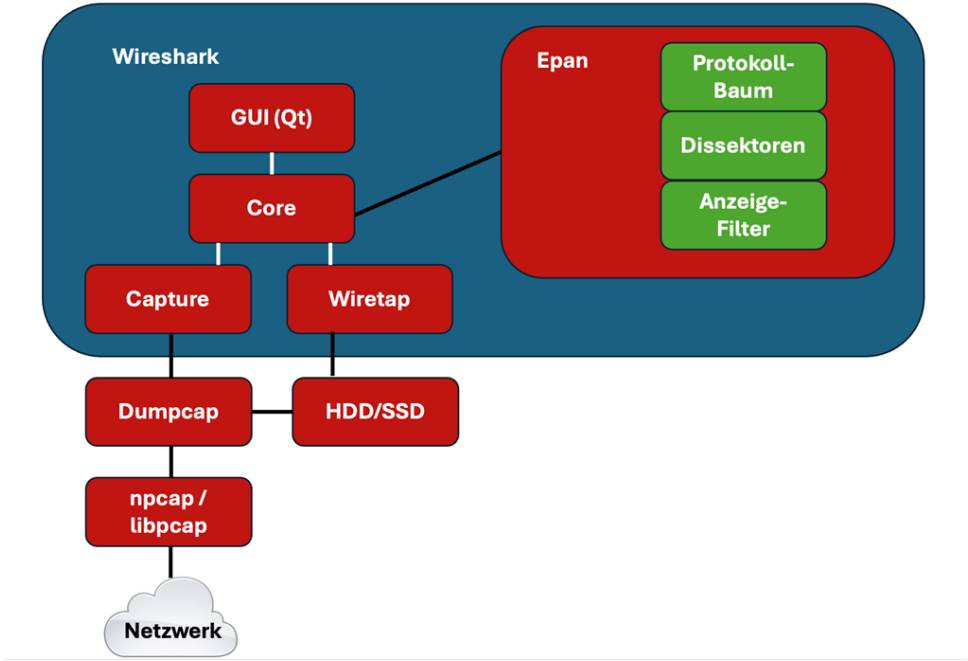
```
pktmon filter remove
pktmon filter add -t TCP -p 5060
pktmon filter –i 192.0.2.1
pktmon filter list
pktmon start --etw -f vaf.etl
pktmon counters
pktmon stop
pktmon pcapng vaf.etl -o vaf.pcapng
```



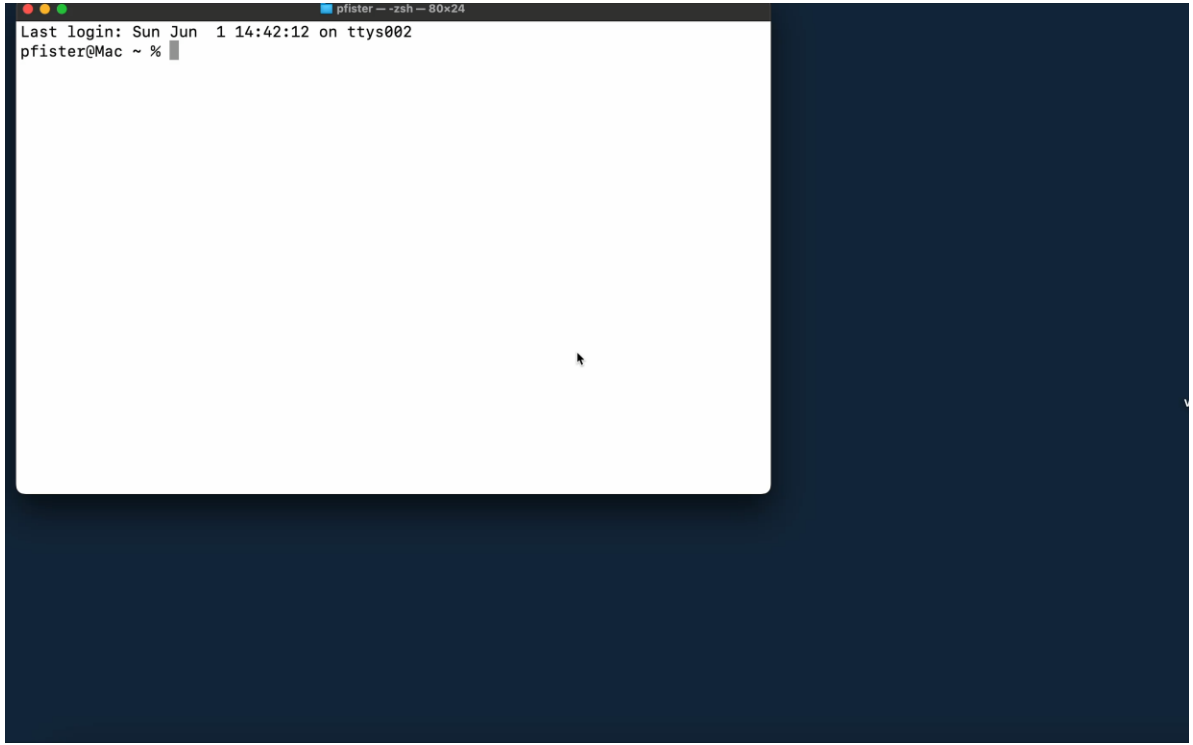
Host-basierte Aufzeichnung | pktmon



Host-basierte Aufzeichnung | Wireshark



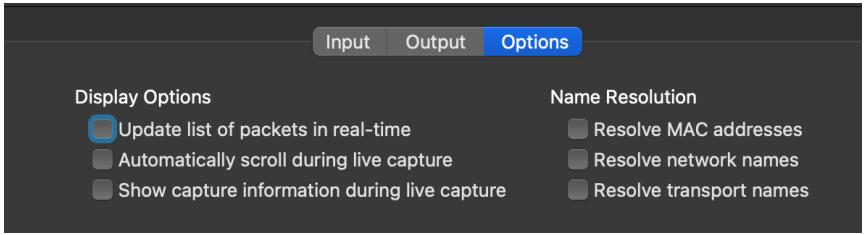
Host-basierte Aufzeichnung | Wireshark

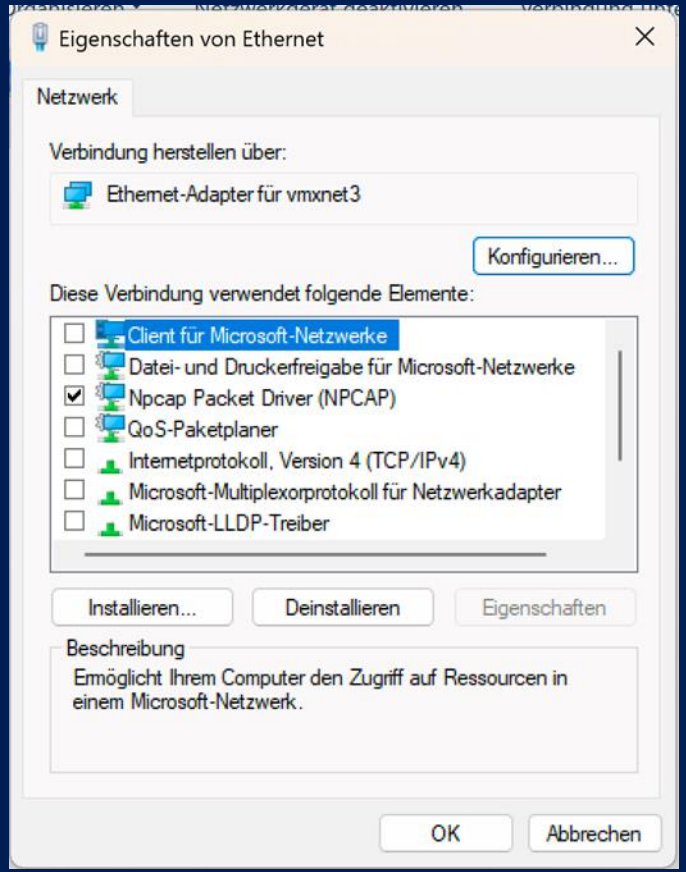


Host-basierte Aufzeichnung | Wireshark

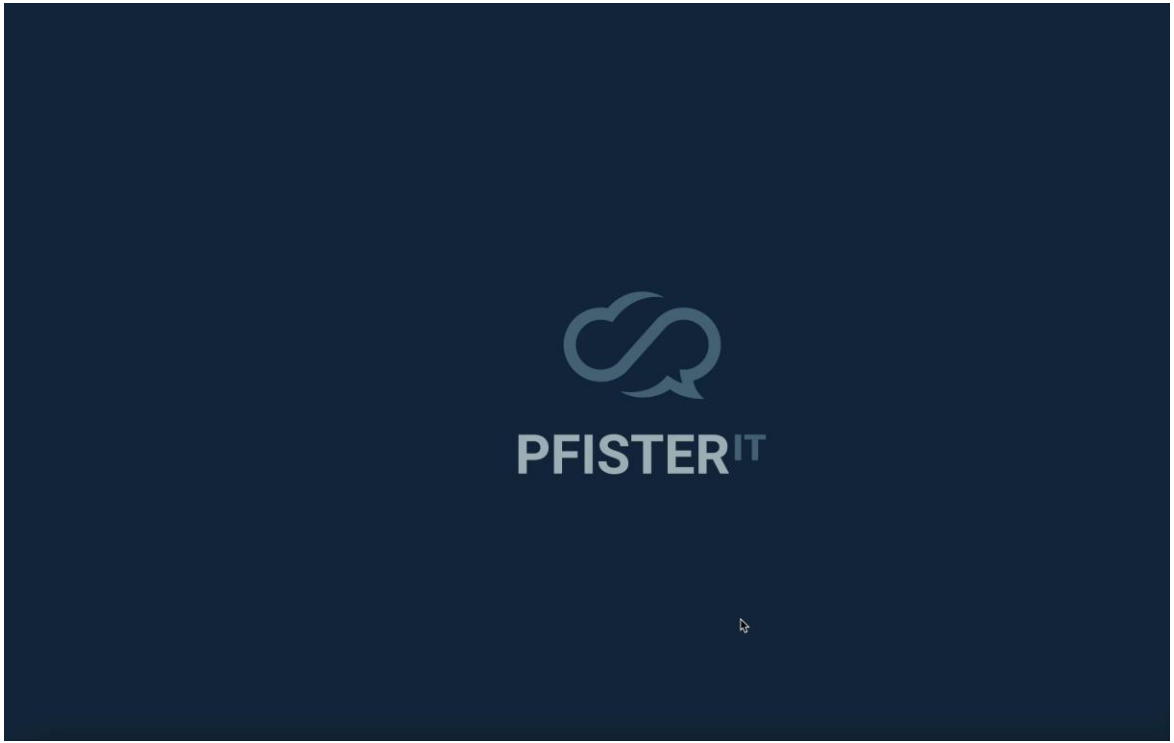
Optimierungspotenzial für Mittschnitt

- Puffer
- MAC nicht auflösen
- Namen nicht auflösen
- Update der Paketliste

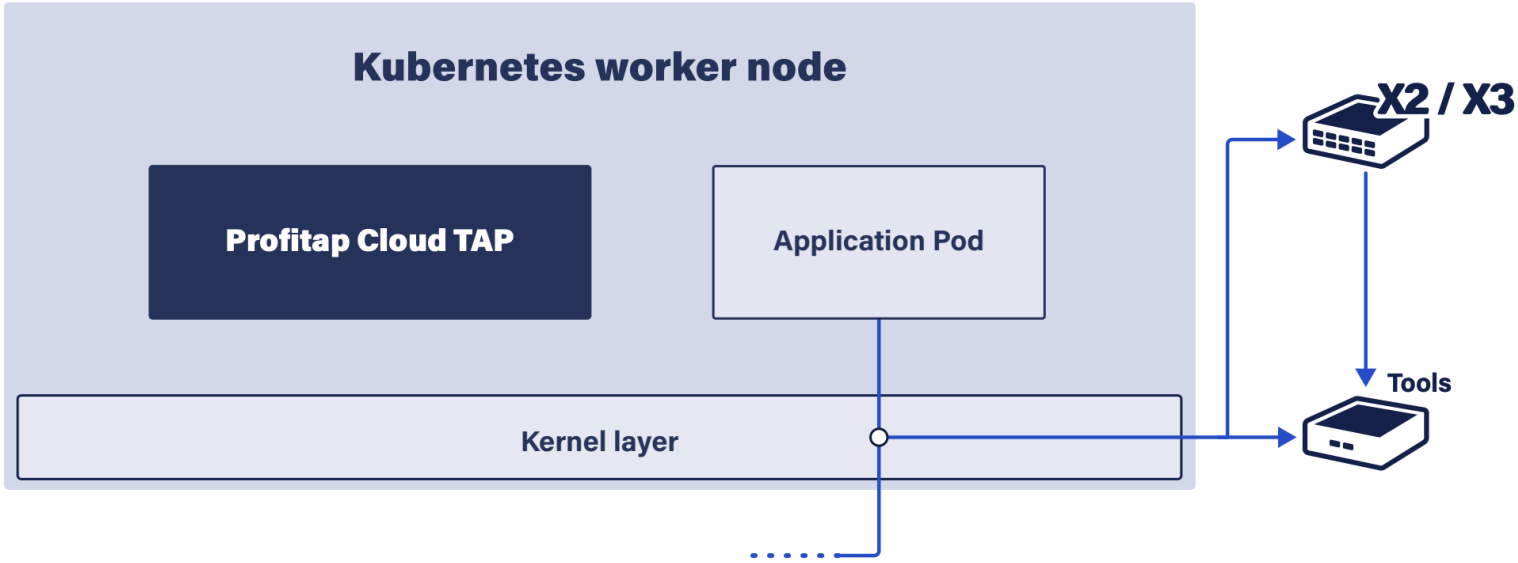




Host-basierte Aufzeichnung | Docker Container



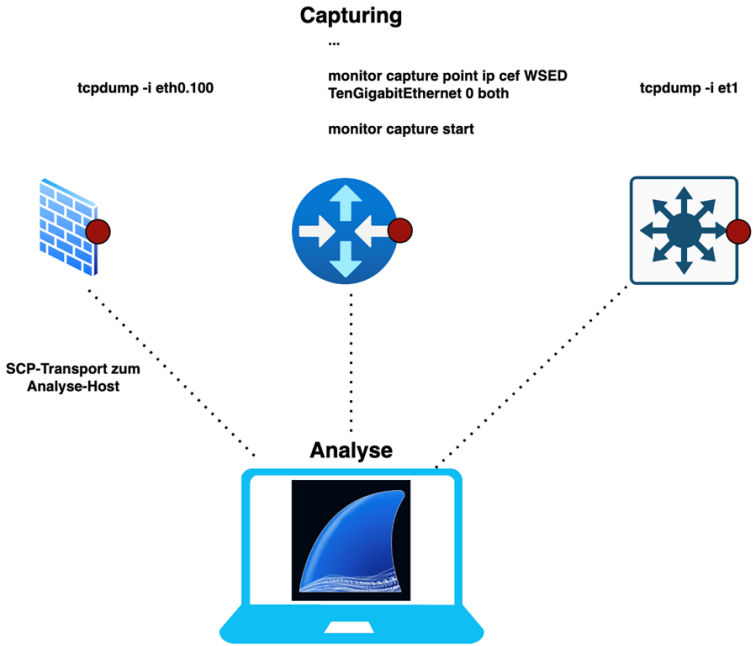
Host-basierte Aufzeichnung | K8S



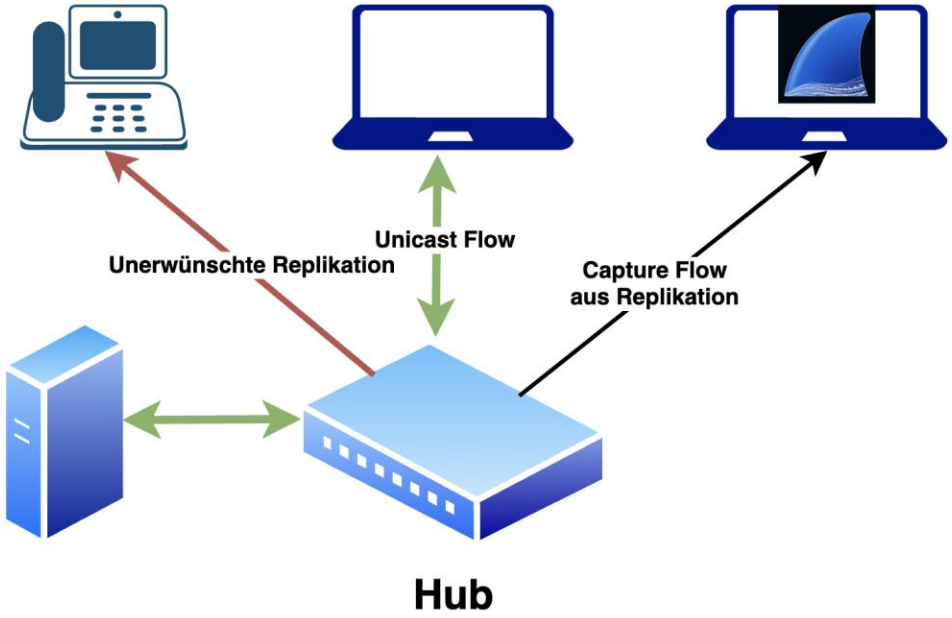
Host-basierte Aufzeichnung | Warum nicht?

- Ressourcenabhängigkeit
- Verfälschung der Aufzeichnung
- Berechtigung

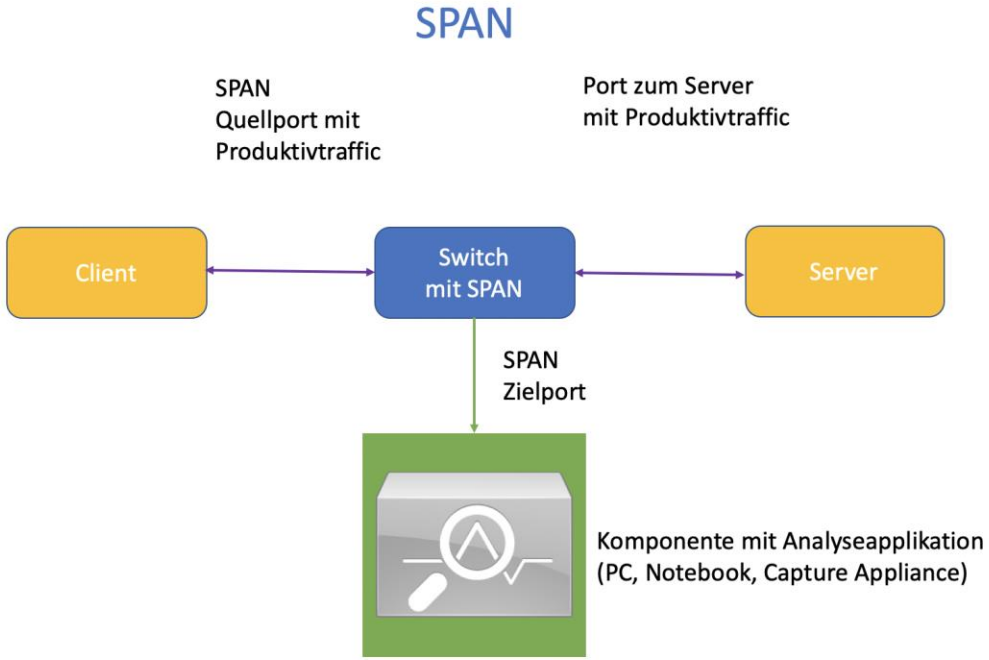
Capturing auf Netzwerkkomponenten



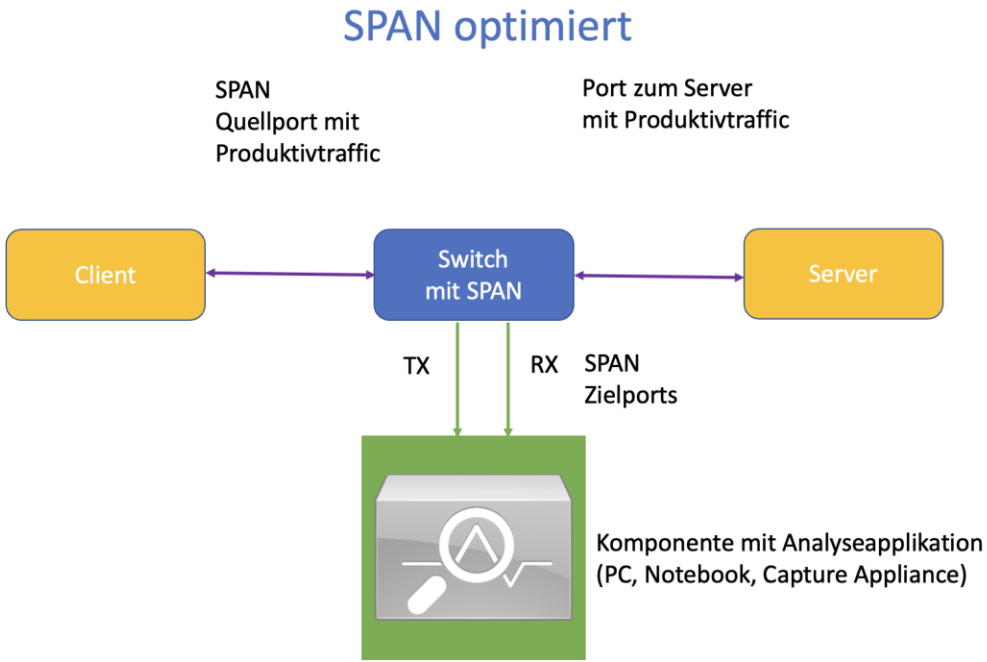
Hubs


Unerwünschte Replikation
Unicast Flow
Capture Flow
aus Replikation
Hub

Port Mirroring / SPAN



SPAN optimiert

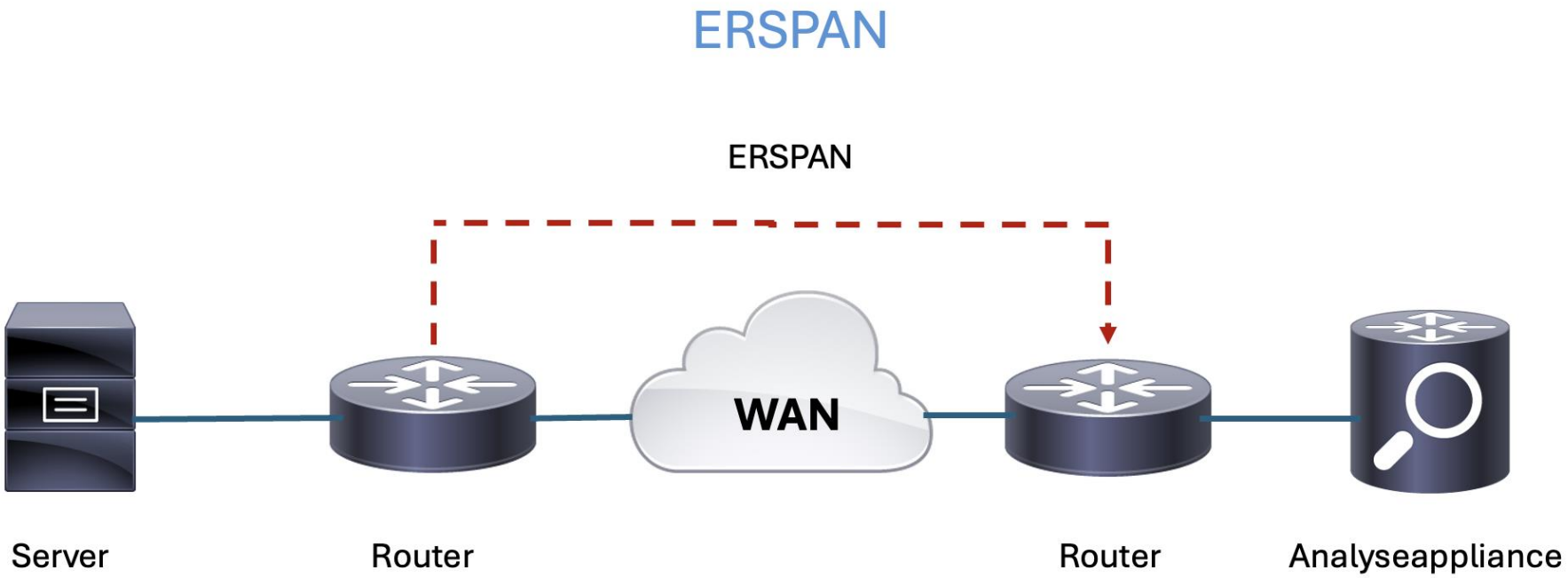


SPAN Config

- **Beispielconfig Standard**
- Switch(config)**#monitor session 1 source interface Eth0/1**
- Switch(config)**#monitor session 1 destination interface Eth0/2**

- **Beispielconfig optimiert**
- Switch(config)**#monitor session 1 source interface Eth0/1 tx**
- Switch(config)**#monitor session 2 source interface Eth0/1 rx**
- Switch(config)**#monitor session 1 destination interface Eth0/2**
- Switch(config)**#monitor session 2 destination interface Eth0/3**

ERSPAN



ERSPAN Config

Quelle

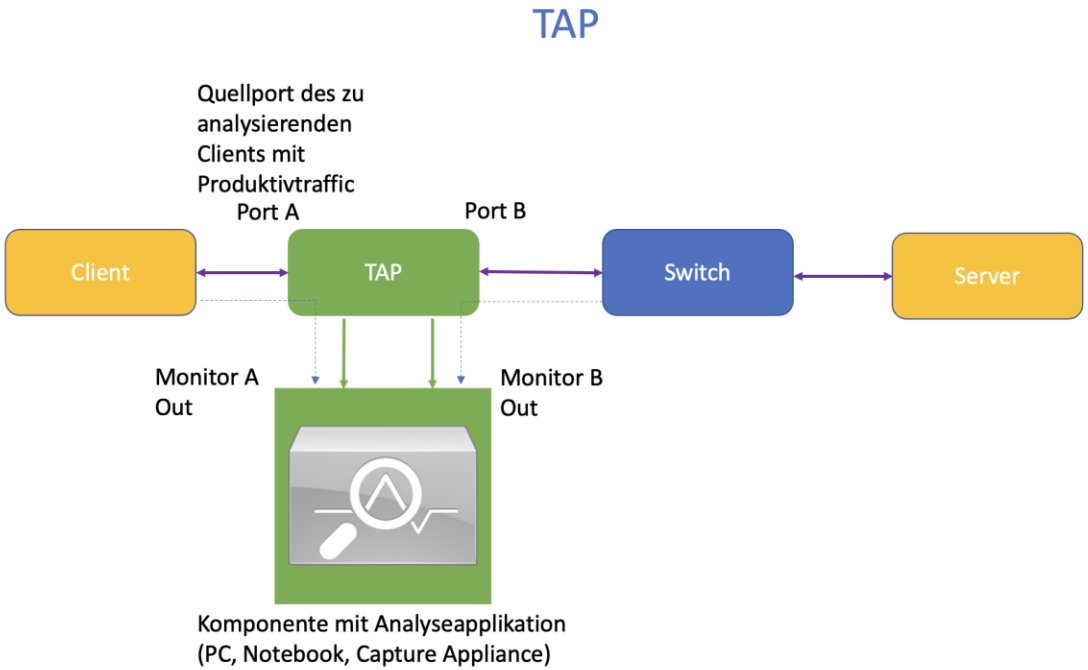
- R1(config)#**monitor session 1 type erspan-source**
- R1(config-mon-erspan-src)#**source interface GigabitEthernet 0/0**
- R1(config-mon-erspan-src)#**no shutdown**
- R1(config-mon-erspan-src)#**destination**
- R1(config-mon-erspan-src-dst)#**erspan-id 100**
- R1(config-mon-erspan-src-dst)#**ip address 172.16.2.200**
- R1(config-mon-erspan-src-dst)#**origin ip address 172.16.12.1**

ERSPAN Config

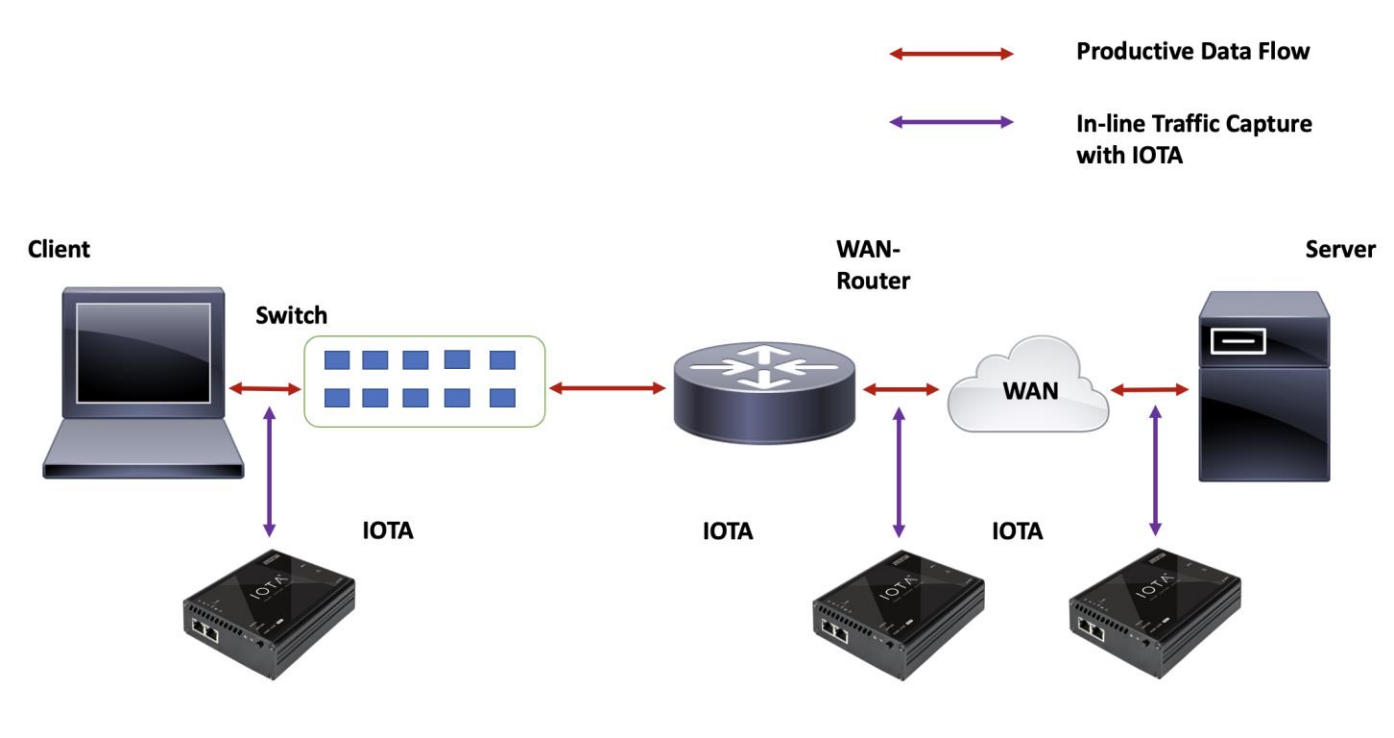
Senke/Ziel

- R2(config)#**monitor session 1 type erspan-destination**
- R2(config-mon-erspan-dst)#**no shutdown**
- R2(config-mon-erspan-dst)#**destination interface GigabitEthernet 0/0**
- R2(config-mon-erspan-dst)#**source**
- R2(config-mon-erspan-dst-src)#**erspan-id 100**
- R2(config-mon-erspan-dst-src)#**ip address 172.16.12.1**

TAPs – Professionelle Netzwerkanalyse



Capture Appliances



Bildquellen

Pexels https://www.pexels.com/de-de/

Unsplash https://unsplash.com/de

Danke

linkedin.com/in/benjamin-pfister-90136b298

Sponsored by PROFITAP & emitec datacom

WIRESHARK