



Digital Investigation in OpenFlow Networks with ForCon

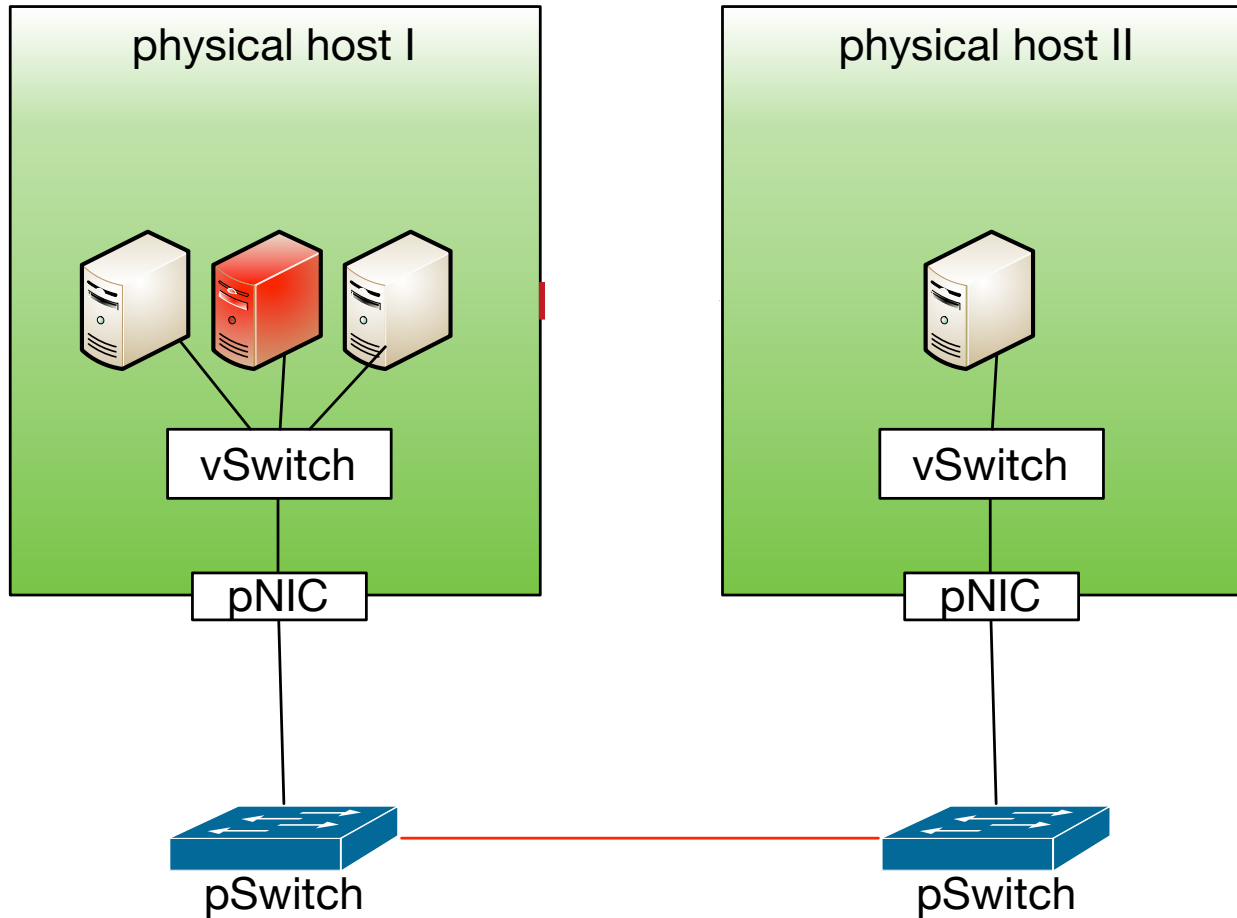
DFRWS EU 2017

Überlingen, 23.03.2017

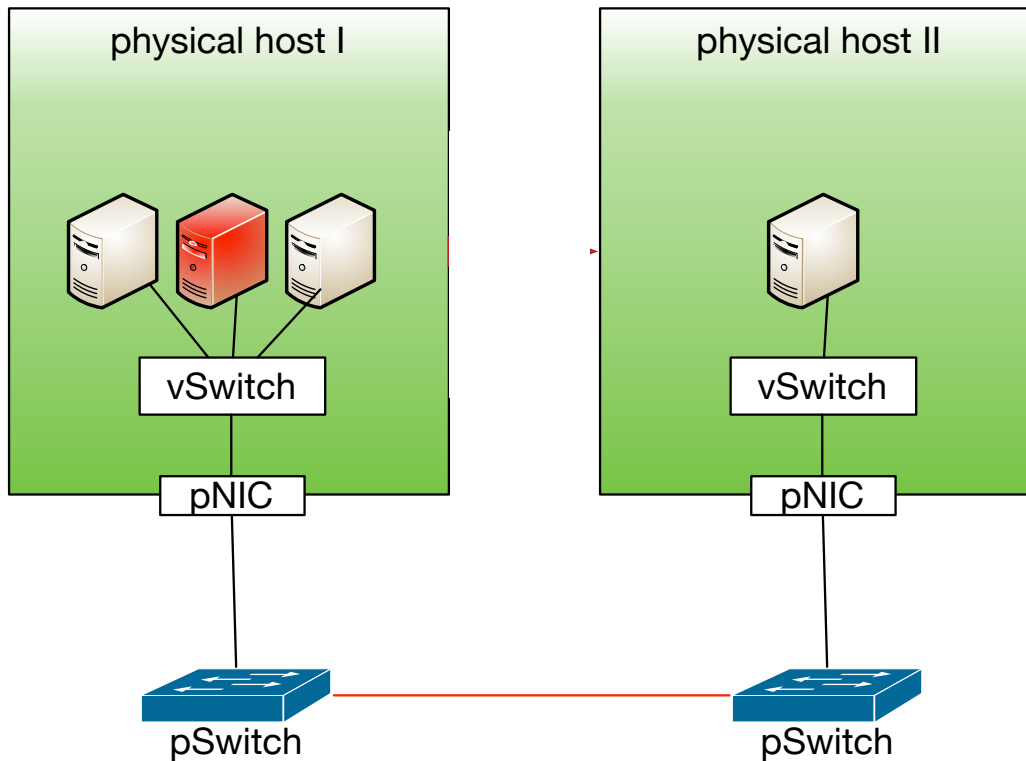
Daniel Spiekermann, Jörg Keller, Tobias Eggendorfer

© FernUniversität in Hagen / Horst Pierdolla

Your job ... wiretap the red VM

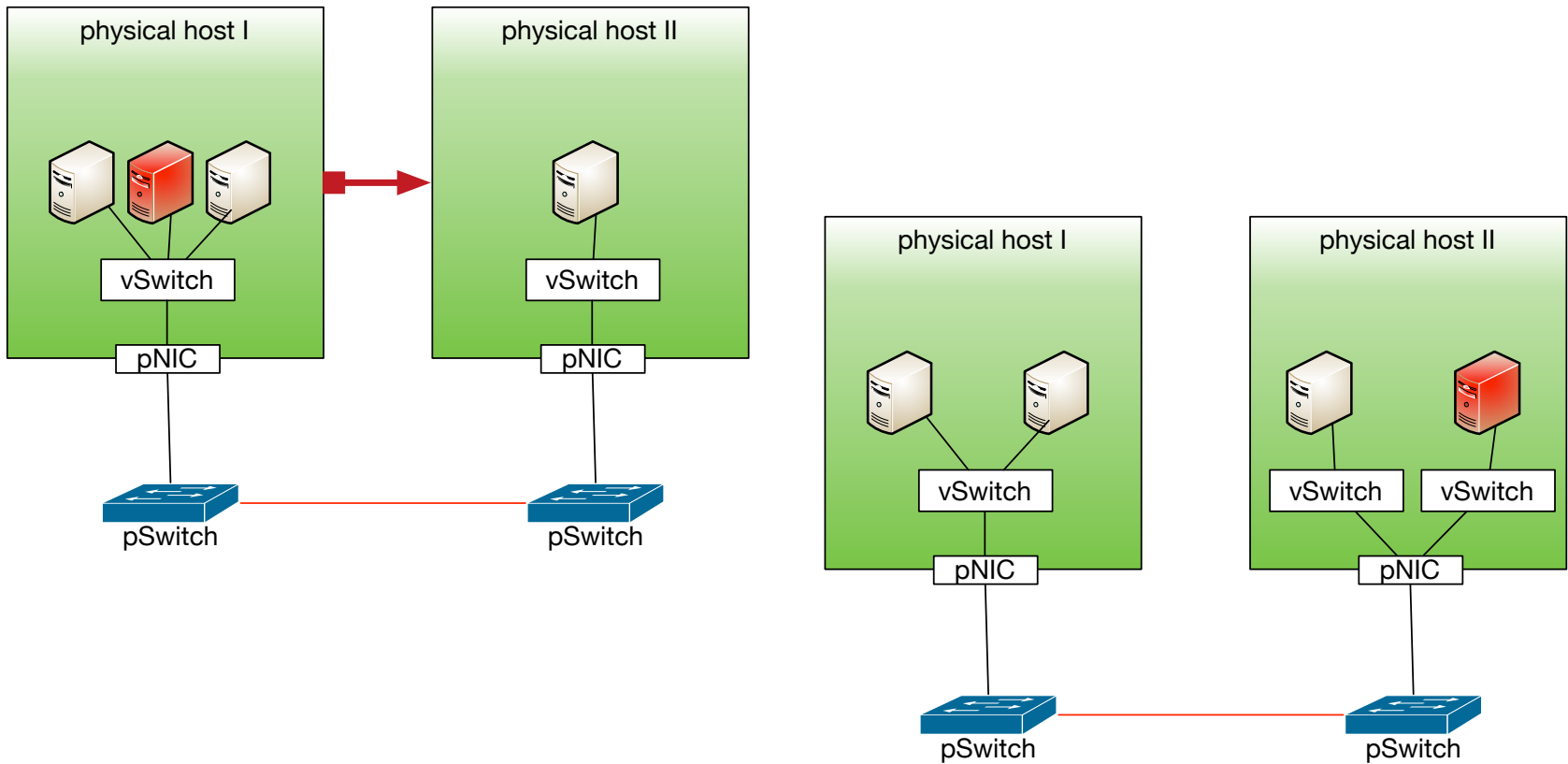


Your job ... wiretap the red VM



- Identify the target
- Install your equipment
- Capture traffic
- Wait
- Analysis

Your job ... wiretap the red VM



Research Questions

- How can you capture the entire network traffic of the SOI?
 - How can you determine the migration of the SOI?
 - How can you reconfigure the capture process as fast as possible?
 - How can the network traffic be reduced to the relevant information?

Overview

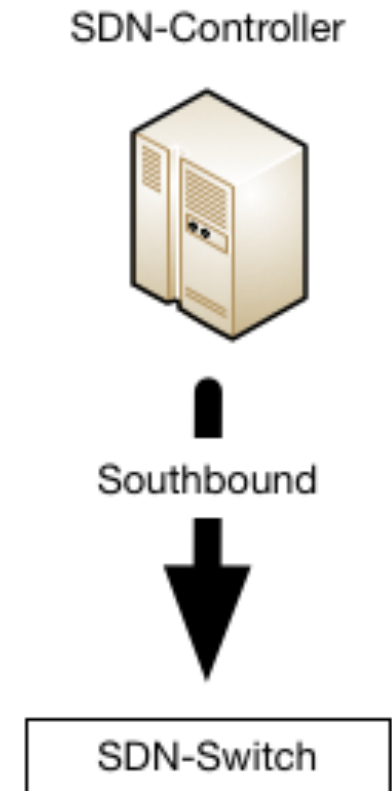
- A new challenge
- SDN and OpenFlow
- Virtual Network Forensic Process
- ForCon
- Evaluation

A new challenge

- Migration of VM is managed autonomous by the environment
 - Cloud controller manages the VM
 - SDN controller manages the network
 - Traffic control
 - Routing policies
 - ACLs

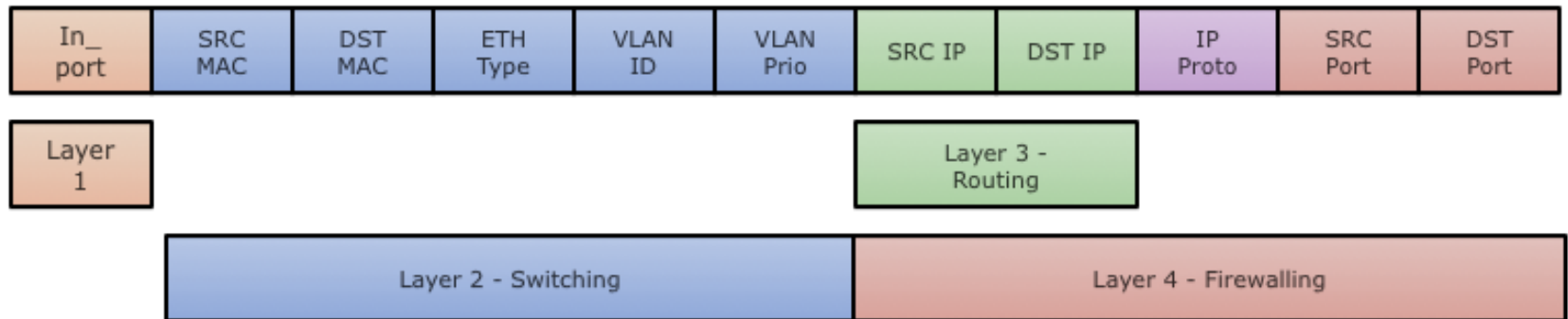
SDN with OpenFlow

- Most notable protocol for southbound api
- Uses flows to process the packets
- Flows are stored in flow table on the OF-switch



SDN with OpenFlow


- Most notable protocol for southbound api
- Uses flows to process the packets
- Flows are stored in flow table on the OF-switch
- A flow is a combination of header fields



```
SKB_PRIORITY(0),IN_PORT(2),ETH(SRC=00:1B:11:B4:DE:FC,DST=FF:FF:FF:FF:FF:FF),ETH_TYPE(0X0800),IPV4(SRC=17.2.20.10.4/0.0.0.0,DST=255.255.255.255/0.0.0.0,PROTO=17/0,TOS=0/0,TTL=64/0,FRAG=NO/0XFF), ACTIONS=OUTPUT:3
```

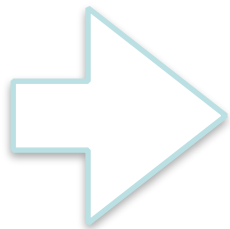
A new challenge

- Migration of VM is managed autonomous by the environment
 - Cloud controller manages the VM
 - SDN controller manages the network
 - Traffic control
 - Routing policies
 - ACLs

 Highly dynamic environment

A new challenge

- Migration of VM is managed autonomous by the environment
 - Cloud controller manages the VM
 - SDN controller manages the network
 - Traffic control
 - Routing policies
 - ACLs



Highly dynamic environment

- But:
 - Traditional network forensic investigation is static

How to capture traffic in virtual environments

- Find the SOI
- Find the relevant OF-switch

Identification

How to capture traffic in virtual environments

- Find the SOI
- Find the relevant OF-switch
- Extract needed information
- Manipulate flows in relevant OF-switch

Identification

Preparation

How to capture traffic in virtual environments

- Find the SOI
- Find the relevant OF-switch
- Extract needed information
- Manipulate flows in relevant OF-switch
- Capture and store the traffic

Identification

Preparation

Capture

Recording

How to capture traffic in virtual environments

- Find the SOI
- Find the relevant OF-switch
- Extract needed information
- Manipulate flows in relevant OF-switch
- Capture and store the traffic
- Monitor the environment

Identification

Preparation

Capture

Recording

Monitoring

How to capture traffic in virtual environments

- Find the SOI
- Find the relevant OF-switch
- Extract needed information
- Manipulate flows in relevant OF-switch
- Capture and store the traffic
- Monitor the environment
- React on relevant changes

Identification

Preparation

Capture

Evaluation

Recording

Monitoring

How to capture traffic in virtual environments

- Find the SOI
- Find the relevant OF-switch
- Extract needed information
- Manipulate flows in relevant OF-switch
- Capture and store the traffic
- Monitor the environment
- React on relevant changes
- Adapt relevant flows

Identification

Preparation

Capture

Adaptation

Evaluation

Recording

Monitoring

How to capture traffic in virtual environments

- Find the SOI
- Find the relevant OF-switch
- Extract needed information
- Manipulate flows in relevant OF-switch
- Capture and store the traffic
- Monitor the environment
- React on relevant changes
- Adapt relevant flows
- Analysis

Identification

Preparation

Capture

Adaptation

Evaluation

Recording

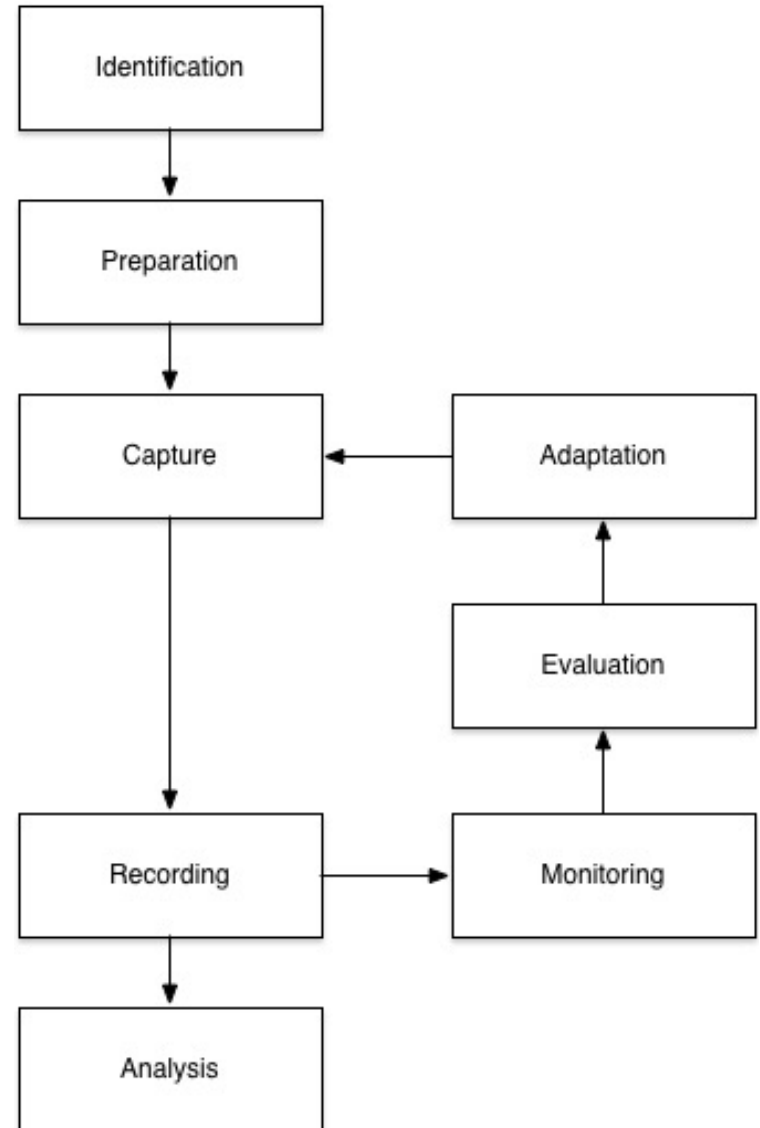
Monitoring

Analysis

Virtual network forensic process

Process model for network forensic
Investigation in virtual networks

Circuit of different phases
Repetitive use of phases



ForCon

- (still a proof-of-concept)
- Forensic Controller
- Based on the VNFP
- Implements network forensic investigation in virtual networks

- Central server, distributed agents
 - SDN-agent (1/host)
 - Mirror-agent (1/network)
- Extract and manipulates OpenFlow-Flows

ForCon Workflow I

- Agents connect to ForCon

Connection from agent 172.16.40.129 established

Connection from mirror-agent 172.16.40.122
established

- Agent transmits the local flows to ForCon

```
I;s1;00:00:00:00:00:03;00:00:00:00:00:01
```

```
I;s1;00:00:00:00:00:01;00:00:00:00:00:03
```

- ForCon analyses these flows and searches for the identifier of the target
- Decision:
 - Hit: Create vxlan-tunnel between mirror agent and involved vswitch
 - Miss: Just wait for newer flows (send by agents)

ForCon flow manipulation

- Ingress

```
cookie=0x0, duration=11965.378s, table=0,  
n_packets=10120, n_bytes=975632,  
priority=2, in_port=1, dl_dst=00:00:00:00:00:03  
actions=output:2, 99
```

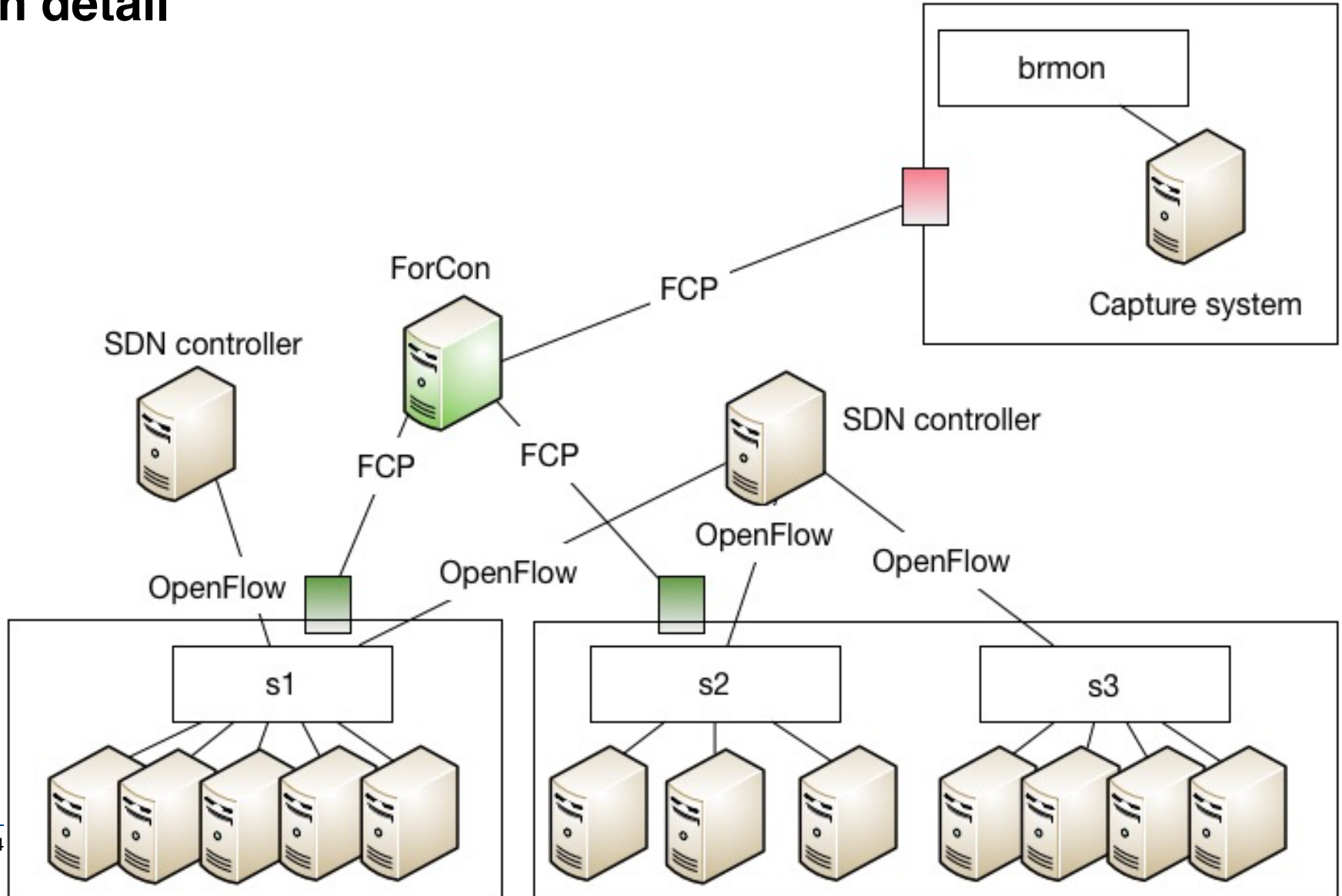
- Egress (Destination-MAC is needed)

```
cookie=0x0, duration=1604.682s, table=0, n_packets=0,  
n_bytes=0,  
priority=2, dl_src=00:00:00:00:00:03, dl_dst=00:00:00:0  
0:00:01 actions=output:1, output:99
```

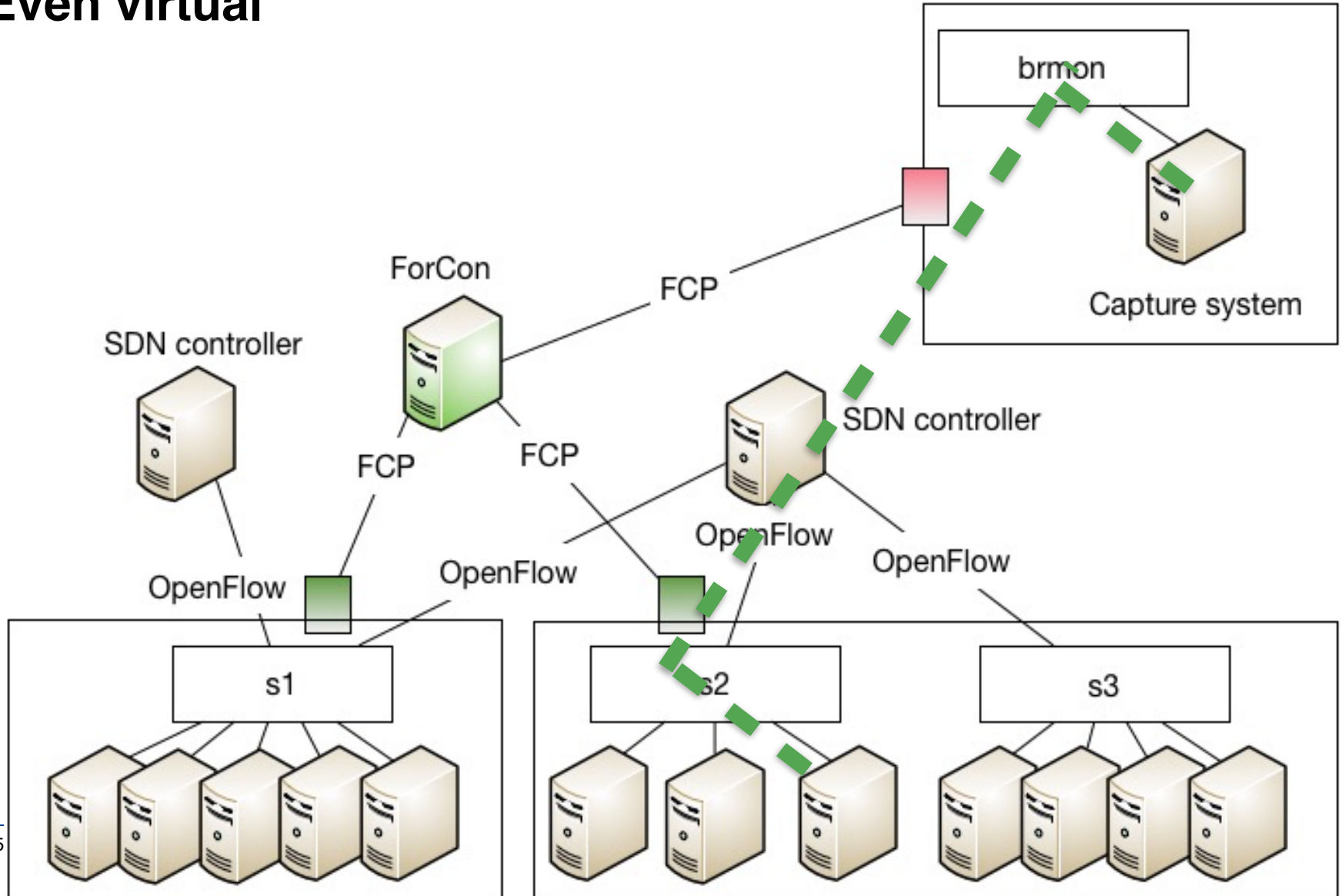
ForCon - just a shallow dive

- Use of existing tools: *ovs-ofctl dump-flows*
- Format of flows deterministic, but vendor specific
- Classification of fields
 - Priority
 - Action
 - Group
 - Timer
 - Hard-TO
 - Idle-TO
- Split the flow
- Store relevant data
- Adaptation regarding to the given situation

In detail



Even virtual



Evaluation

- How is ForCon operating in different situation?
 - Limiting resources are cpu-load, CAM, network bandwidth
- Does ForCon capture all network packets?
 - Compare number of transmitted and received data
 - regarding to target VM and capture system
- Are the captured packets „correct“?

Result

- High CPU load (*stress*)
- CAM (*vNICs*)
- Network usage (*iperf*)
- Integrity
- 100% packet match
- 100% packet match
- 100% packet match
- Extracted payload matches

```
md5 *.pcap
MD5 (ChunkedFile.pcap) =
ed96fa2fba48ade3f7d2e8a7dc20f9d4
MD5 (ChunkedFile_mirror.pcap) =
ed96fa2fba48ade3f7d2e8a7dc20f9d4
```

Conclusion

- SDN (and network virtualization) increase flexibility and dynamic in nowadays data centers
- OpenFlow as the most notable protocol provides no forensic capabilities
- Migration of VMs is most critical
- ForCon eradicates the static implementations and provides an ongoing capture process even by moving of the SOI
- Distributed agents monitor and manipulate flows
- Evaluation of ForCon validates the correctness of the process

Thank you

Contact:

Daniel Spiekermann

daniel.spiekermann@fernuni-hagen.de