Software-Defined Security

Seungwon Shin
claude@kaist.ac.kr

[redacted]

[redacted]

Opportunities for Security Functions

- Network security functions
  - Network abnormal detection (DDoS, network scan)
  - In-line mode security functions (firewall, NIPS)
  - Passive mode security functions (NIDS)
  - Advanced network security functions (stateful firewall, reflector net)

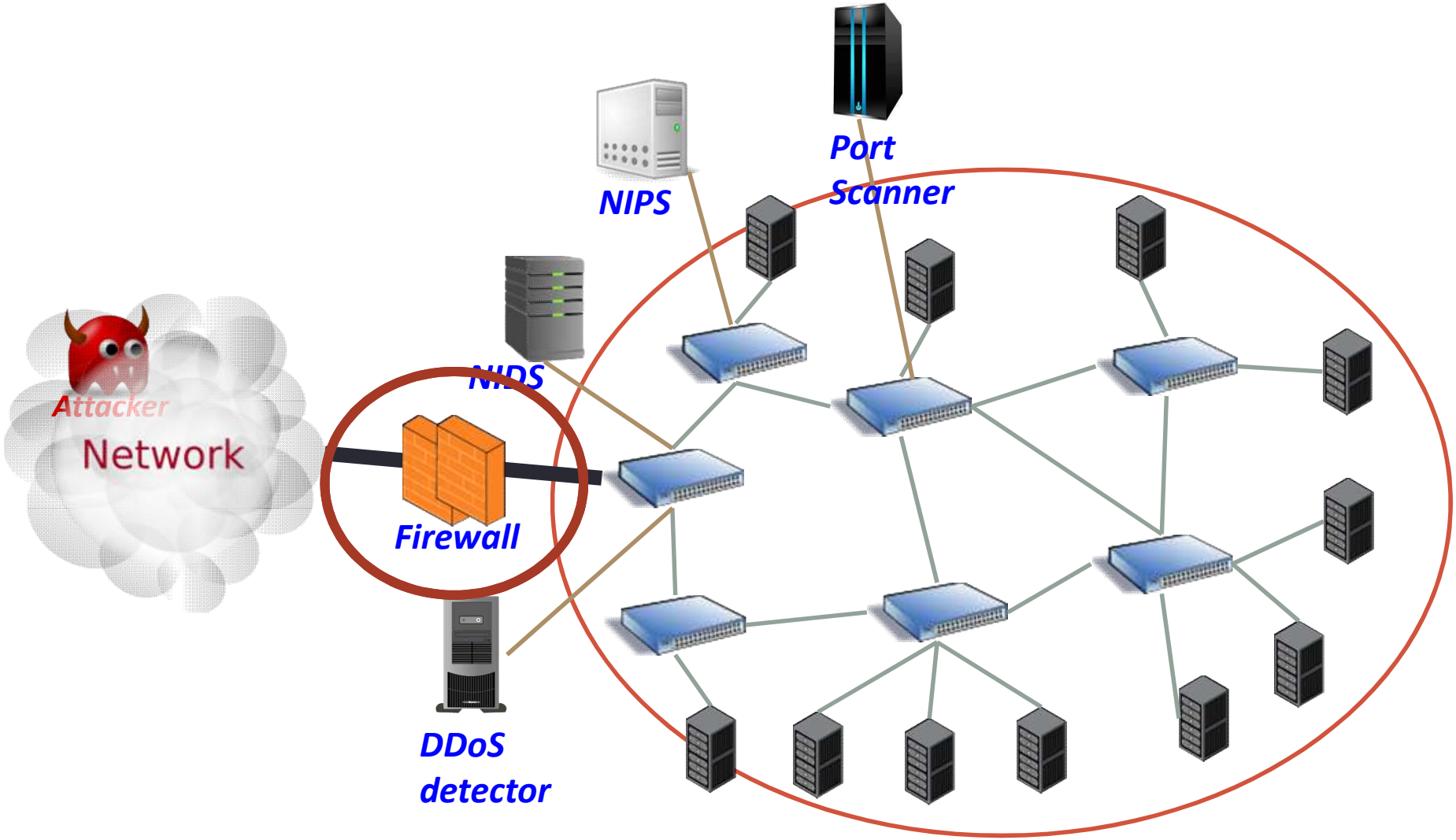
Can SDN technology help in implementing network security functions?

Goal

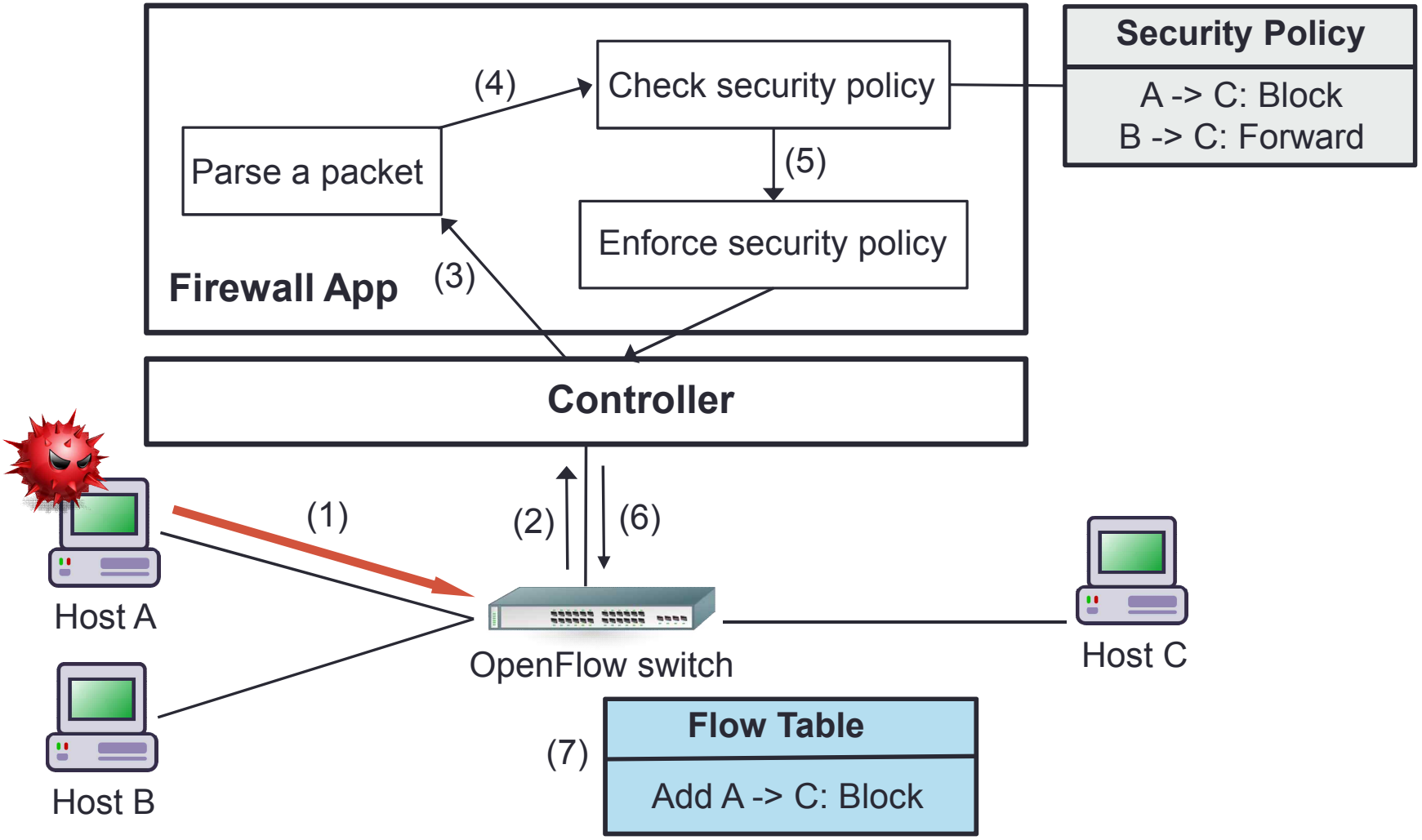
Translation

Firewall with SDN	NIDS with SDN	NIPS with SDN	DDoS Detector with SDN

Motivating Examples



Conceptual Firewall Implementation
(FloodLight case)



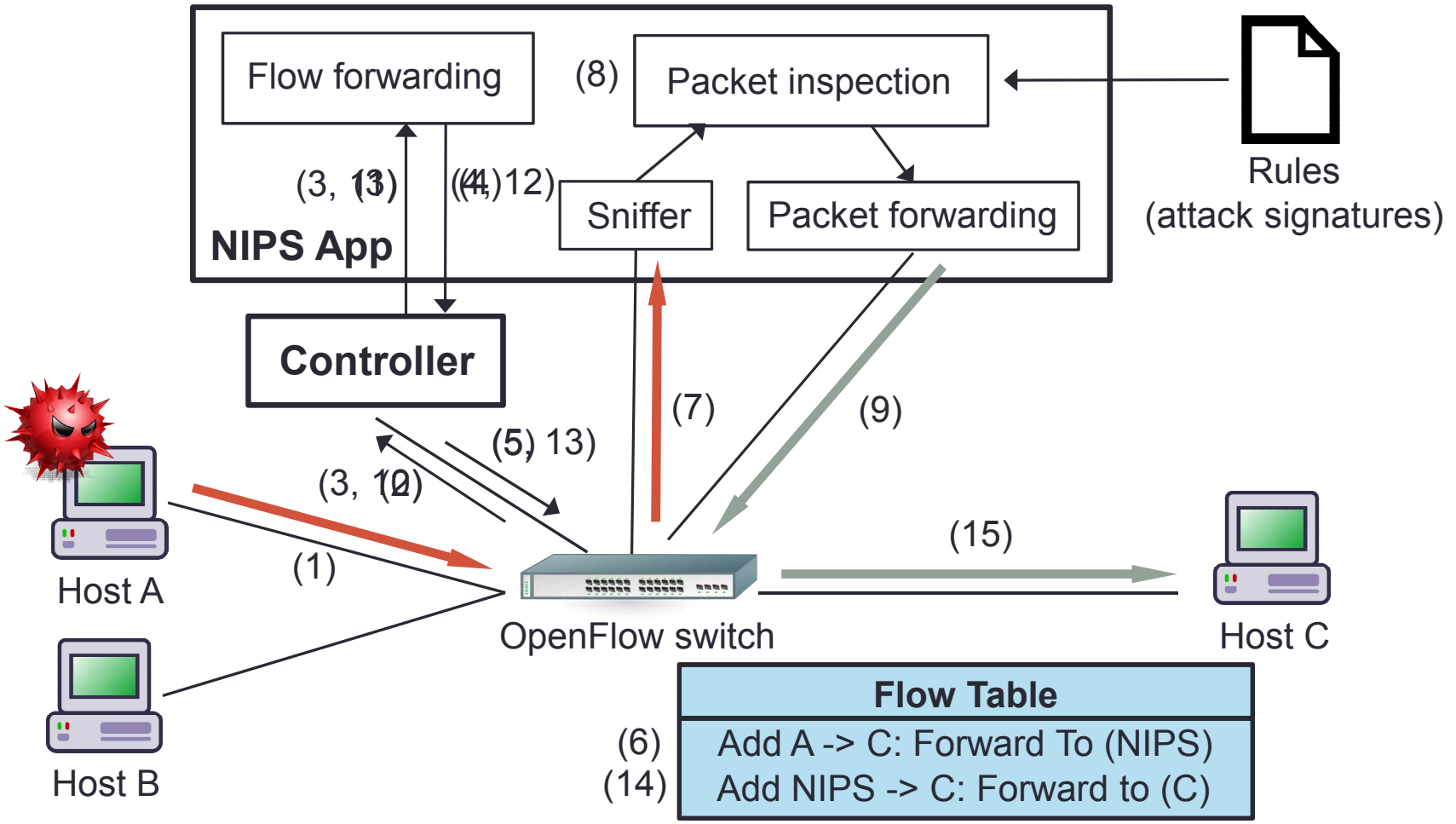
More USE CASES

[redacted]

[redacted]

In-line Mode Security Application

- Network intrusion prevention system (NIPS)



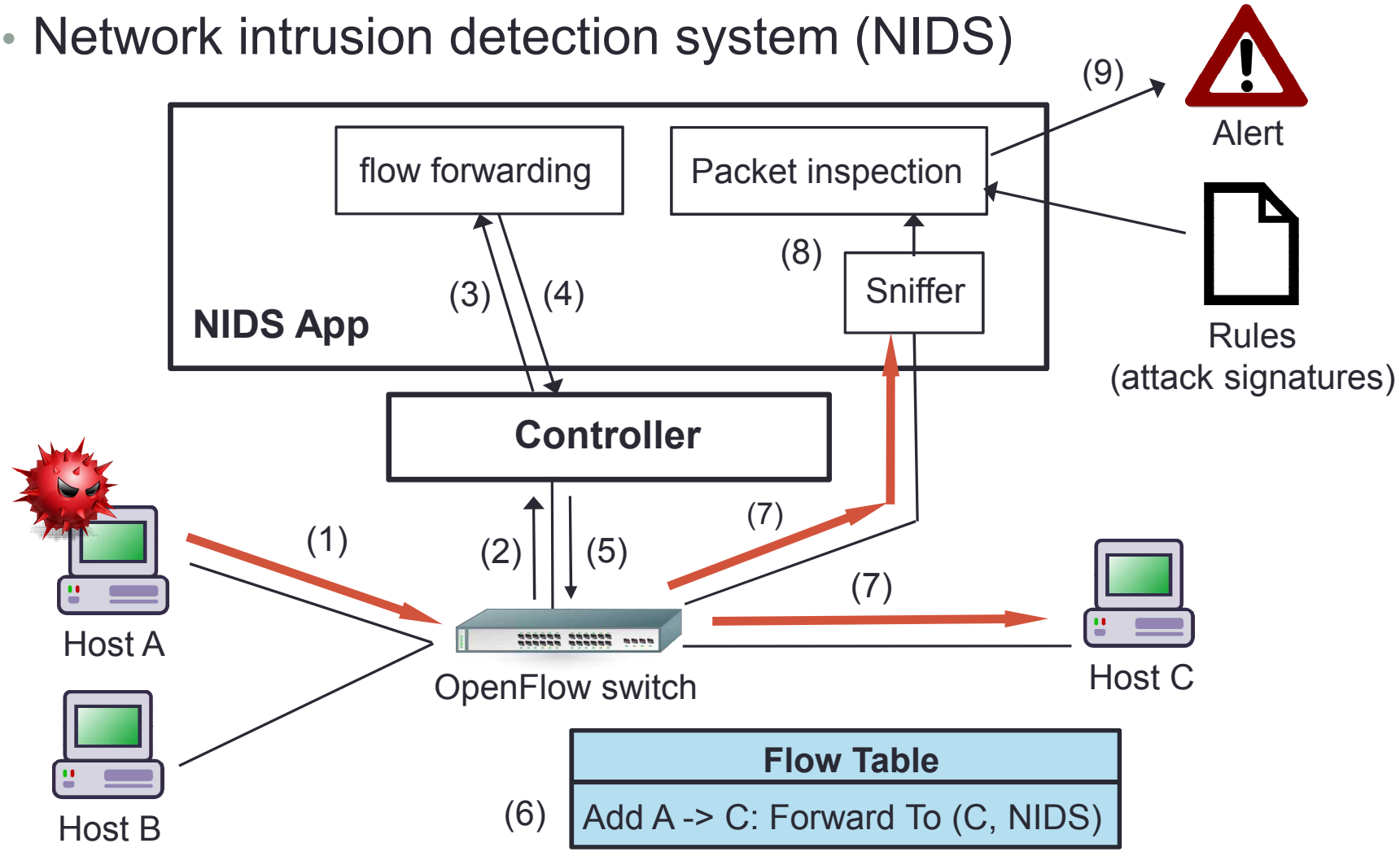
In-line Mode Security Application

- Why it works in SDN
  - No additional 3rd-party devices such as middleboxes
  - No placement problem
  - Easy implementation for advanced functions
    - (e.g., Distributed firewall)

- Why it does not work in SDN
  - Bottleneck of network performance
  - Flow rule conflict problem

Passive Mode Security Application

- Network intrusion detection system (NIDS)



Passive Mode Security Application

- Why it Works in SDN
  - Easy implementation (mirroring ports in network devices)
  - Selective delivery for particular network flows
  - No placement problem (monitor any place)

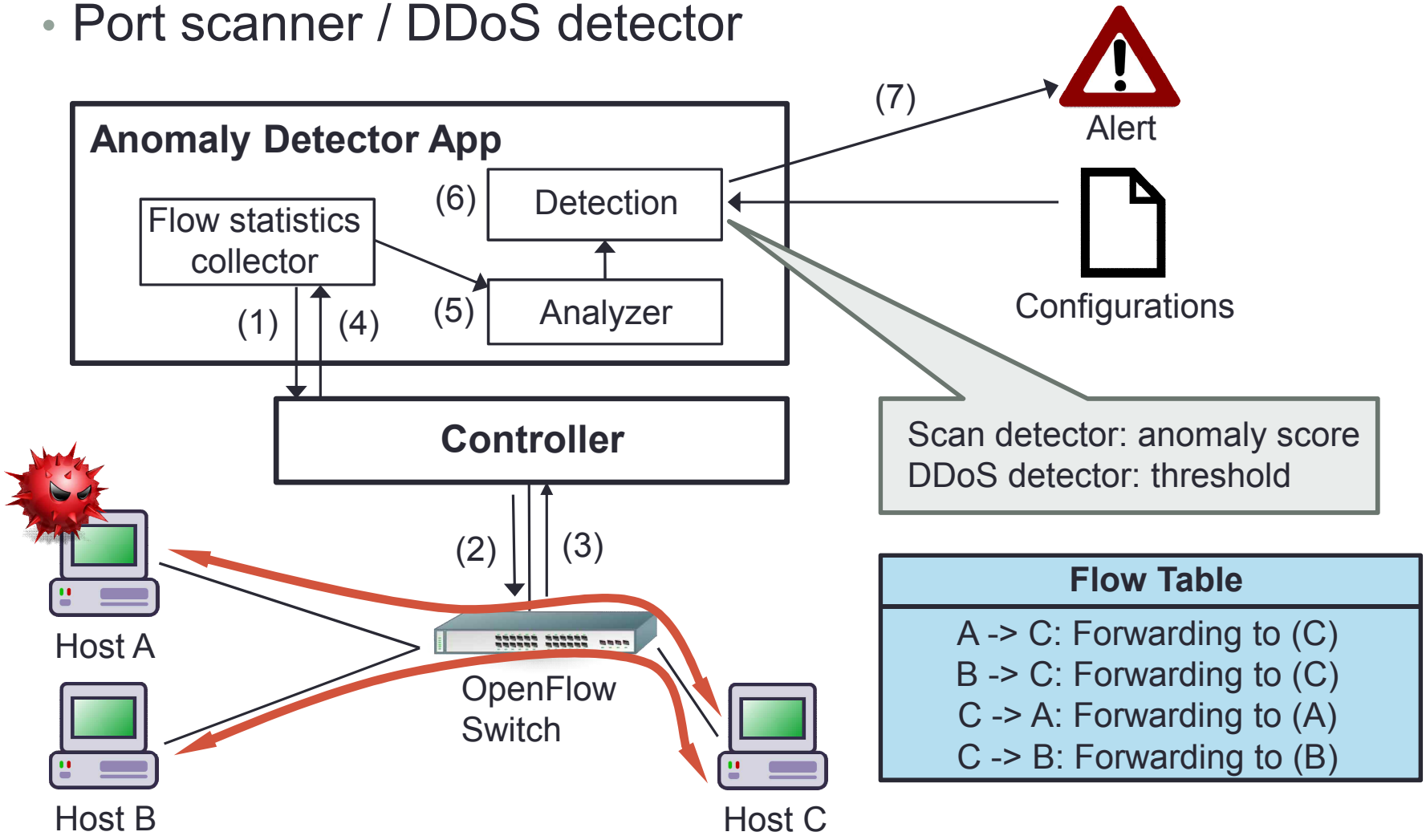
- Why it does not work in SDN
  - Additional network interfaces to collect full payload information between control and data planes
  - Overhead

[redacted]

[redacted]

Network Anomaly Detection Application

- Port scanner / DDoS detector

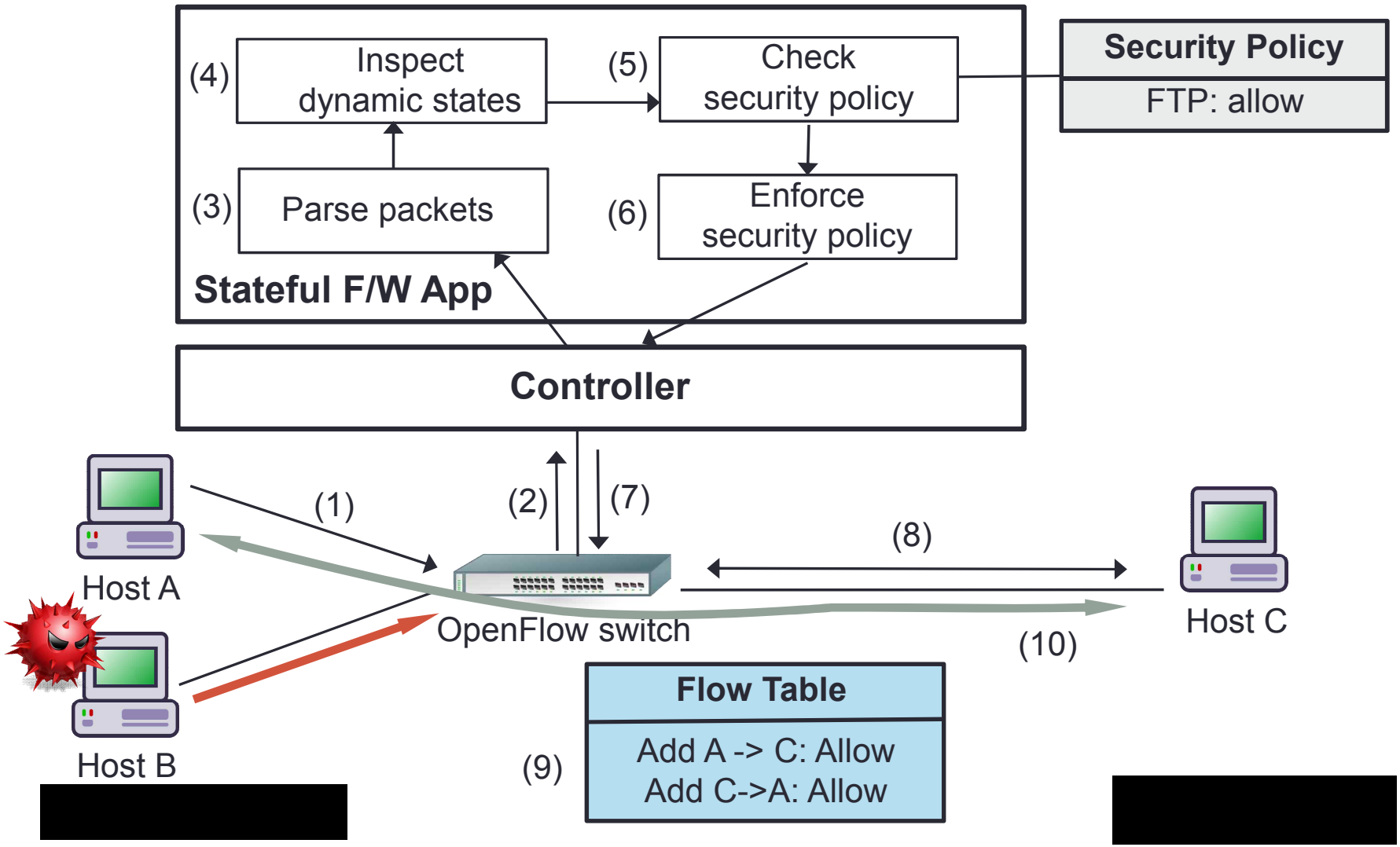


Network Anomaly Detection Application

- Why it works in SDN
  - Easy collection of network information
  - No need for additional devices or complicated configurations
  - No placement problem (monitor any place)

- Why it does not work in SDN
  - Insufficient network information (e.g., TCP session)
  - Performance overhead due to periodical statistics requests

Stateful Firewall Application



Stateful Firewall Application

- Why it works in SDN
  - Low cost
  - No need for additional space for deployment
  - Simple and convenient environment to support various protocols

- Why it does not work in SDN
  - Bottleneck of network performance
  - Additional network interfaces to retrieve raw packets

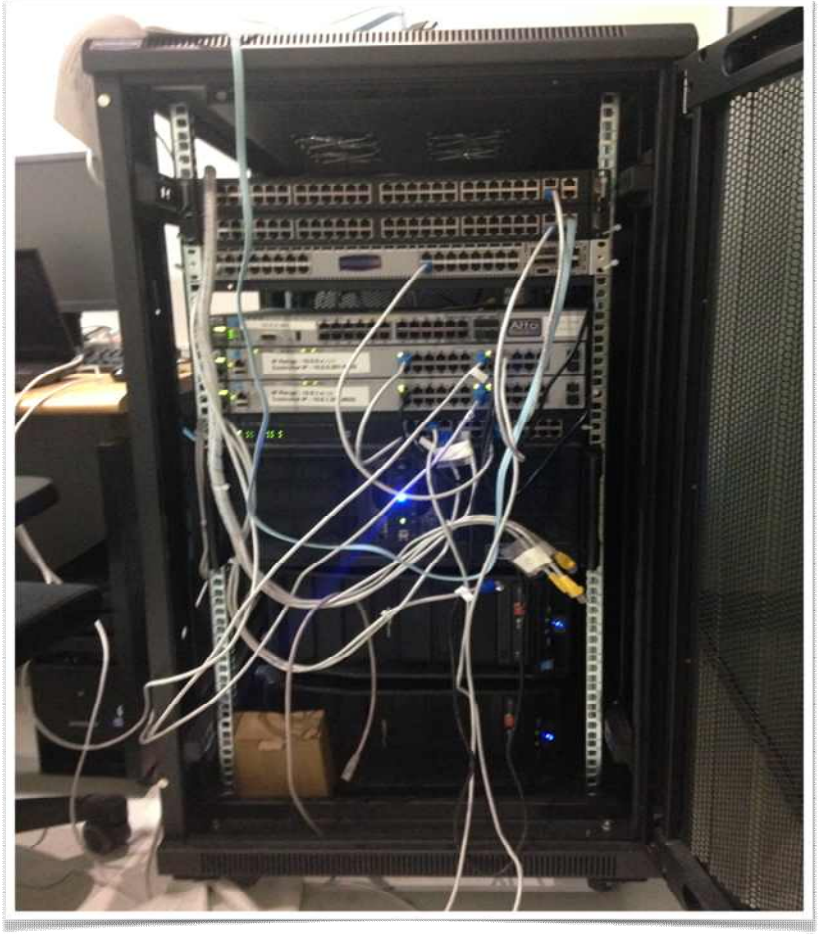
MEASUREMENTS

[redacted]

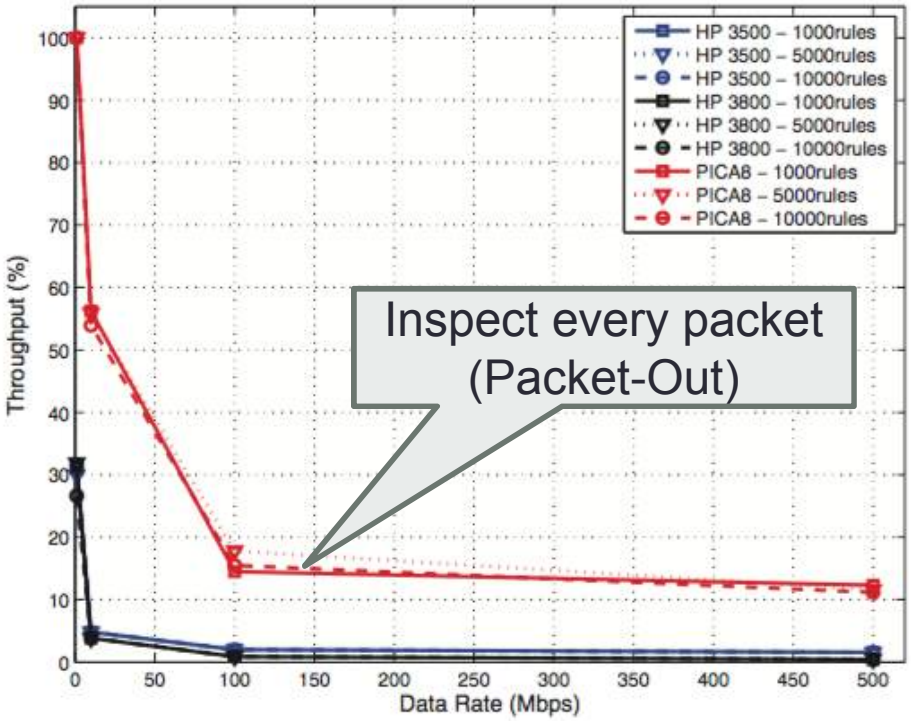
[redacted]

Experimental Setup

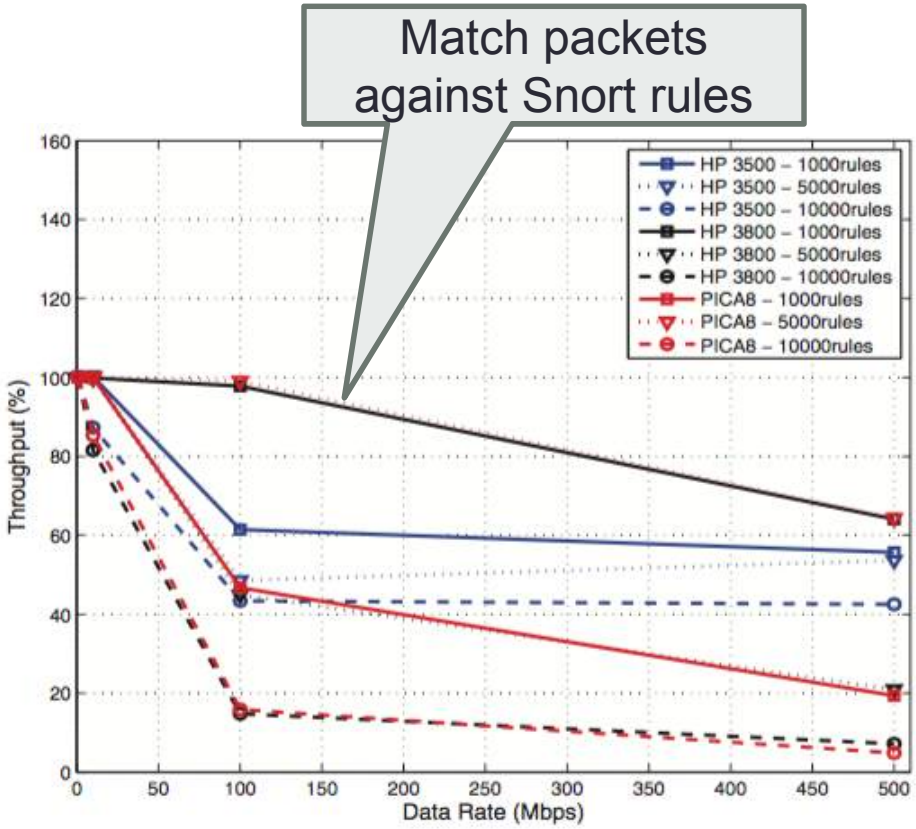
- Physical SDN testbeds
  - A controller machine
    - Core-i5, 16GB Mem
  - Three 1G-bps switches
    - HP 3500yl
    - HP 3800
    - Pica8 P3290
  - Three hosts



In-line Mode Security Applications



Firewall application



NIPS application

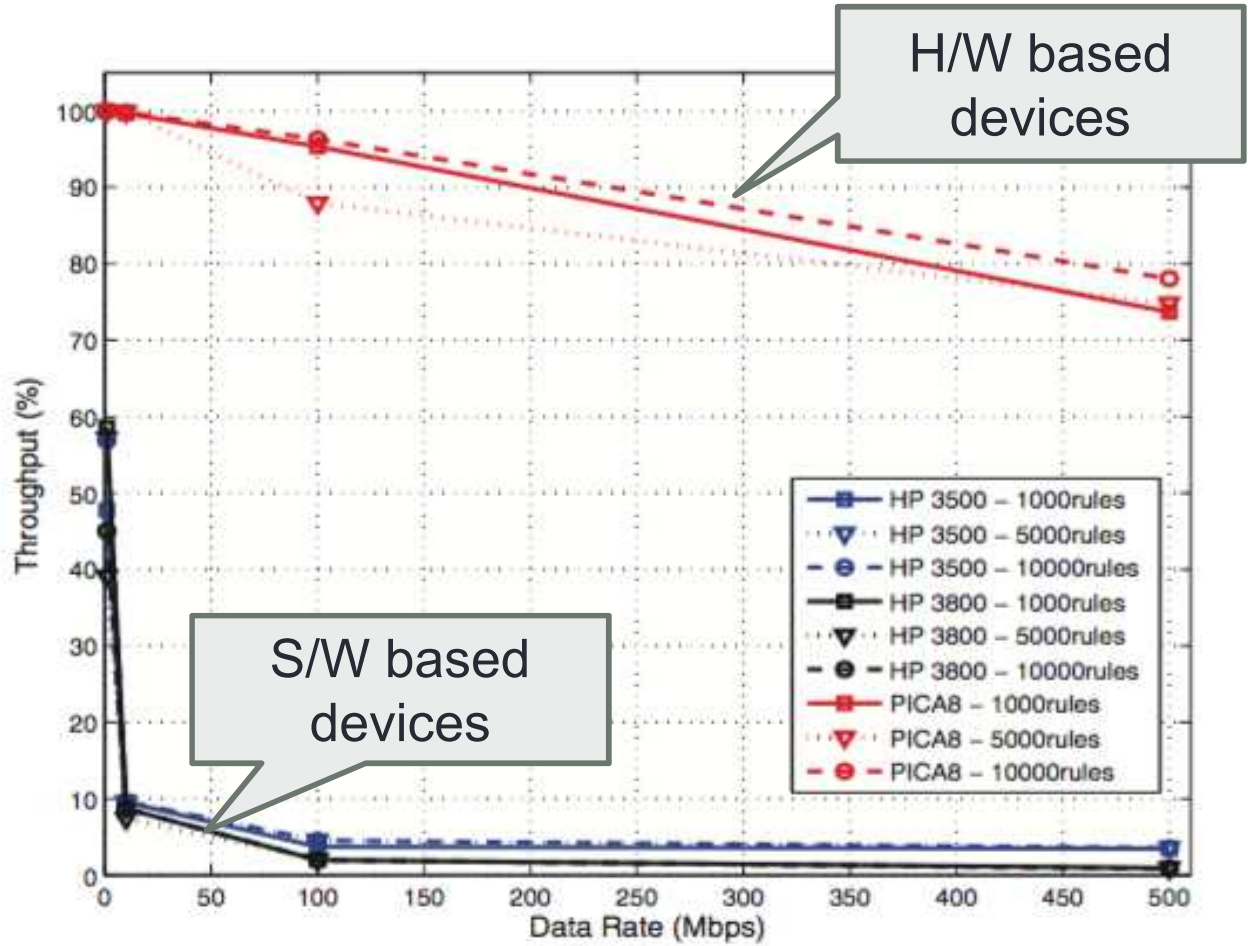
In-line Mode Security Applications

- No substantial overhead against payload delivery
- Feasible to deploy in-line mode security functions
  - Without new flows causing PACKET_IN events
  - With less than 1,000 matching rules
- Beneficial for specific critical services
  - e.g., web, mail, or other services

[redacted]

[redacted]

Passive Mode Security Applications

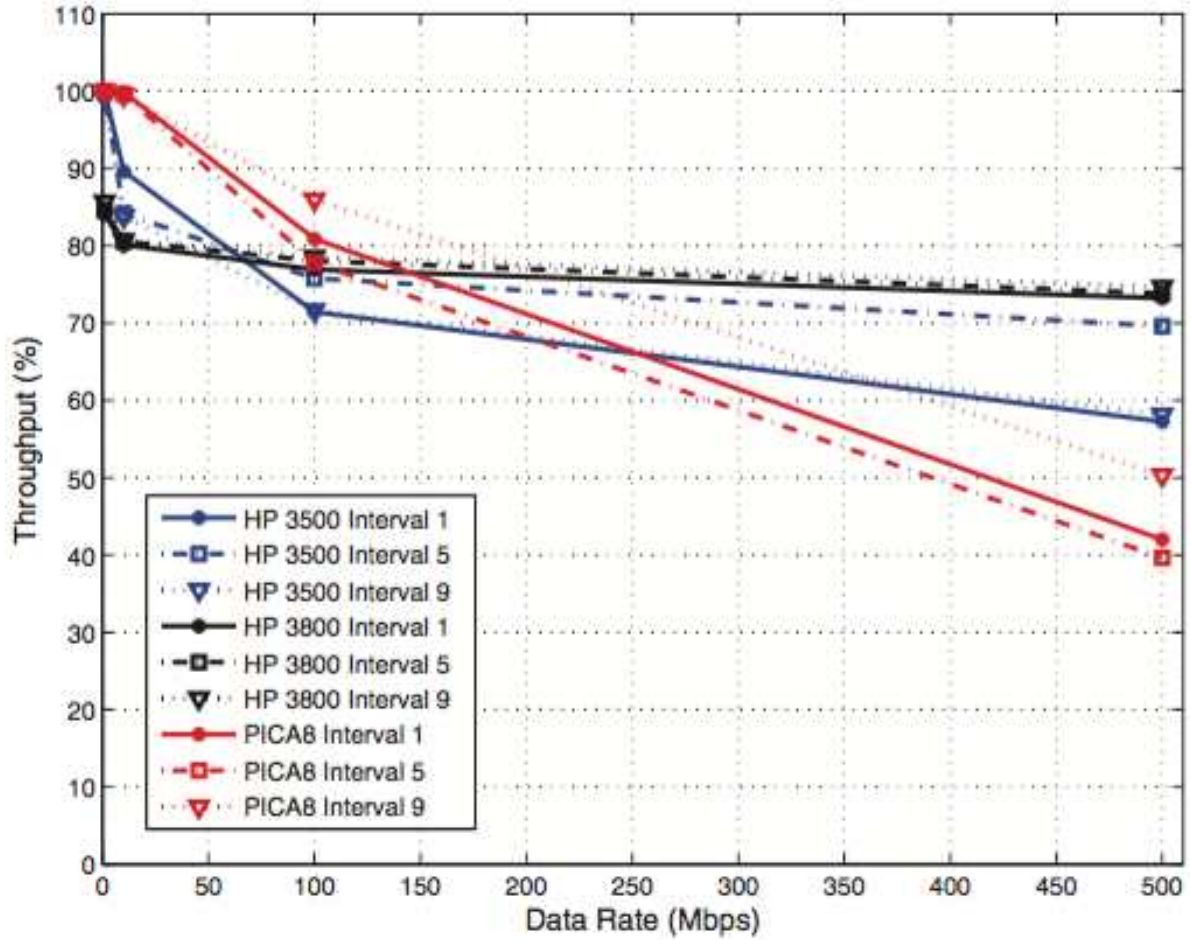


NIDS application

Passive Mode Security Applications

- Feasible to deploy them with H/W based devices
- Too much overhead with S/W based devices
  - Some devices manage SDN specialized functions in software

Network Anomaly Detection Applications



DDoS detection application

Network Anomaly Detection Applications

- No significant overhead to collect network information
- Different styles of network status information
  - Received packet counts of a flow or a range of flows
- Feasible to deploy them in real-world environments if they only work based on the given information

LESSONS

[redacted]

[redacted]

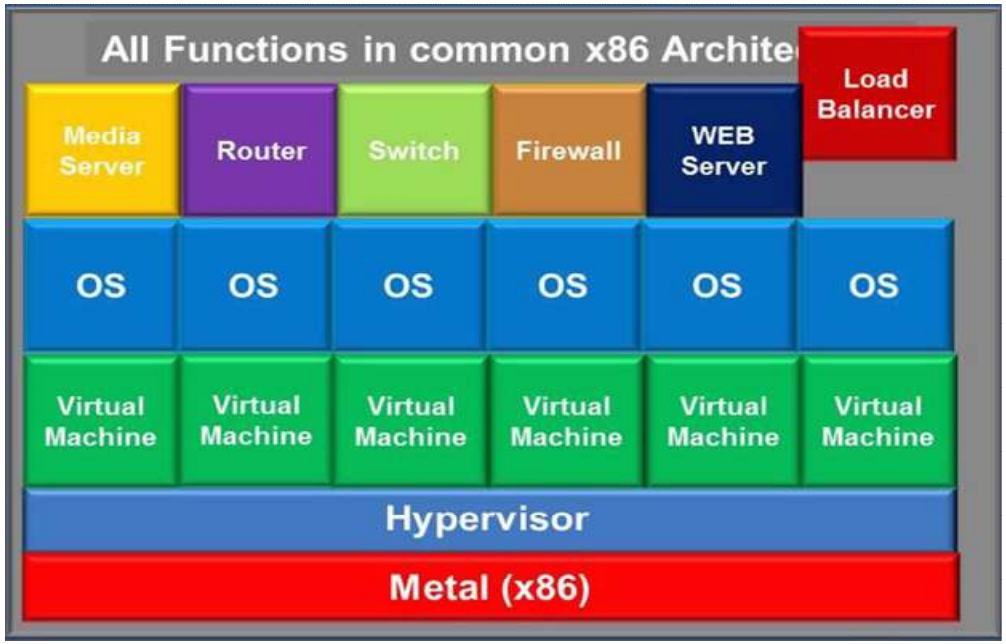
Promising but still Insufficient SDN

- Benefits
  - Flexible and dynamic network control
  - Collection of fine-grained network information in a network-wide view
  - Low cost (in terms of management and deployment)

- Drawbacks
  - Performance bottleneck
  - Insufficient network information (e.g., TCP sessions)
  - Different switch implementation

Network Function Virtualization (NFV)

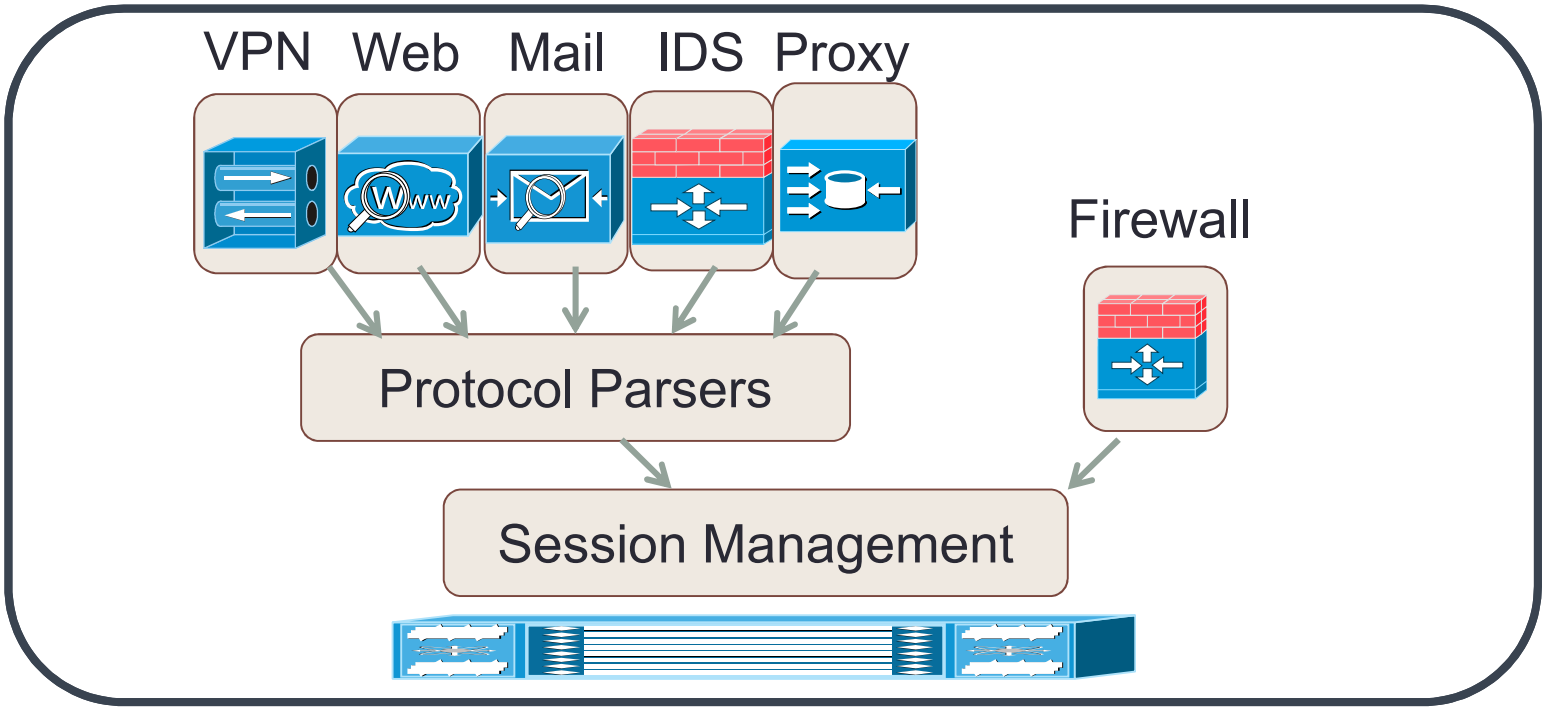
- Characteristics
  - Easy to create network functions
  - Easy to deploy and control (compared to a hardware box)
  - Low cost



From Spirent

Security Functions with NFV

- Intelligent brain (SDN) and powerful actionist (NFV)
  - Implement security functions as VM instances
  - Coordinate them with SDN functions



Conclusion

- Current security functions could be changed with SDN
- SDN is sometimes insufficient to support security functions
- NFV can make up the insufficiency of SDN
- SDN and NFV help to improve security functions

THANK YOU !

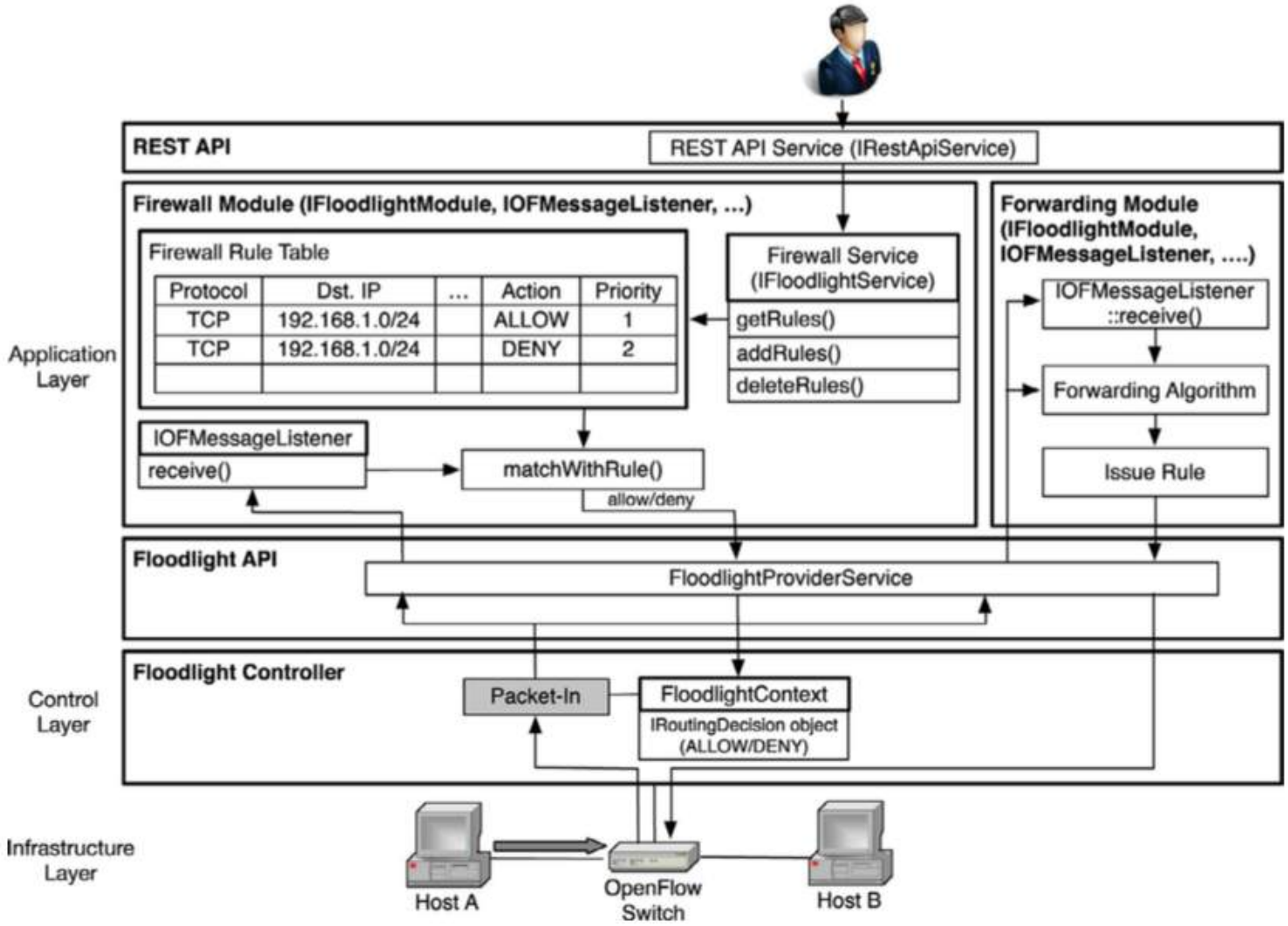
At ONS 2015

APPENDIX

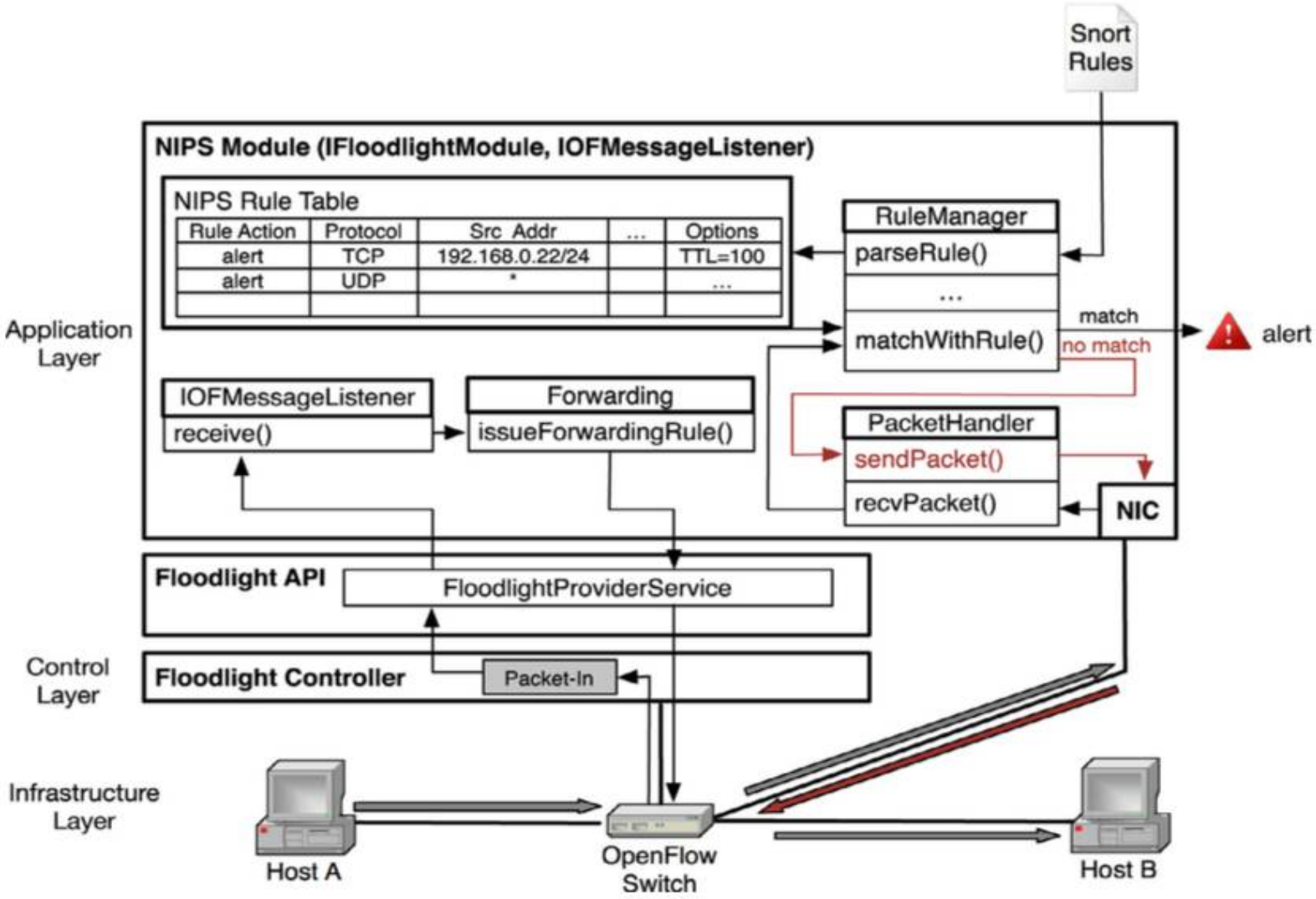
[redacted]

[redacted]

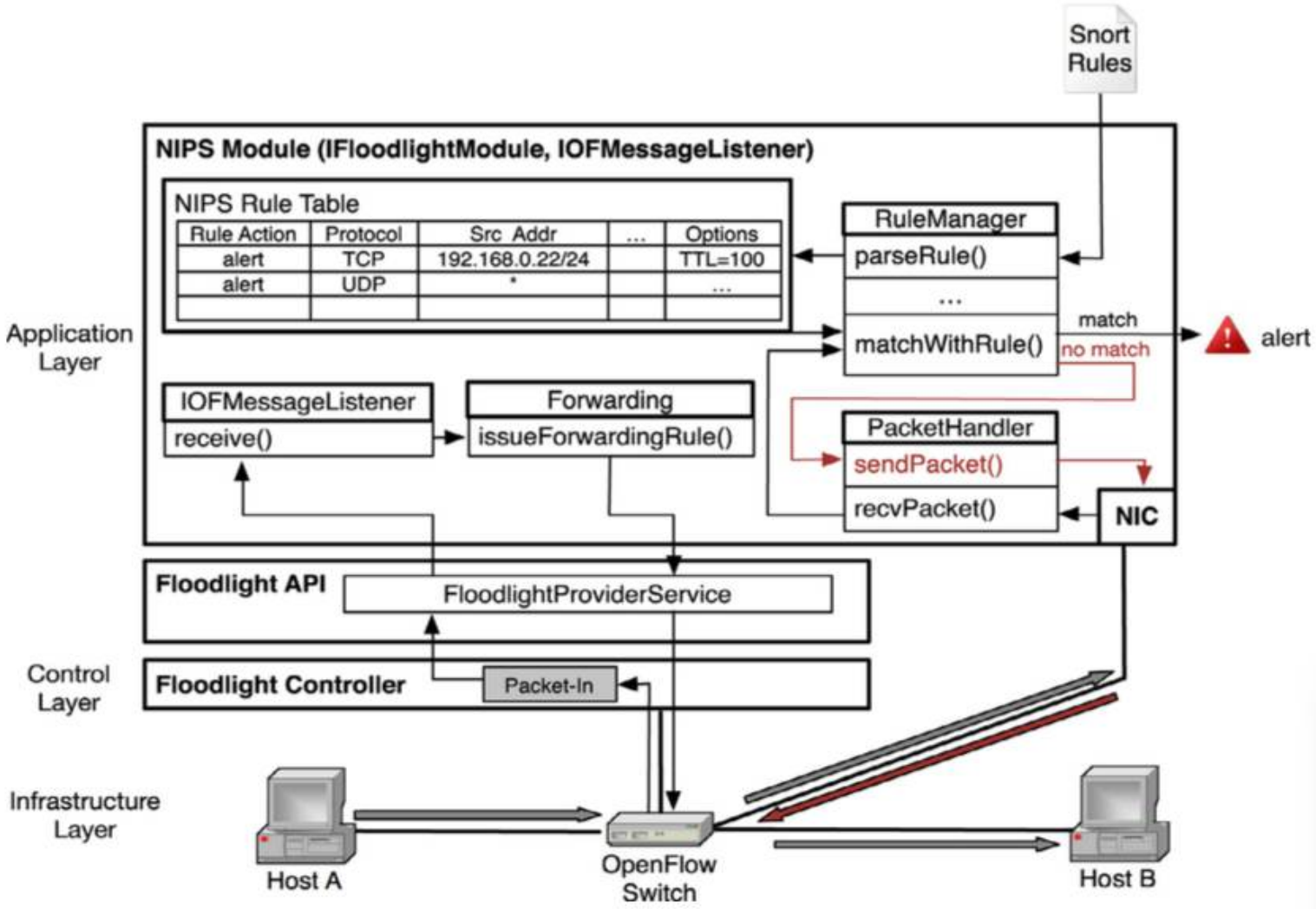
Firewall Application Implementation



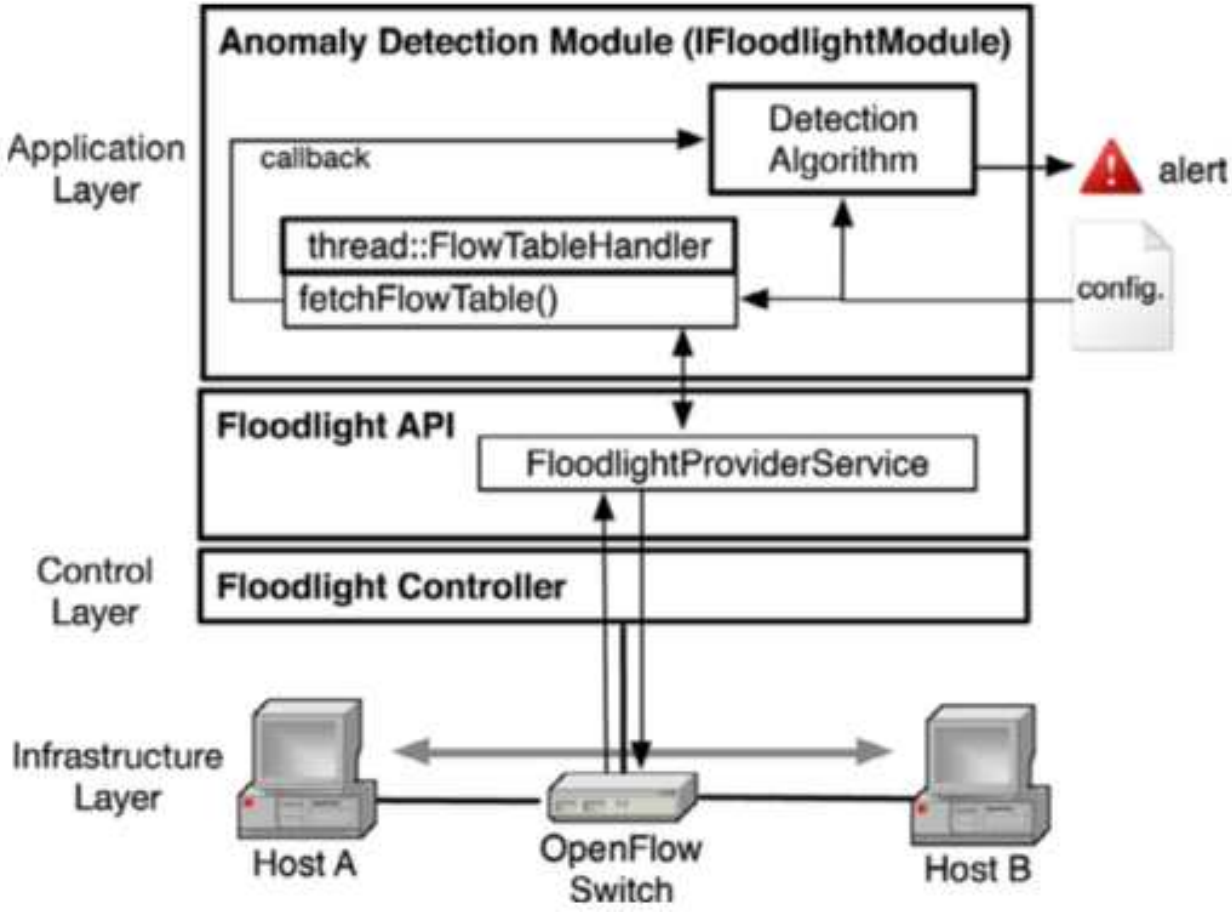
NIPS Application Implementation



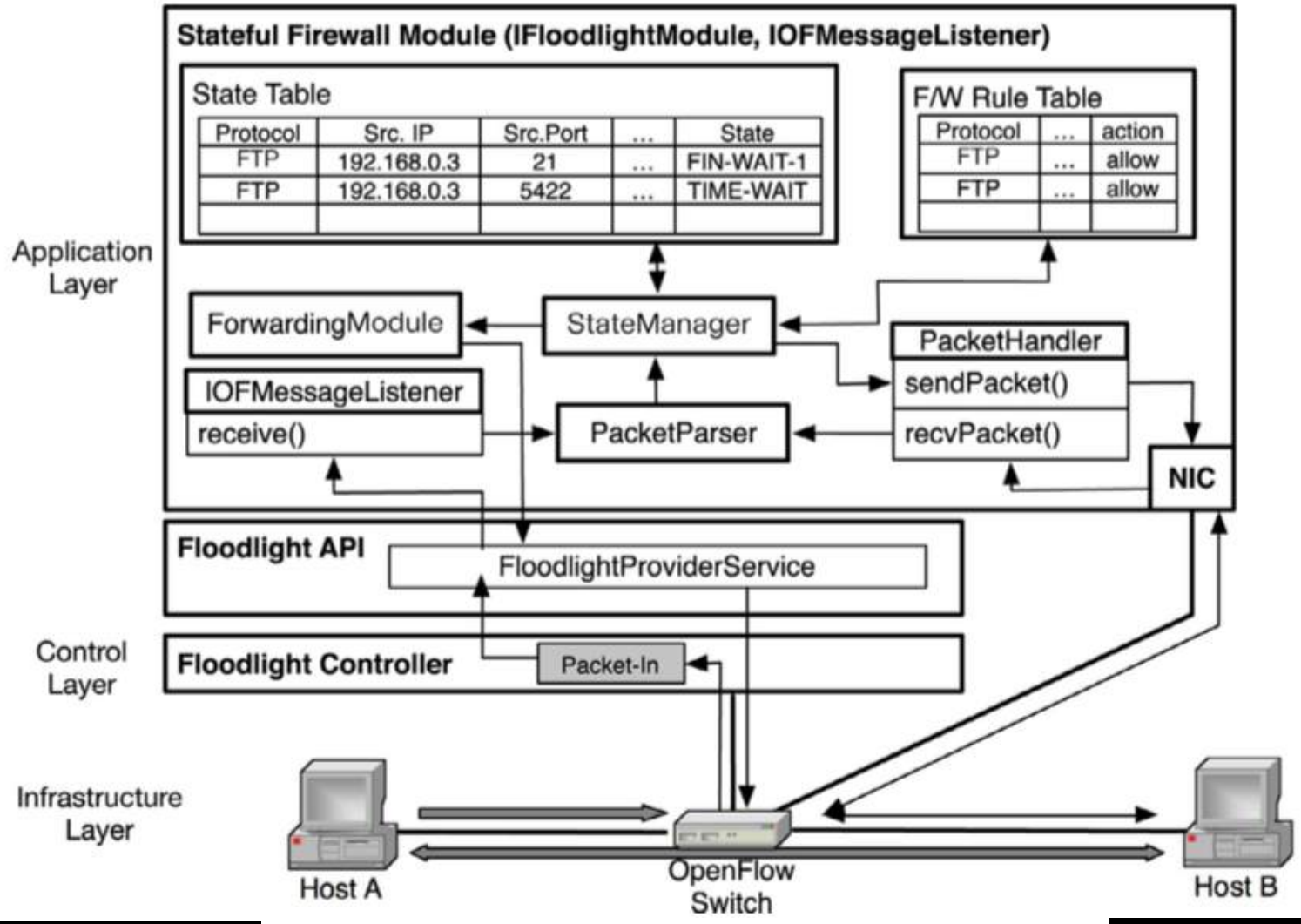
NIDS Application Implementation



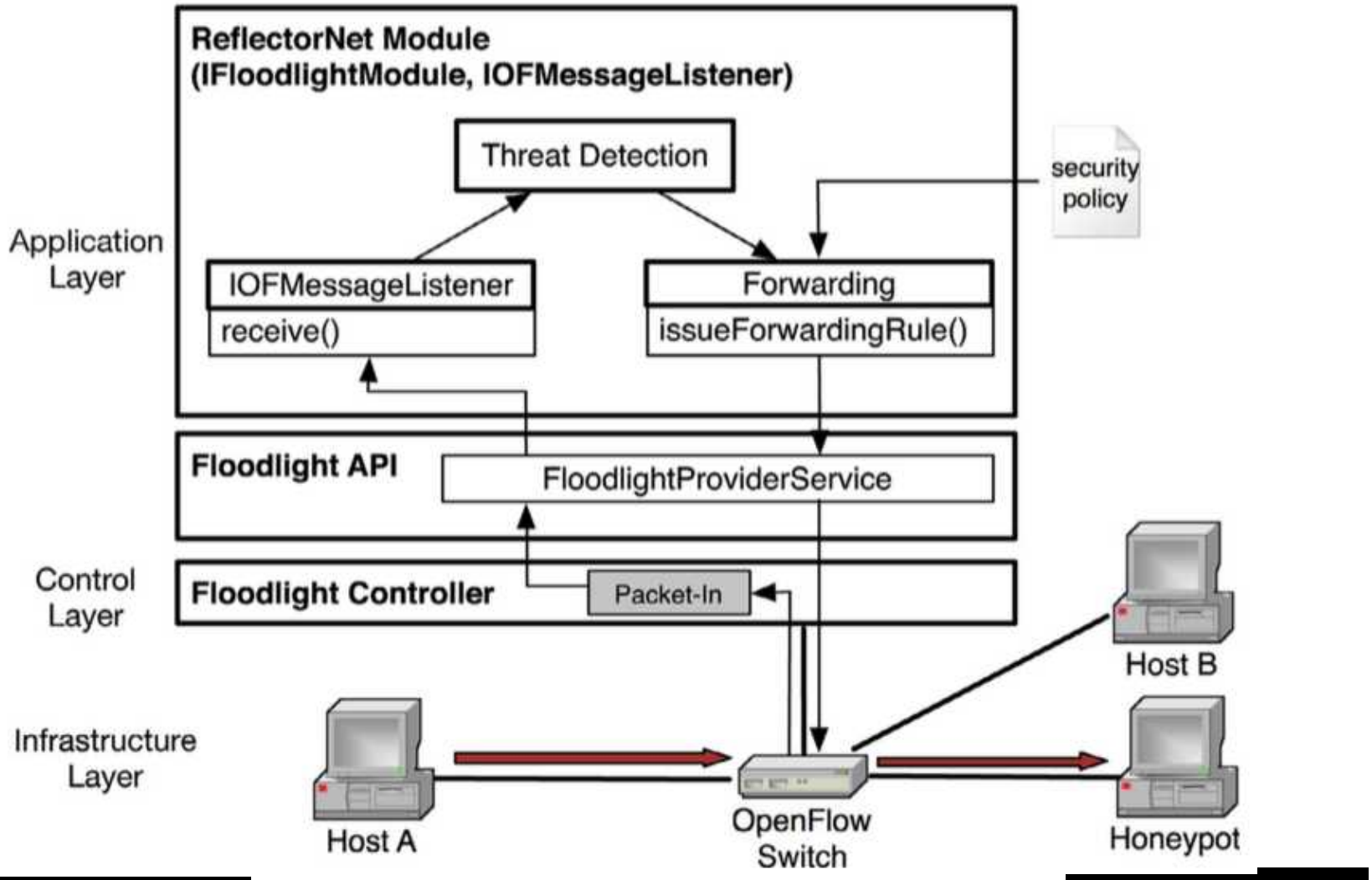
Anomaly Detection Application Implementation



Stateful F/W Application Implementation

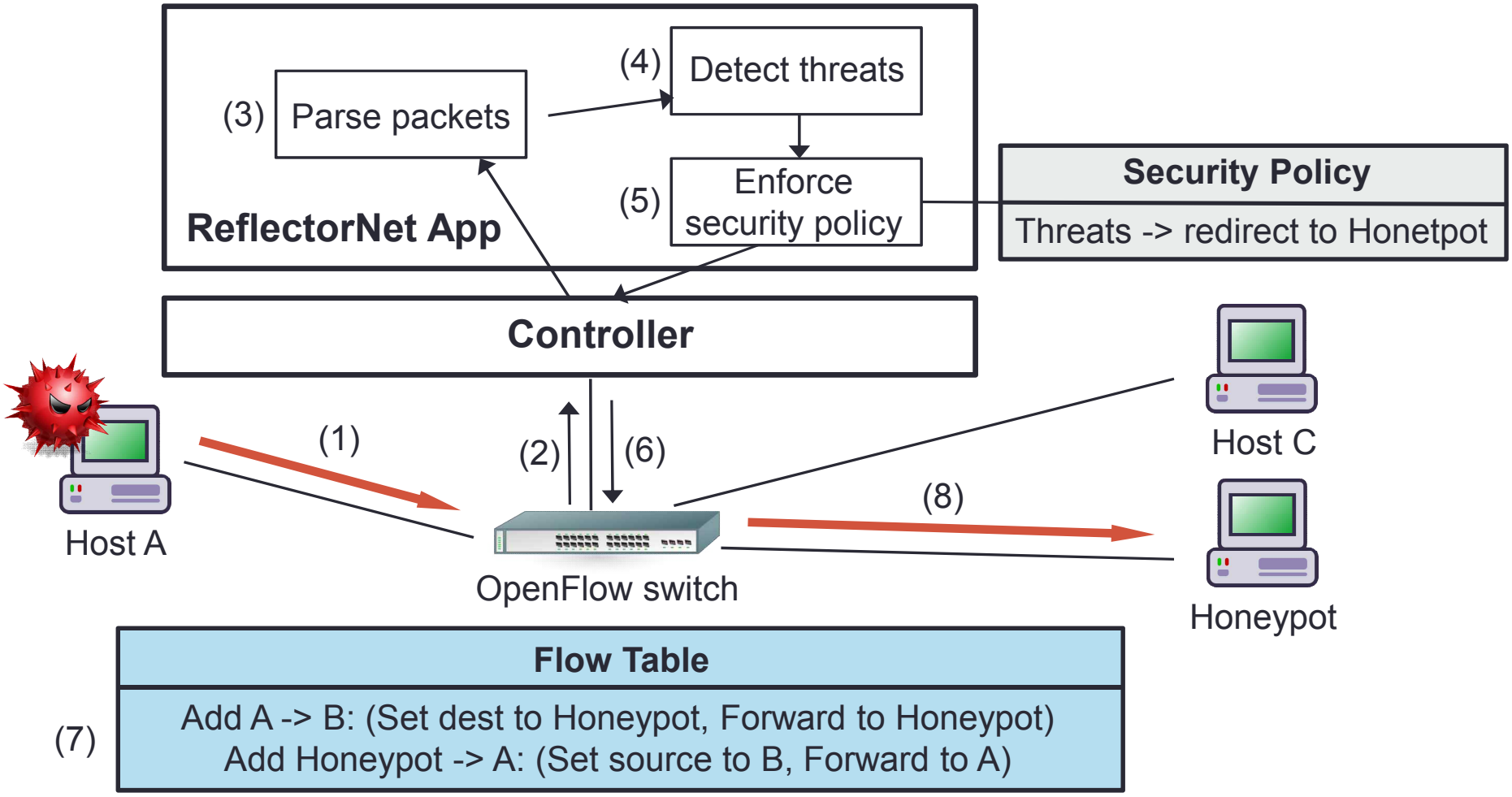


ReflectorNet Application Implementation



Advanced Network Security Applications

- Reflector network



Experimental Setup

- Physical SDN testbeds
  - A controller machine, three switches, and three hosts

	HP 3500yl	HP 3800	Pica8 P-3290
Switch fabric capacity	101.8 Gbps	88 Gbps	176 Gbps
Forwarding speed	75.7 Mpps	65.4 Mpps	132 Mpps
Latency	3.4 us	2.8 us	1 us
Routing table size	10,000	10,000	12,000
MAC table size	64,000	65,5000	32,000

OpenFlow-enabled Switch Specifications

Experimental Setup

- Physical SDN testbeds
  - A controller machine, three switches, and three hosts

Type	NIC	CPU	RAM	OS
Controller	1 Gbps x 5	i5-4570	16 GB	Ubuntu 12.04 64 bit
Host 1	1 Gbps	i7-2640 M	8 GB	Ubuntu 12.04 64 bit
Host 2	1 Gbps	i5-2450 M	8 GB	Windows 7 64 bit
Host 3	100 Mbps	Atom N550	2 GB	Ubuntu 13.10 64 bit

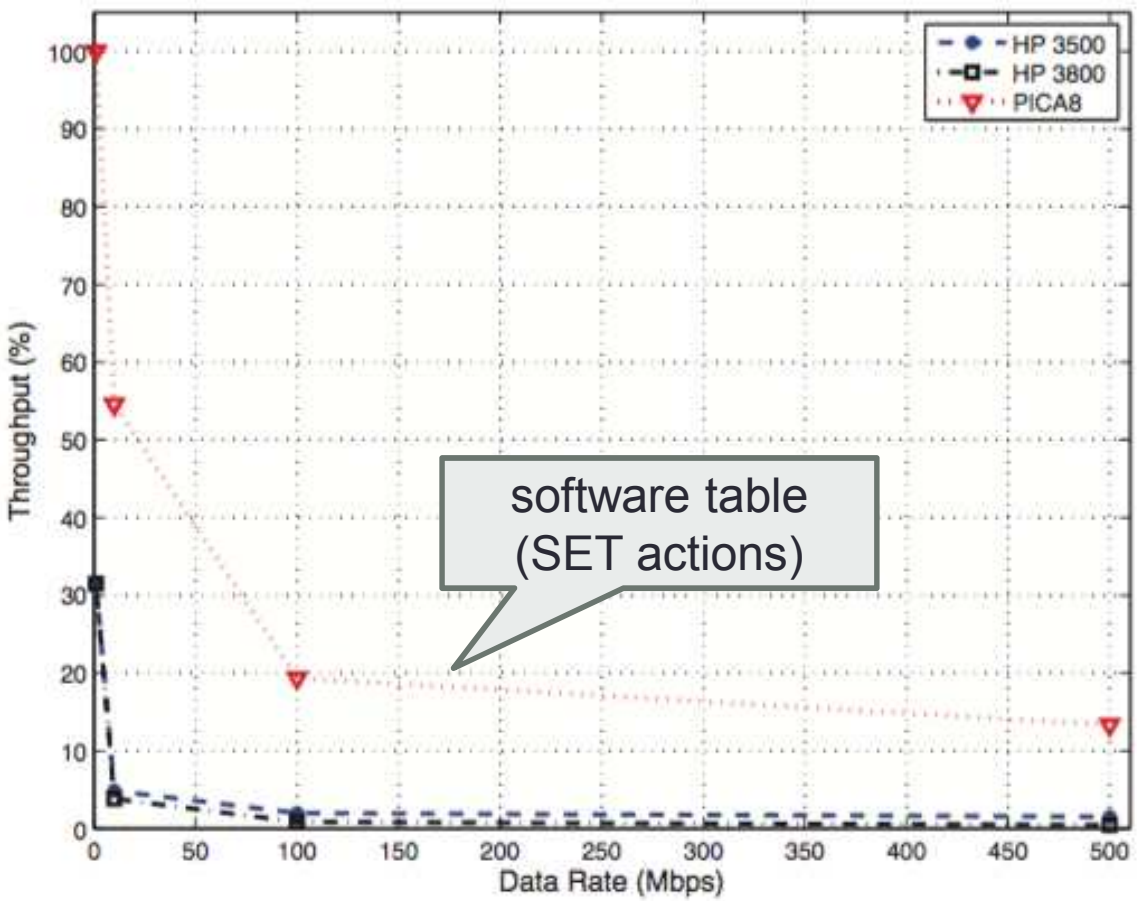
Machine Specifications

Advanced Network Security Applications

- Why ReflectorNet works in SDN
  - Ease implementation of such advanced network security functions
  - Cost effectiveness (complicated security functions with less effort)

- Why ReflectorNet does not works in SDN
  - No proof against the availability of SDN-based security functions yet
  - Need for more consideration to support security functions
    - Many required features are still missing

Advanced Network Security Applications



ReflectorNet application

Advanced Network Security Applications

- Modification of packet headers is the key features of SDN
  - This feature only works in software so far
- Hard to realize them in real cases without H/W support
  - Due to performance issues