# Using SDN and NFV to Realize a Scalable and Resilient Omni-Present Firewall

**Nicholas Gray**

*comnet.informatik.uni-wuerzburg.de*

# SarDiNe Research Project

- **Goal:** Improve the security in enterprise and government networks based on SDN/NFV

sardine-project.org

- Partners

Julius-Maximilians-UNIVERSITÄT WÜRZBURG

TUM

genua Ein Unternehmen der Bundesdruckerei

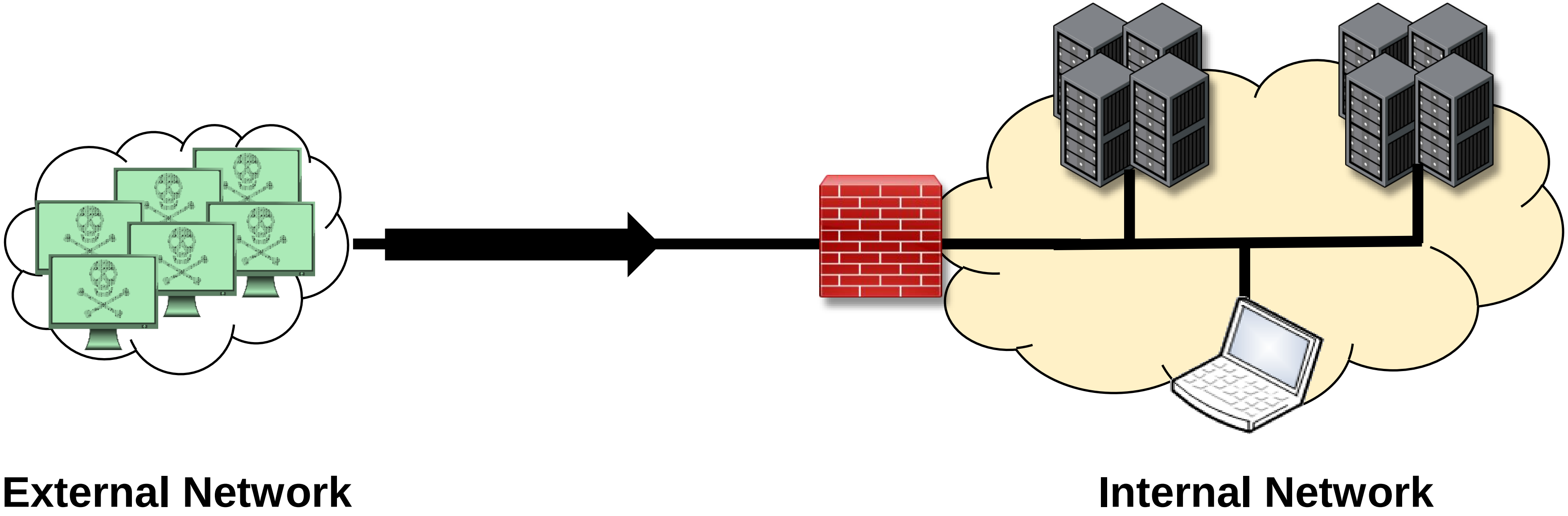
infosim®

- Associated Partners

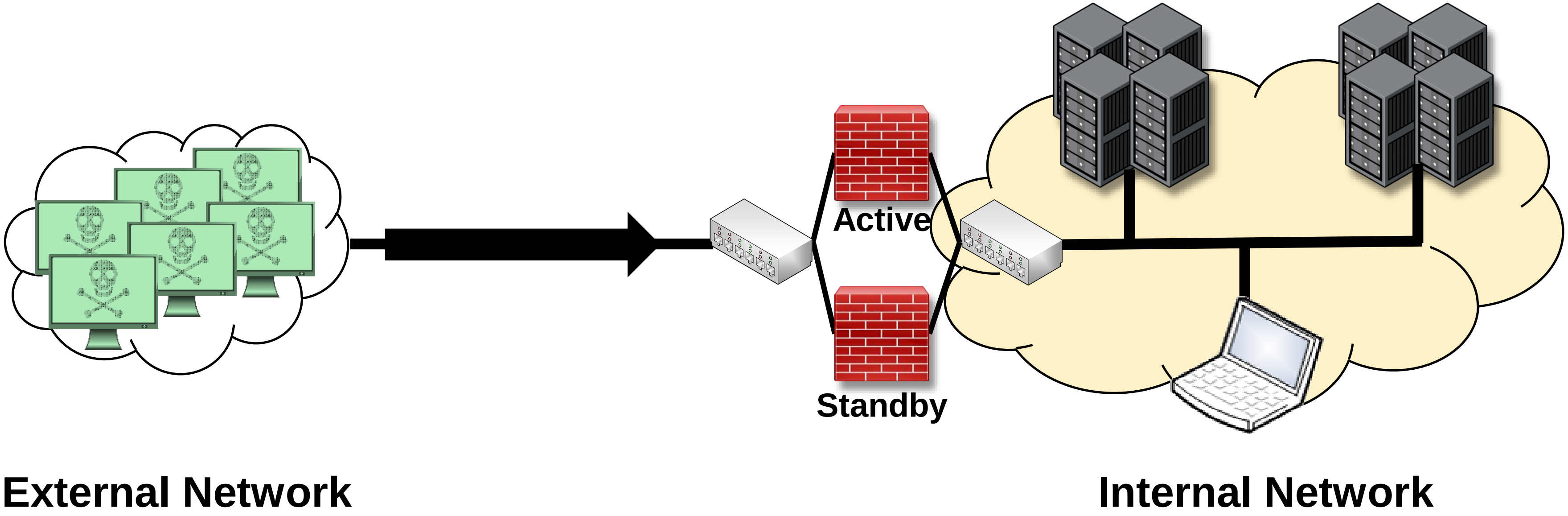
Bundesamt
für Sicherheit in der
Informationstechnik

Informations
Technik
Zentrum Bund

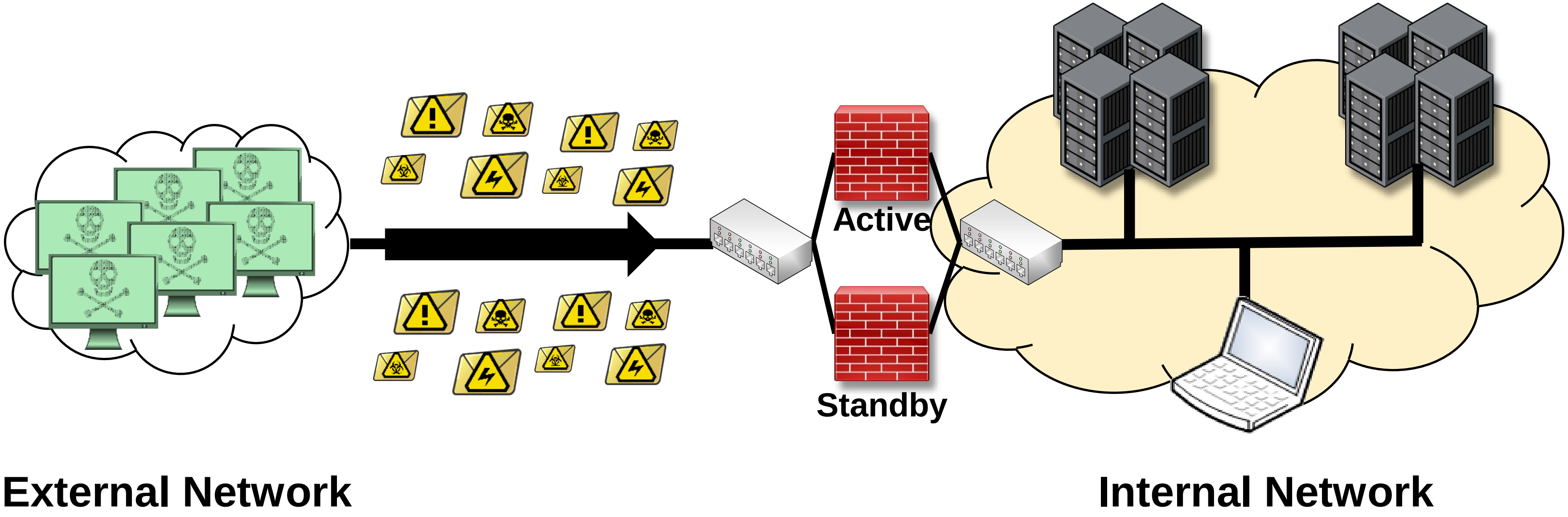
# Motivation



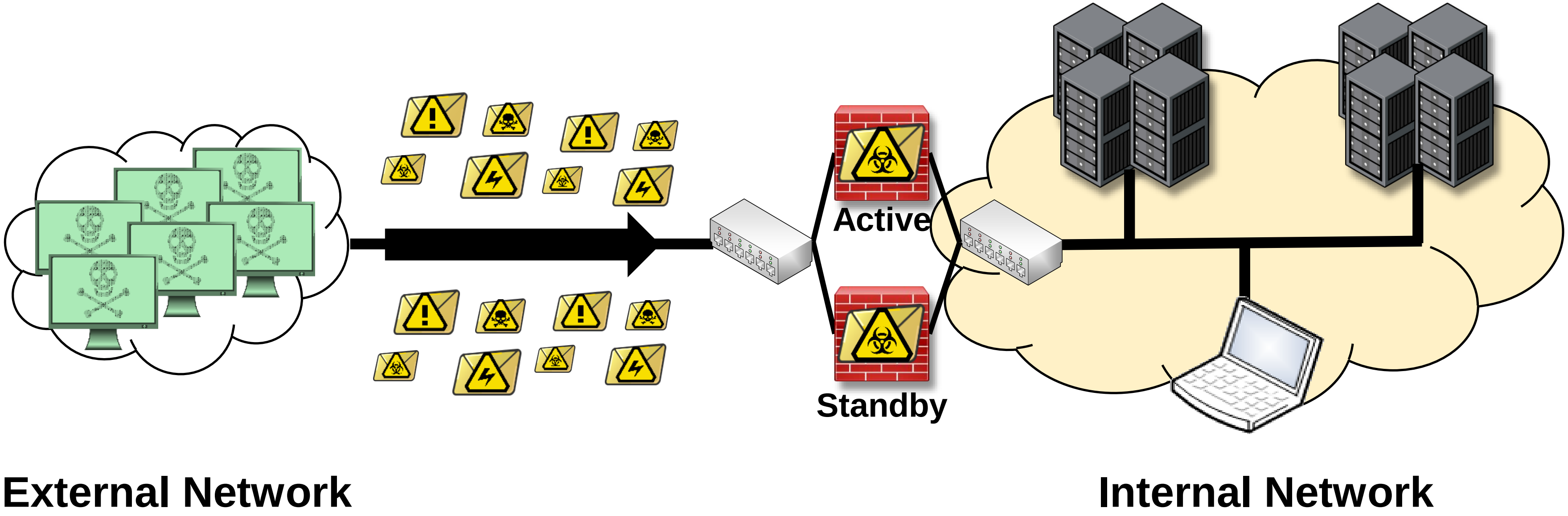
# Motivation



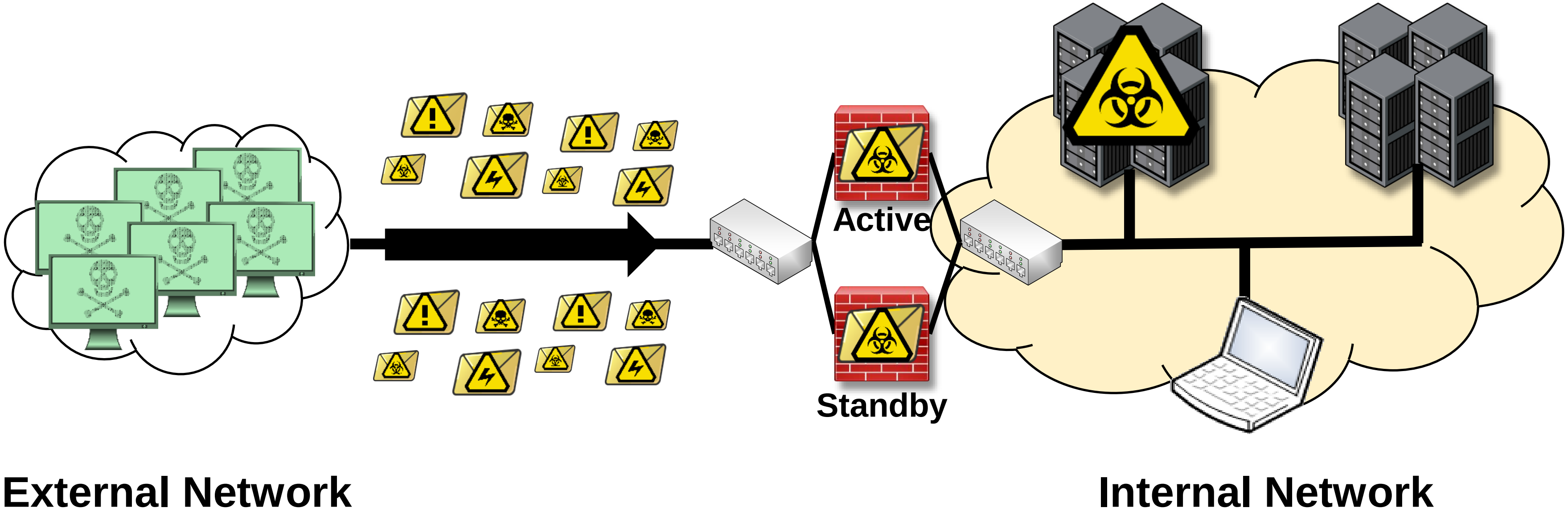
# Motivation



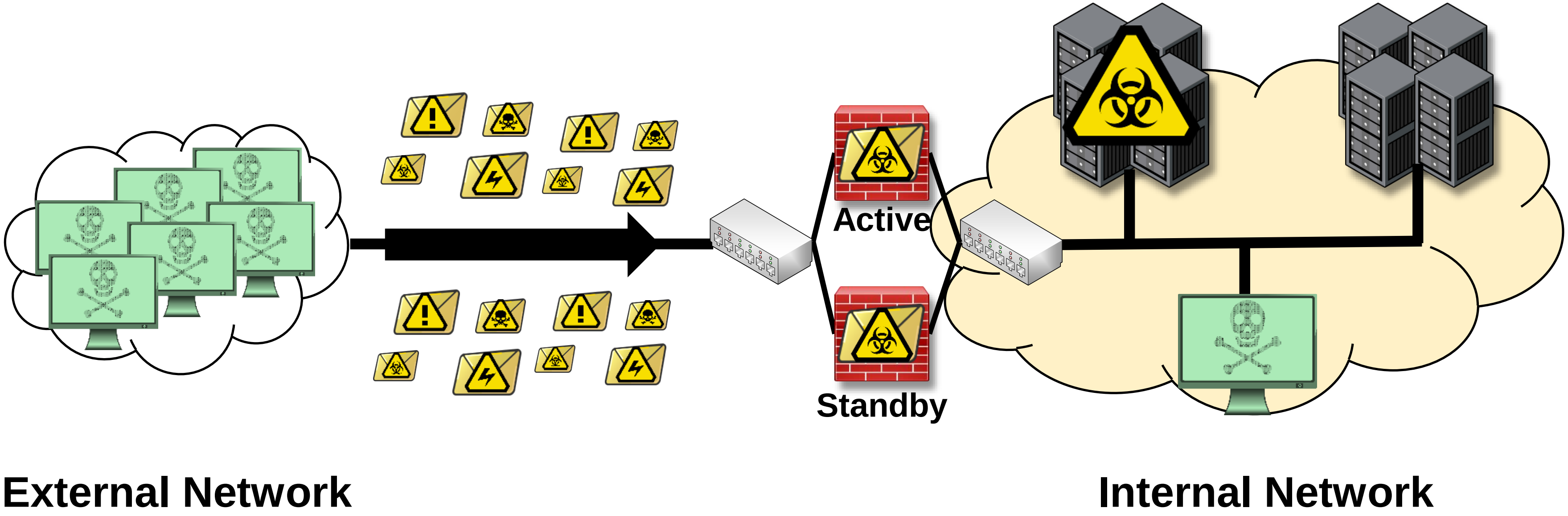
# Motivation



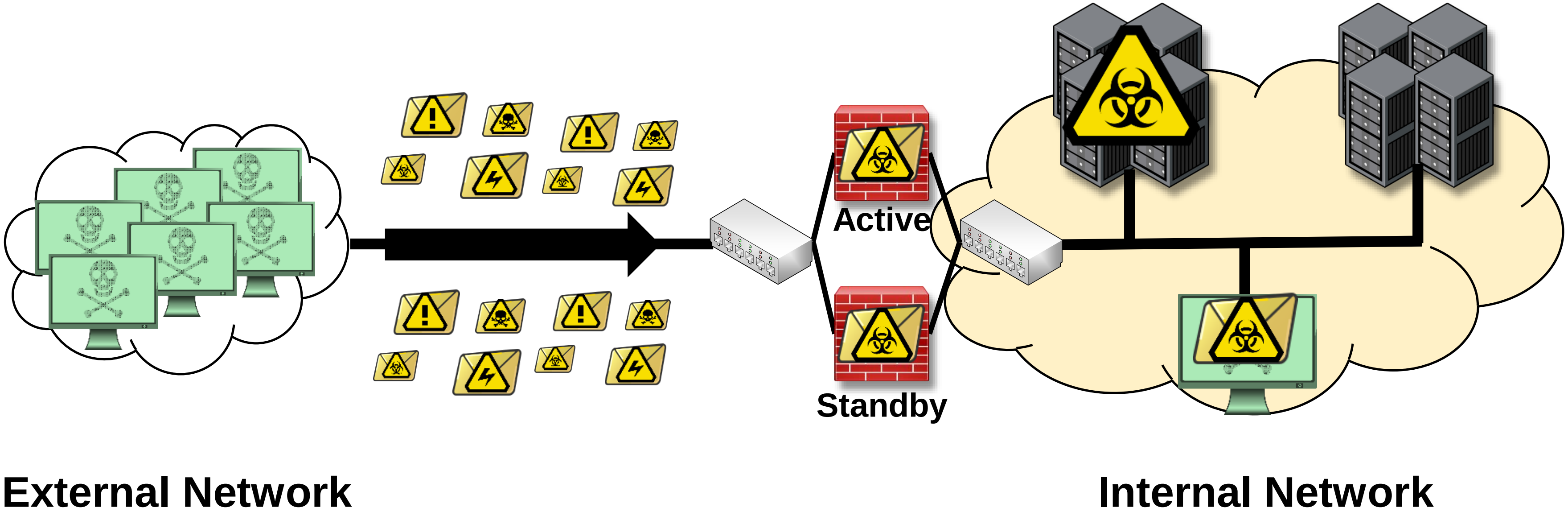
# Motivation



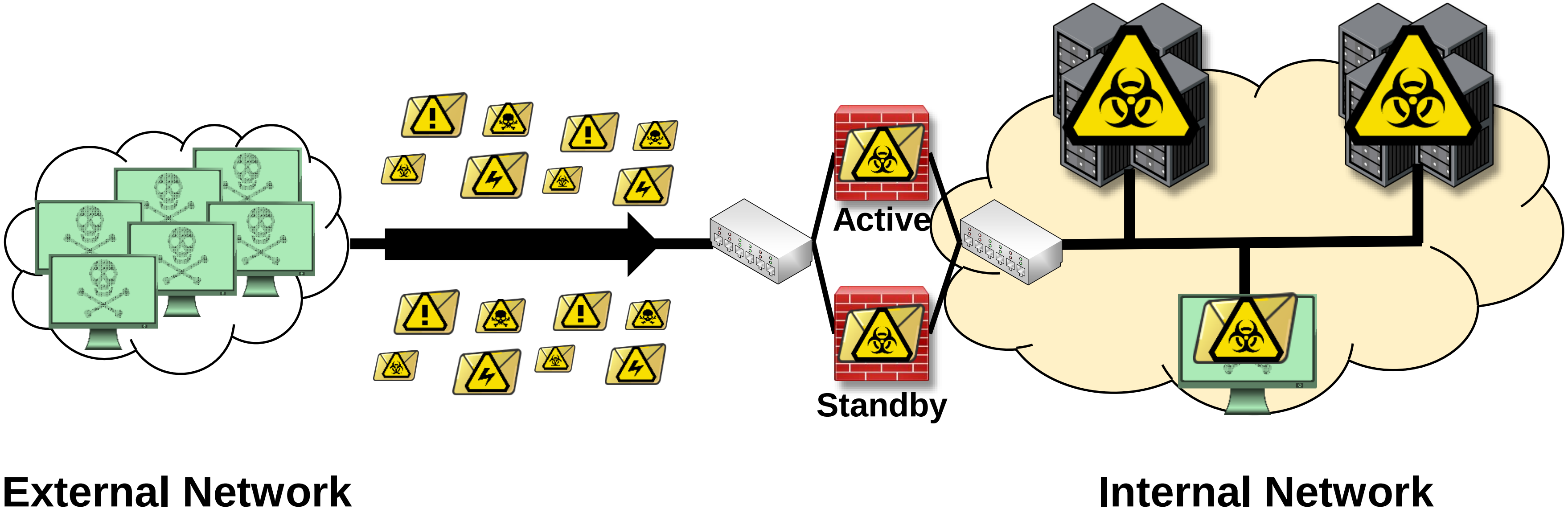
# Motivation



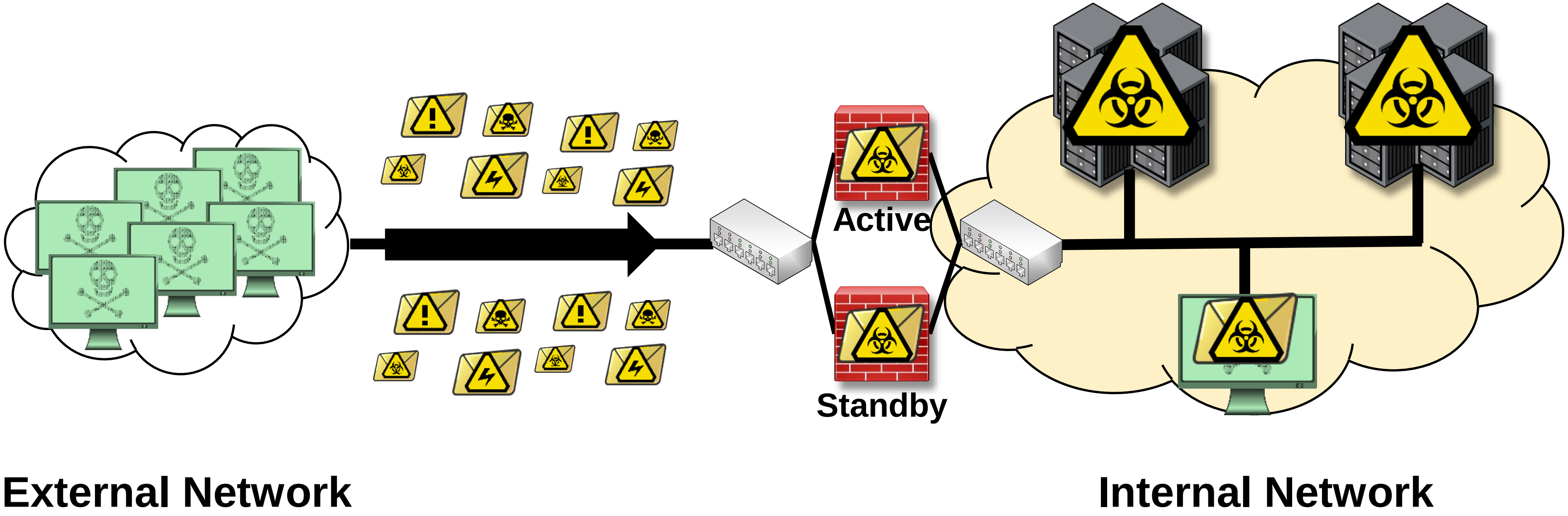
# Motivation



# Motivation

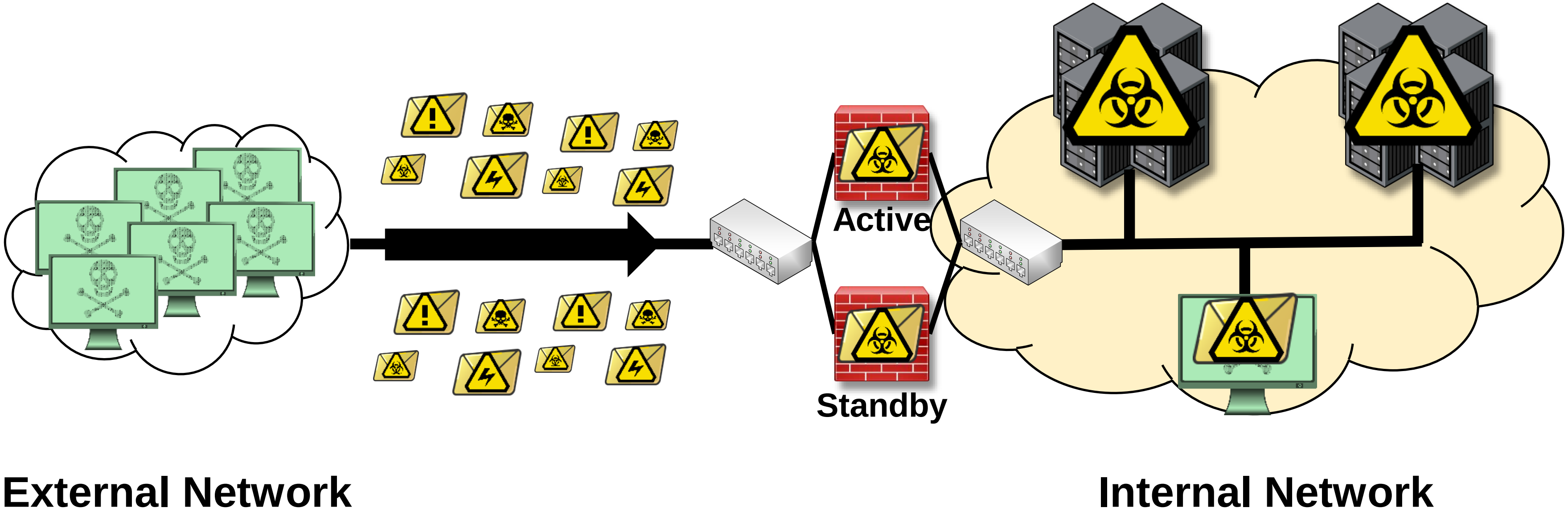


# Motivation



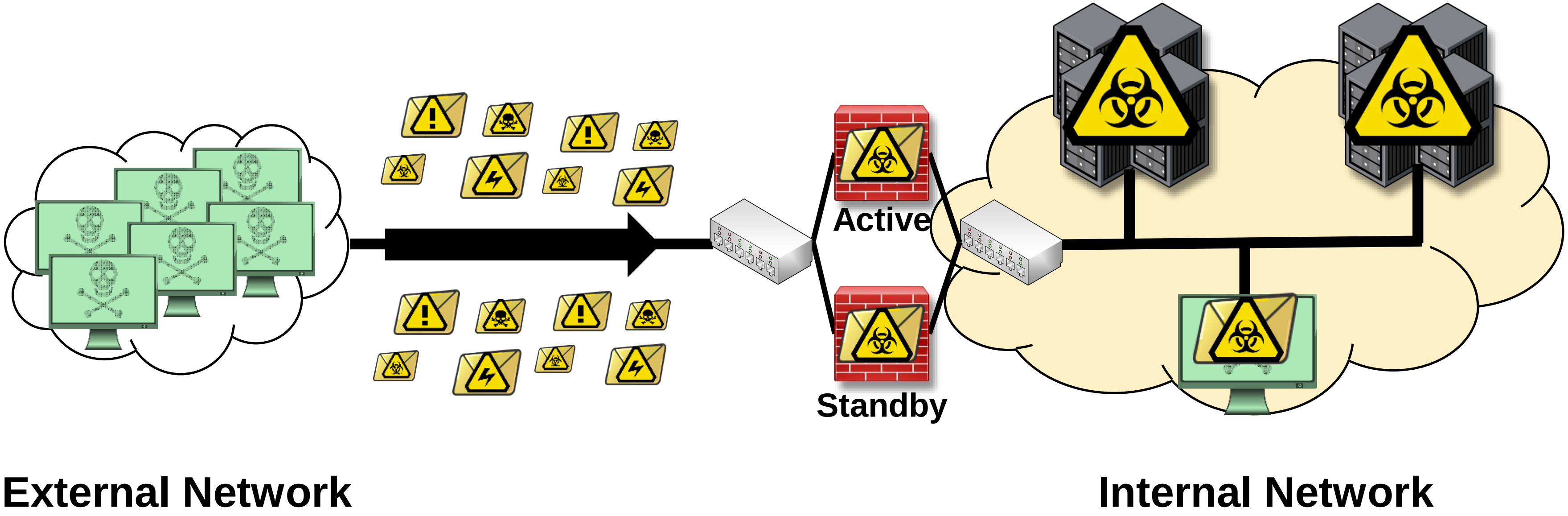
- ✗ Expensive hot standby

# Motivation



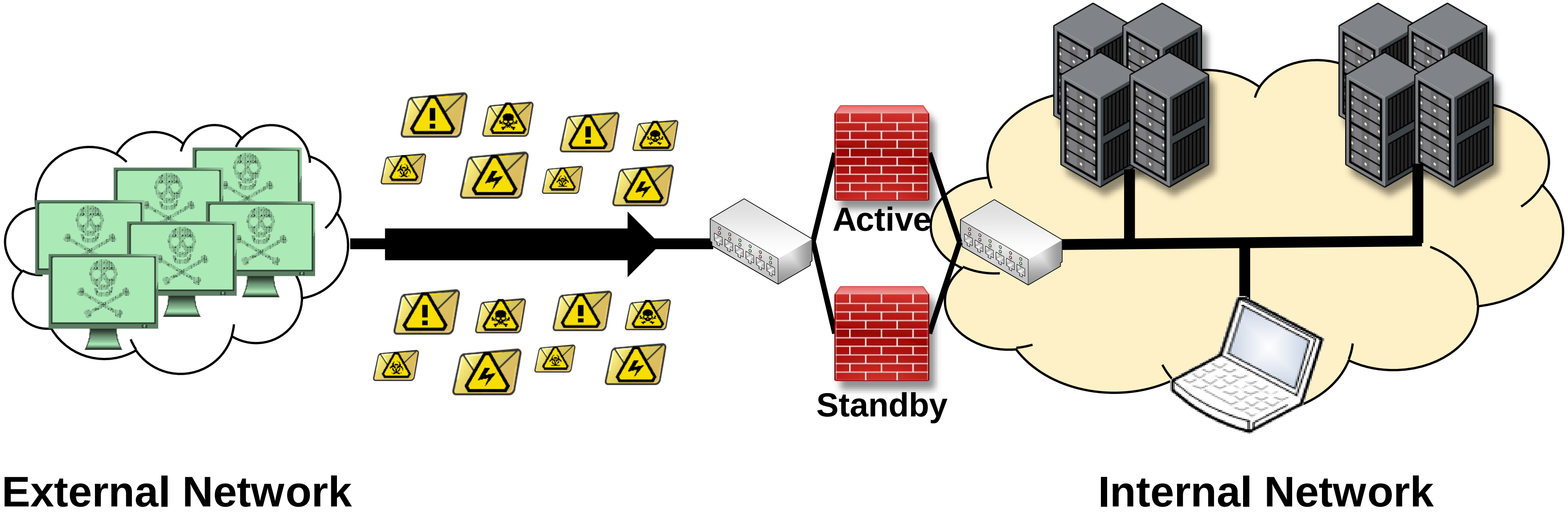
- ✗ Expensive hot standby
- ✗ Little internal defenses

# Motivation

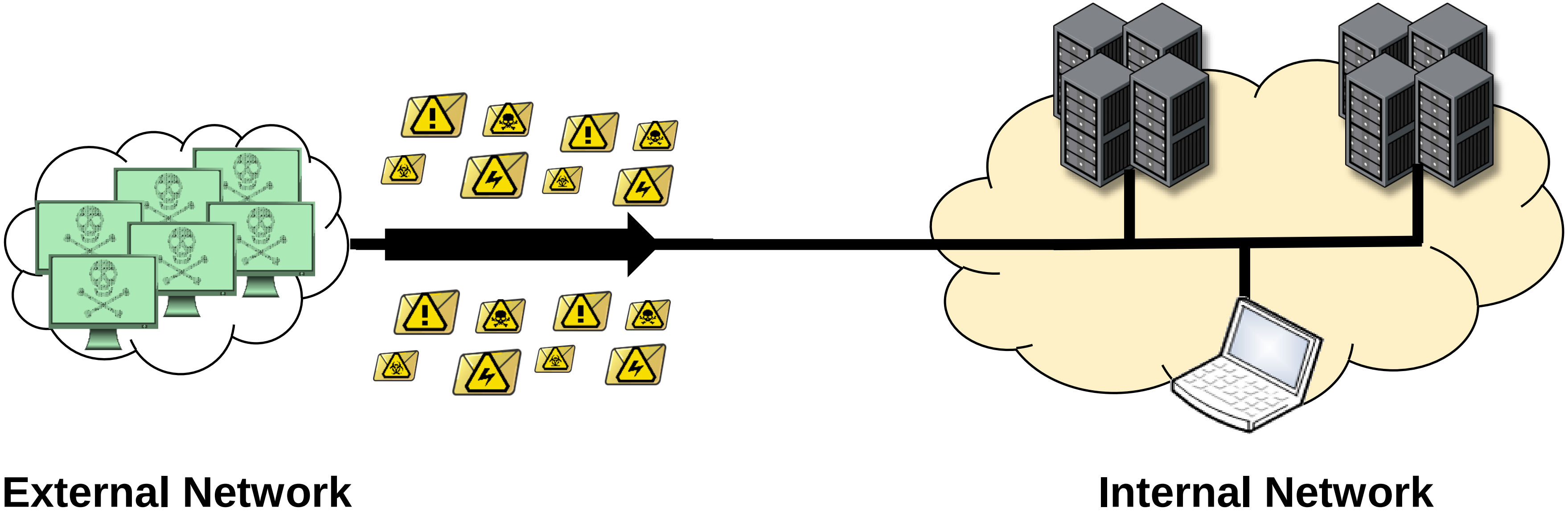


- ✗ Expensive hot standby
- ✗ Little internal defenses
- ✗ Limited scalability

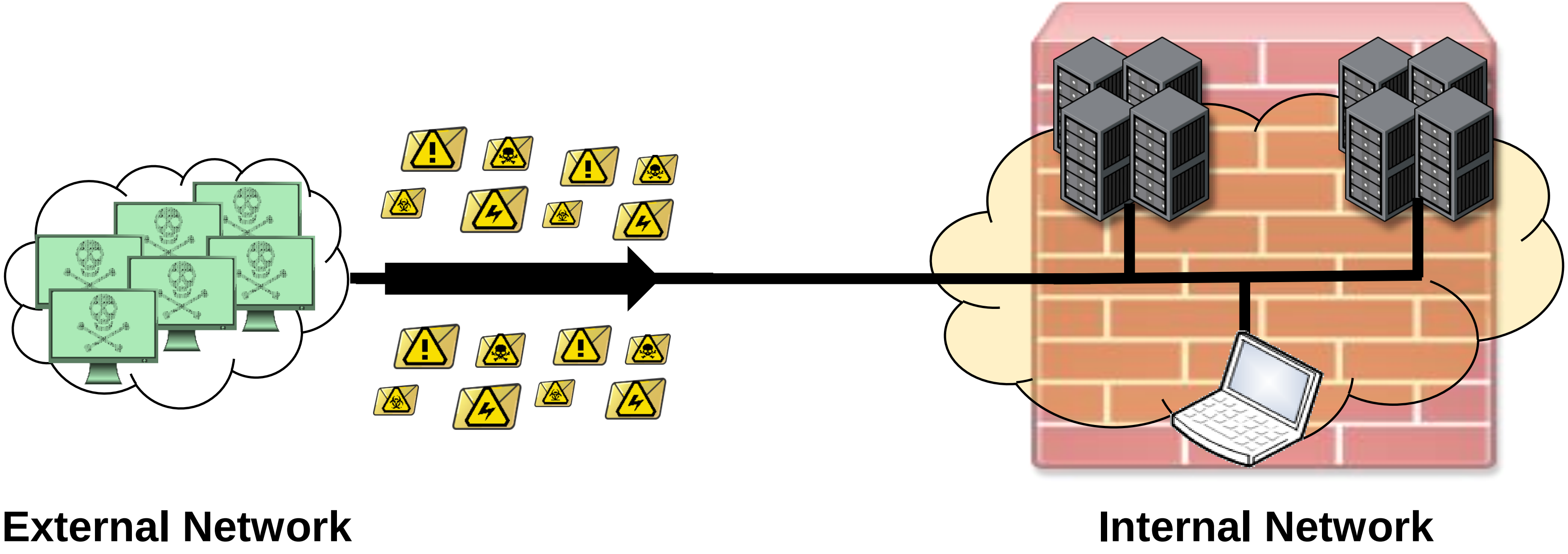
# Motivation



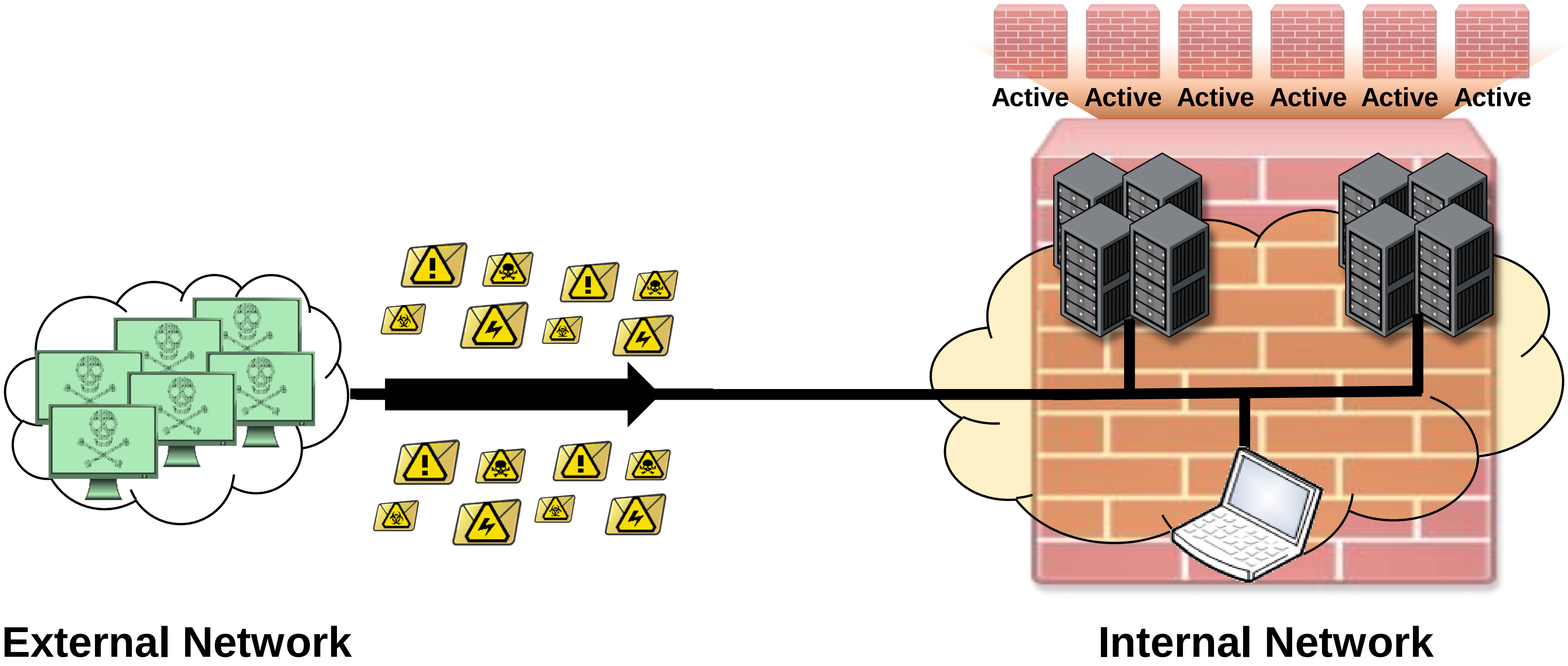
# Motivation



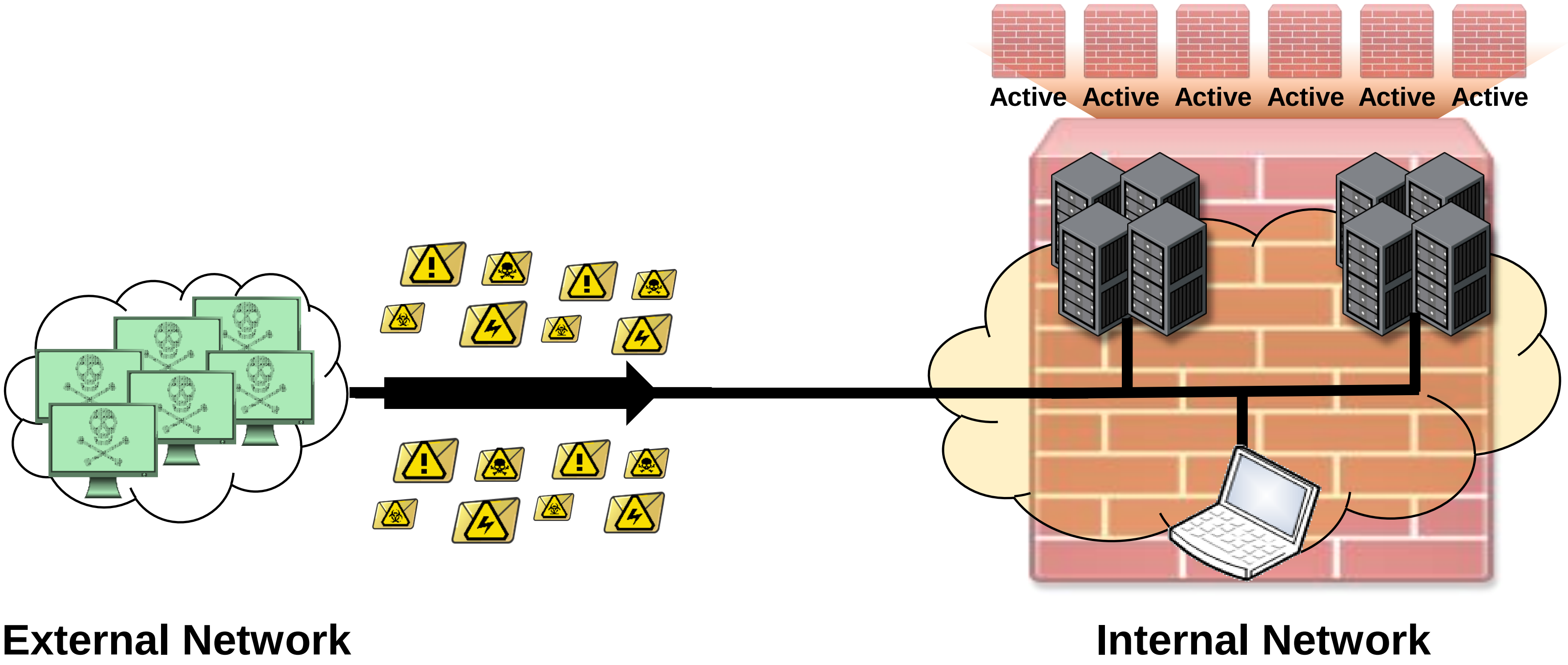
# Motivation



# Motivation

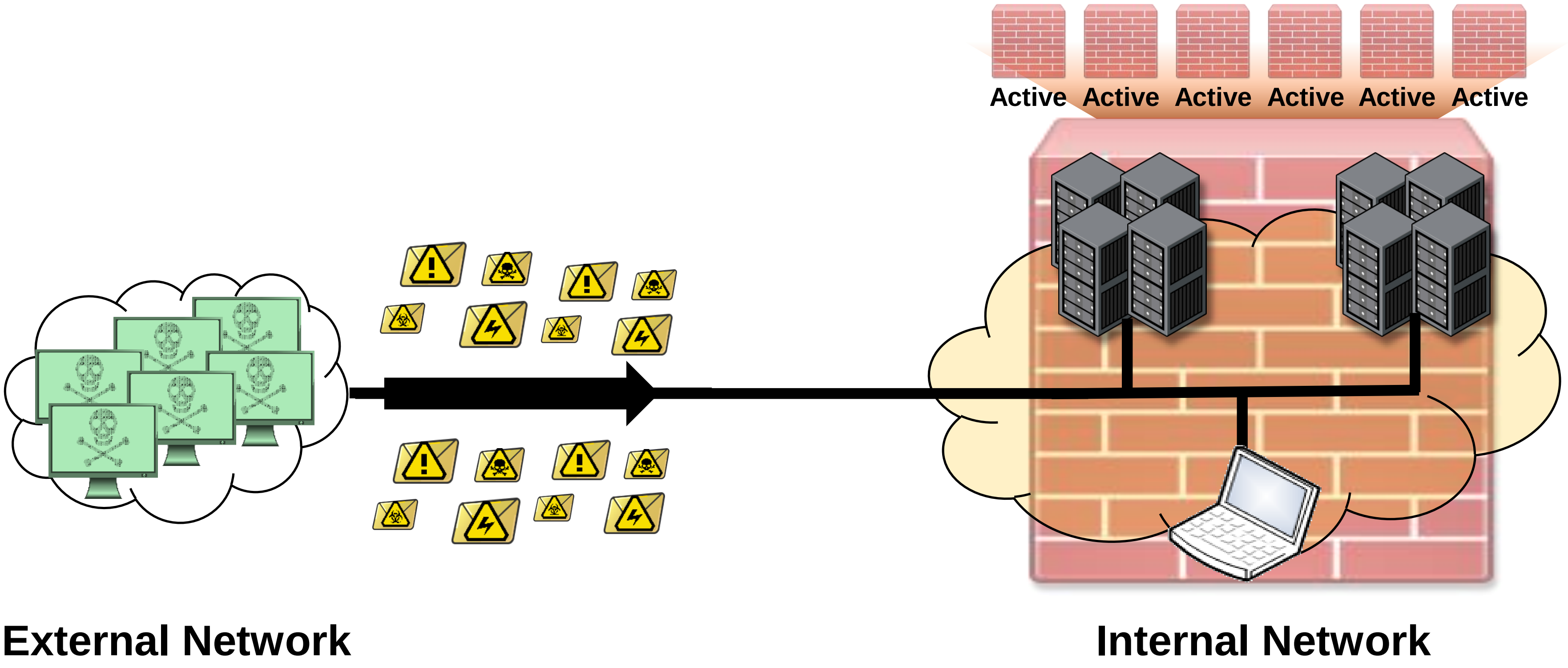

Active
Active
Active
Active
Active
Active
External Network
Internal Network

# Motivation



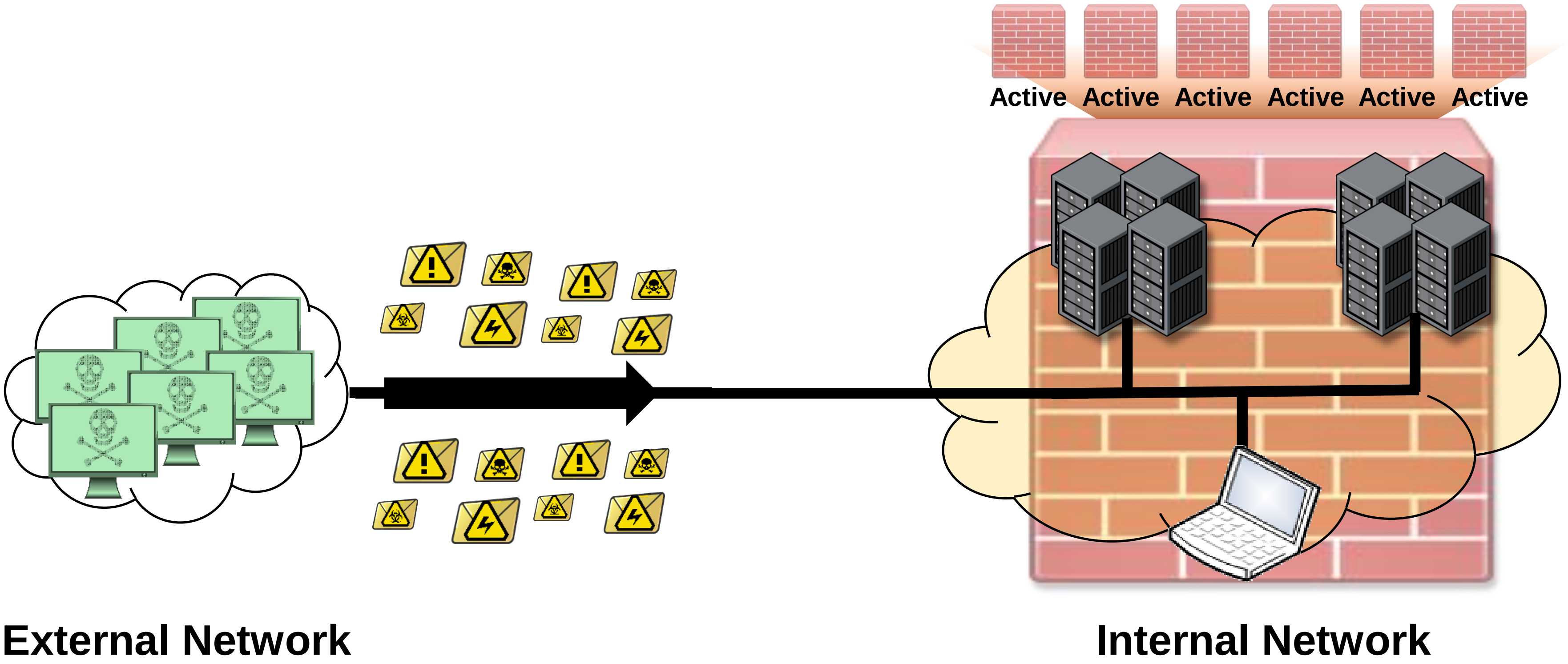
✓ Omni-present protection

# Motivation



- ✓ Omni-present protection
- ✓ Scalable and resilient security solution

# Motivation



✓ Omni-present protection

✓ Scalable and resilient security solution

→ SDN and NFV provide the necessary means

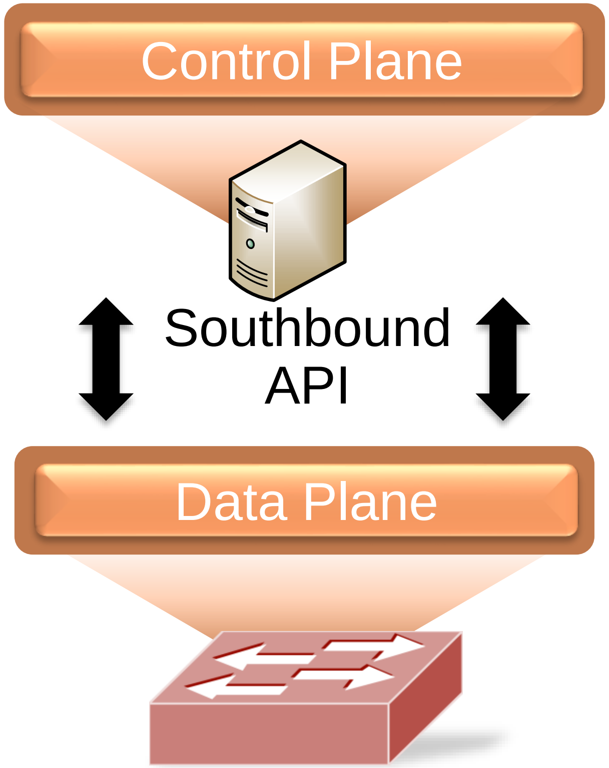
# Agenda

- Motivation
- Background
  - Software-defined Networking (SDN)
  - Network Function Virtualization (NFV)
- Omni-present SDN Firewall
  - Fine-grained access control
  - Scalable & resilient stateful firewalling
  - Firewall offloading
  - Demo
- Conclusion

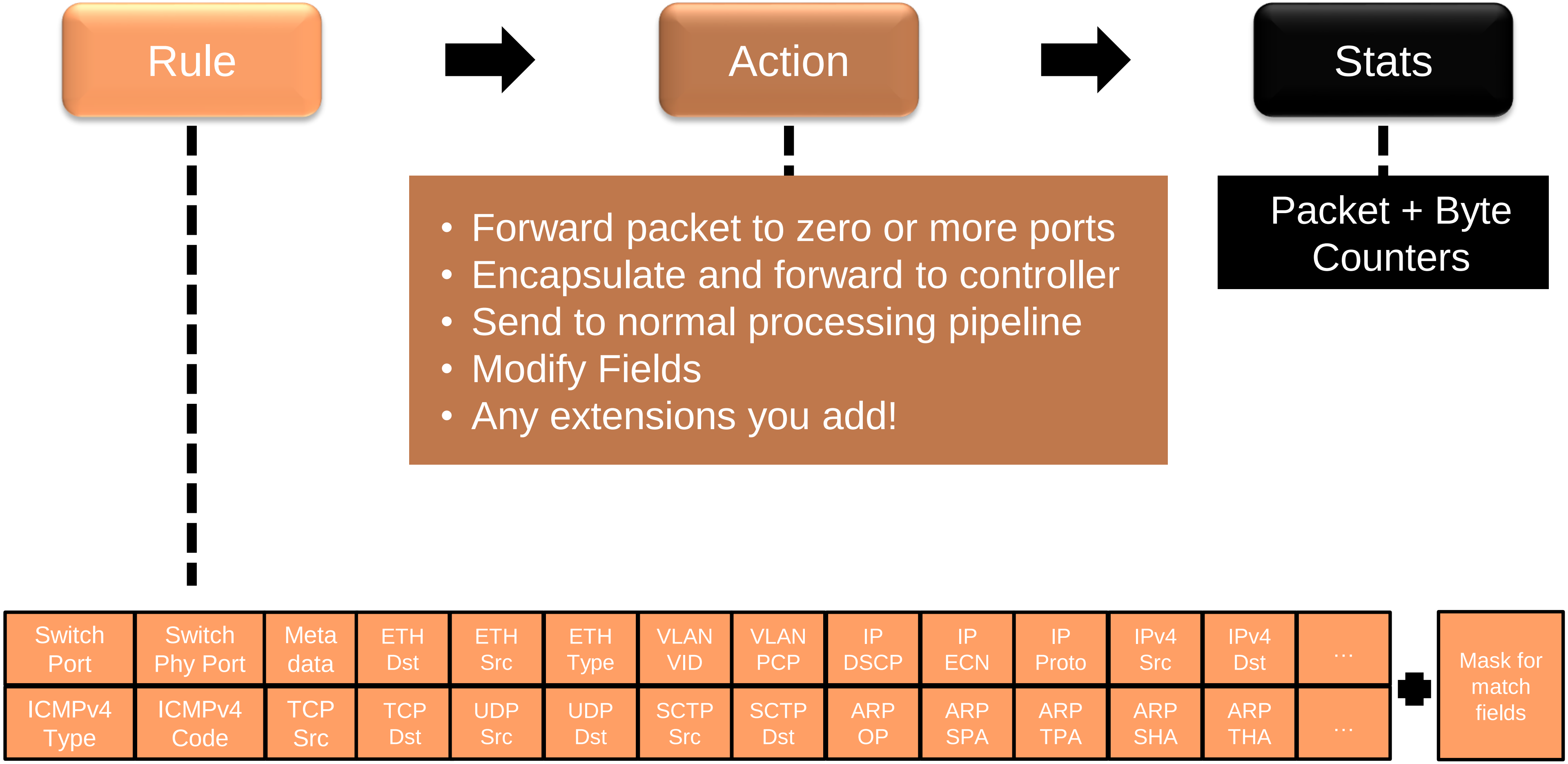
# BACKGROUND

# Software-defined Networking (SDN)

- Key principles
  - Separation of control and data plane
  - Logically centralized control plane
  - Open Interfaces
  - Programmability
- Features
  - Protocol independence
  - Ability to dynamically adapt network parameters
  - Granularity
  - Elasticity
- Use cases
  - Cloud orchestration
  - Network management
  - Network security



# SDN – Packet Handling & Table Structure



- Forward packet to zero or more ports
- Encapsulate and forward to controller
- Send to normal processing pipeline
- Modify Fields
- Any extensions you add!

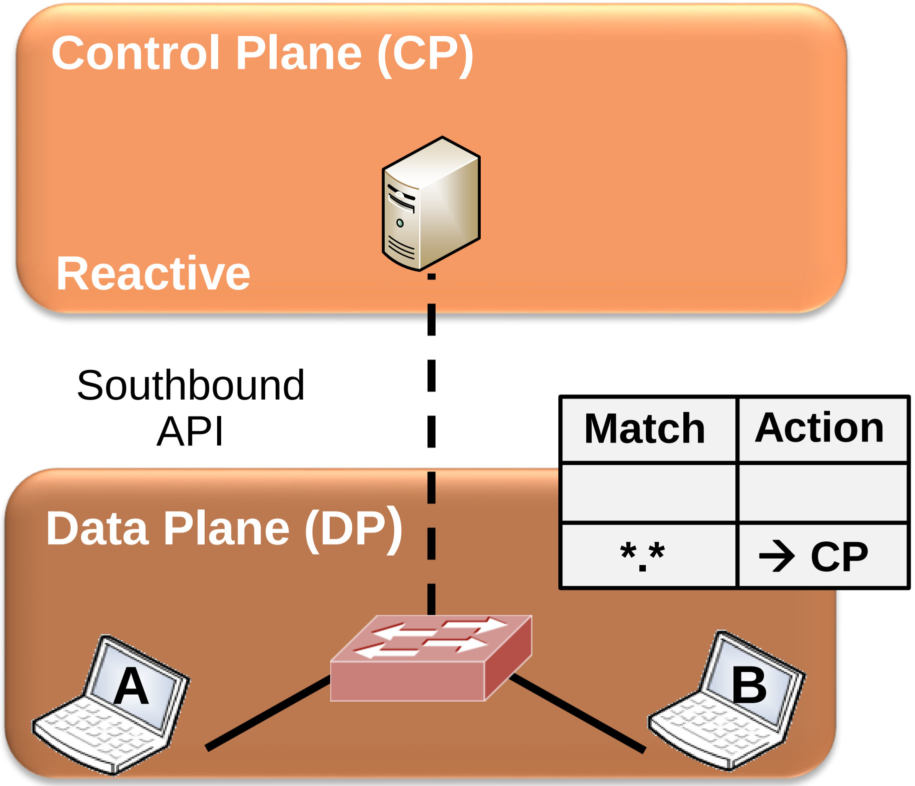
Packet + Byte Counters

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Switch Port | Switch Phy Port | Meta data | ETH Dst | ETH Src | ETH Type | VLAN VID | VLAN PCP | IP DSCP | IP ECN | IP Proto | IPv4 Src | IPv4 Dst | … |
| ICMPv4 Type | ICMPv4 Code | TCP Src | TCP Dst | UDP Src | UDP Dst | SCTP Src | SCTP Dst | ARP OP | ARP SPA | ARP TPA | ARP SHA | ARP THA | … |

+

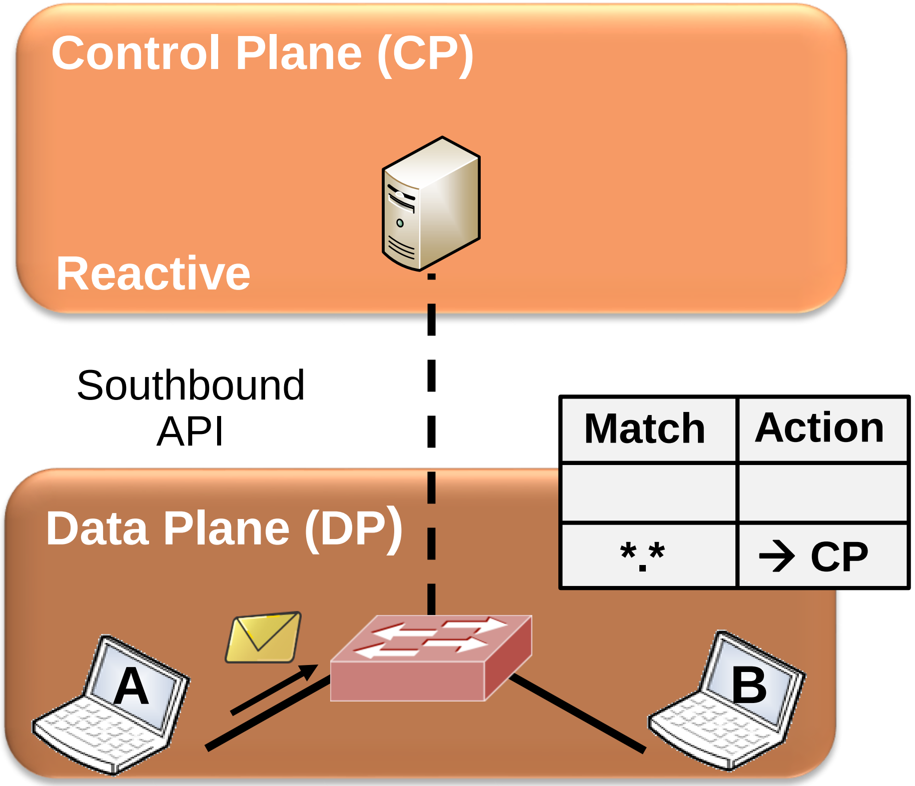
Mask for match fields

# SDN – Modes of Operation



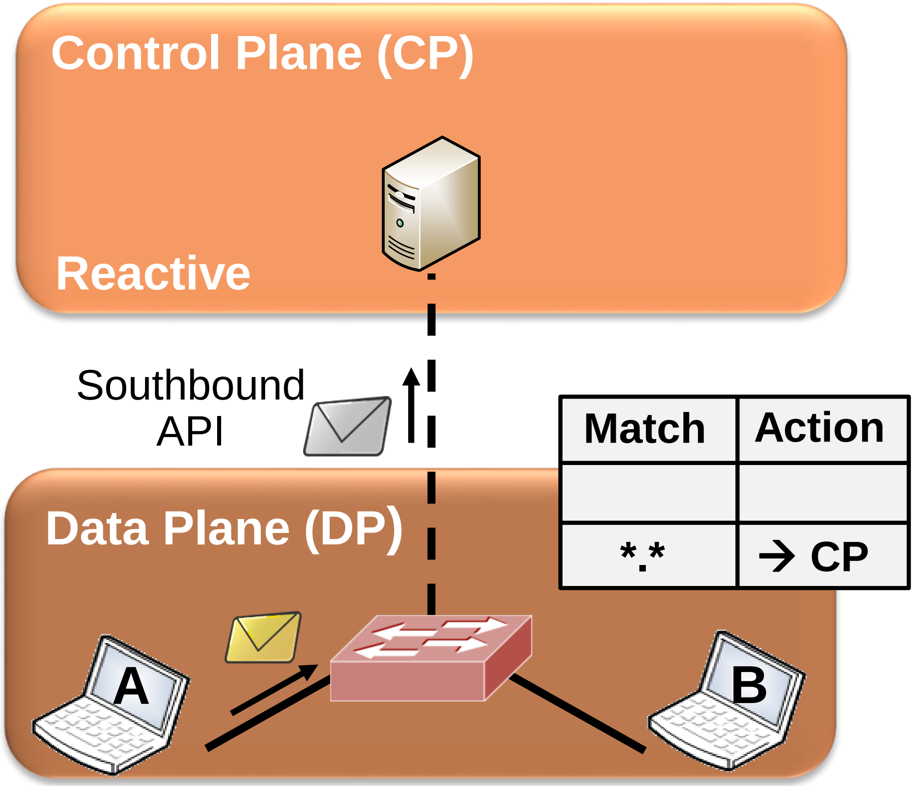
| Match | Action |
|---|---|
| | |
| *.* | → CP |

# SDN – Modes of Operation



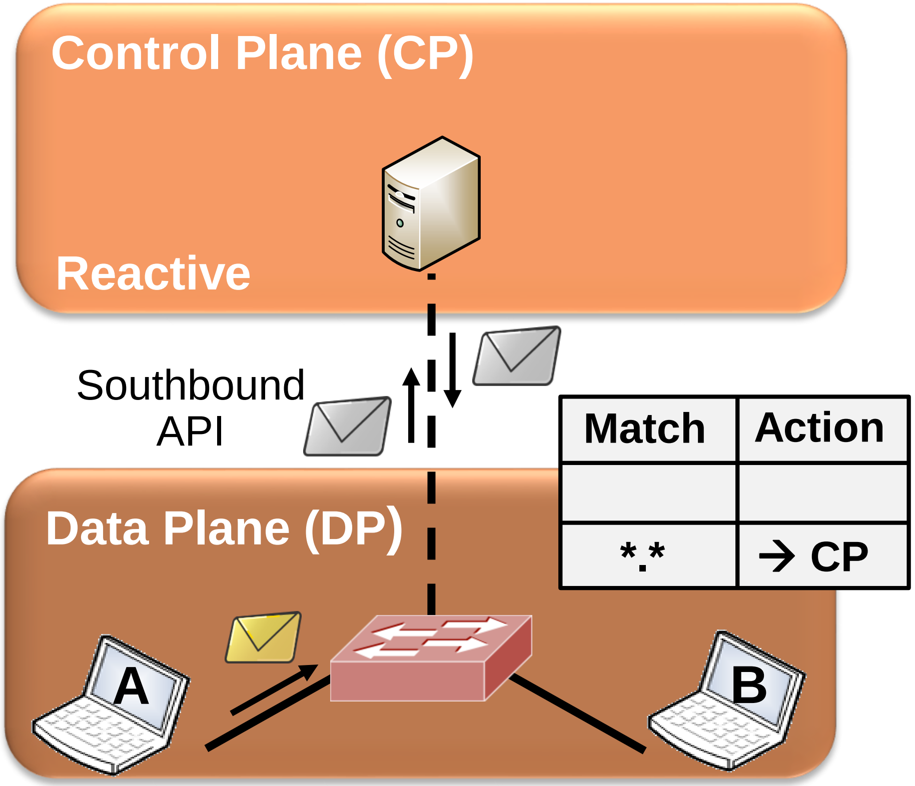
| Match | Action |
|---|---|
| | |
| *.* | → CP |

# SDN – Modes of Operation



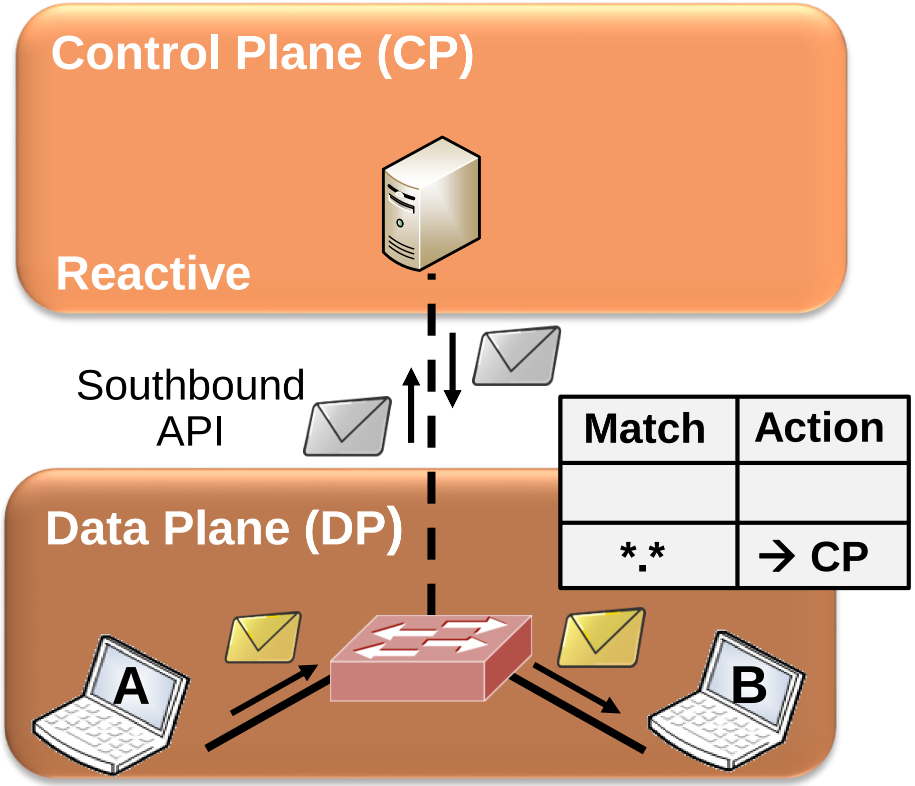
| Match | Action |
|---|---|
| | |
| *.* | → CP |

# SDN – Modes of Operation



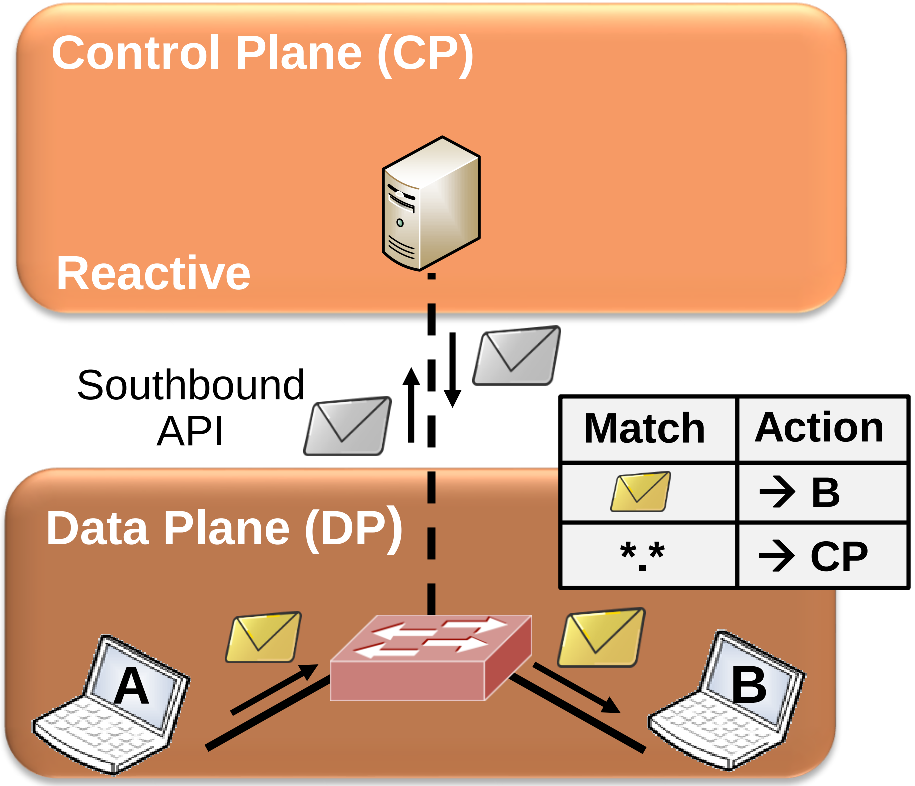
| Match | Action |
|---|---|
| | |
| *.* | → CP |

# SDN – Modes of Operation



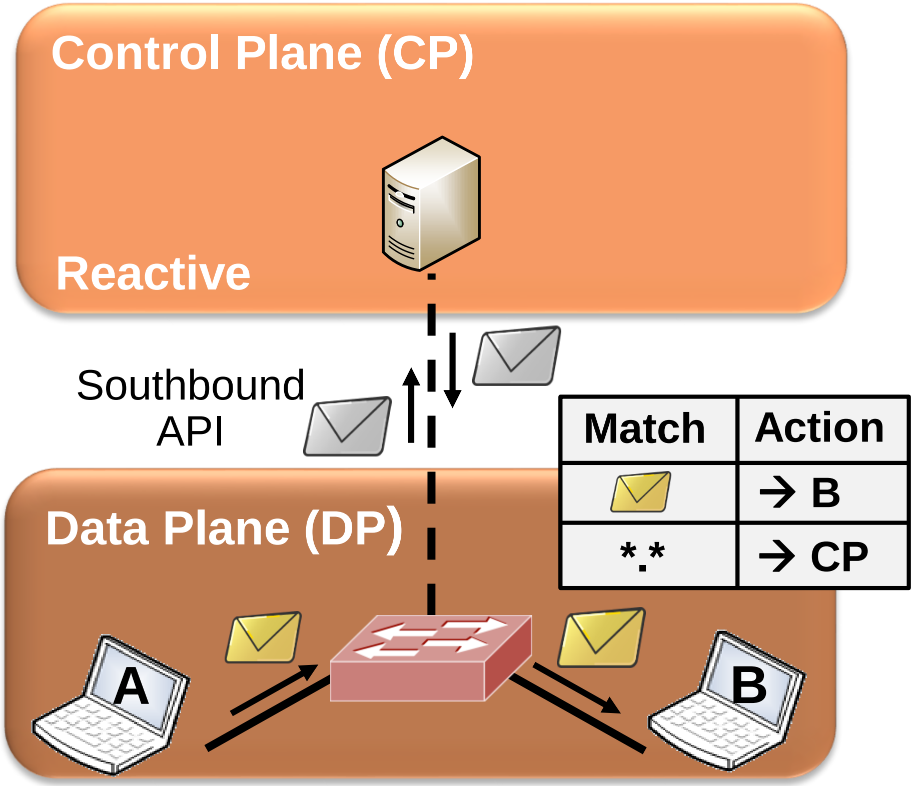
| Match | Action |
|---|---|
| | |
| *.* | → CP |

# SDN – Modes of Operation

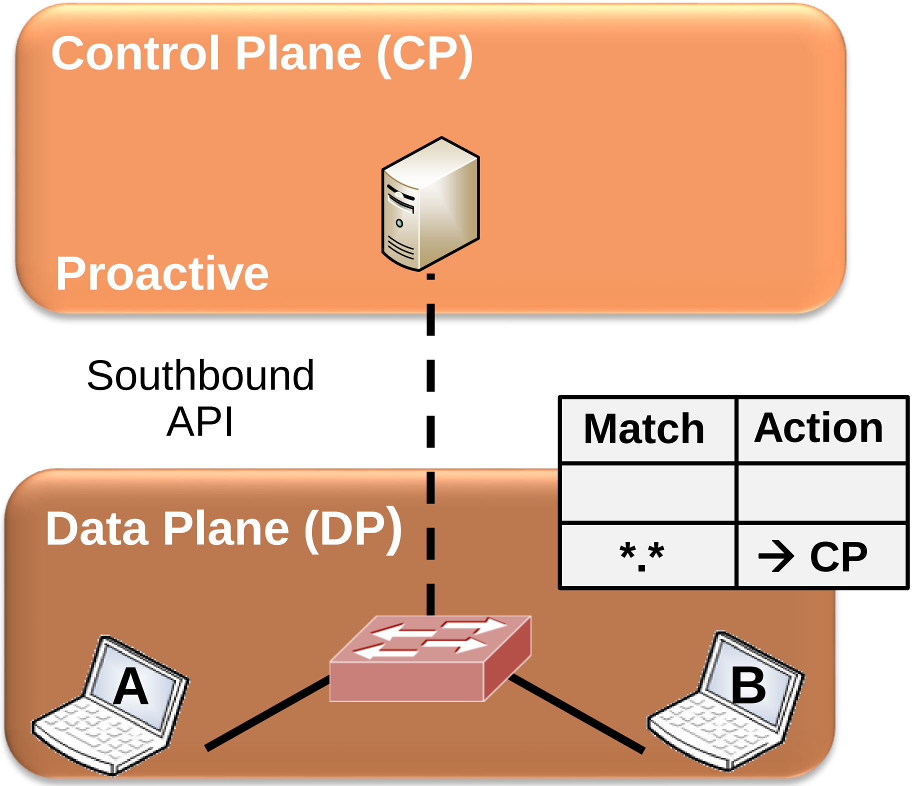


| Match | Action |
|---|---|
| ✉ | → B |
| *.* | → CP |

# SDN – Modes of Operation

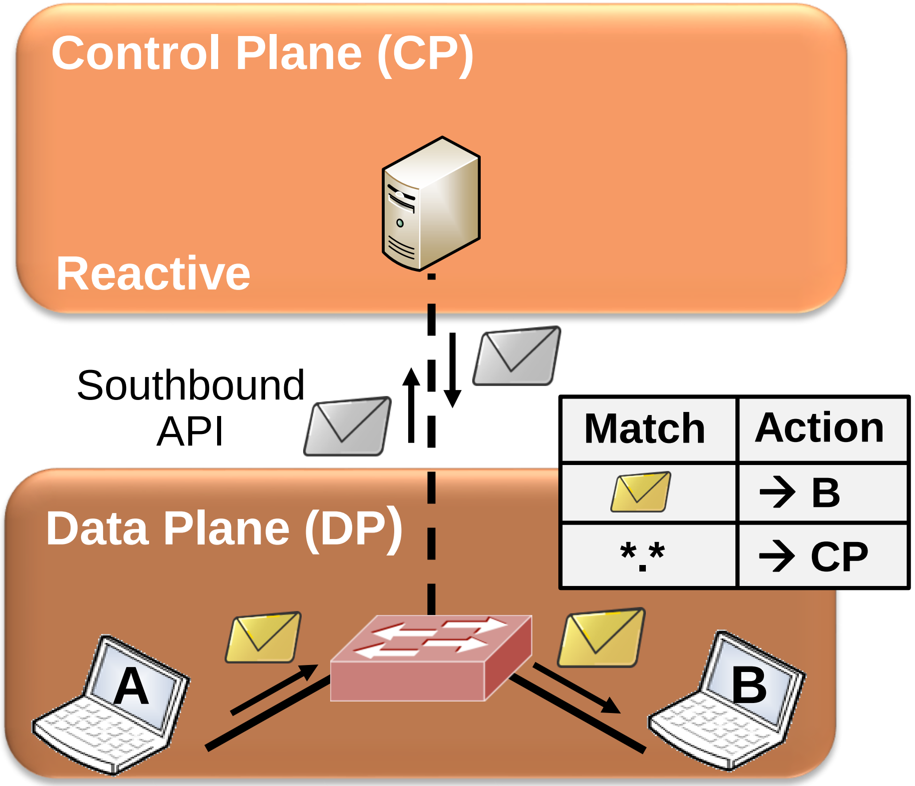


| Match | Action |
|---|---|
| ✉ | → B |
| *.* | → CP |

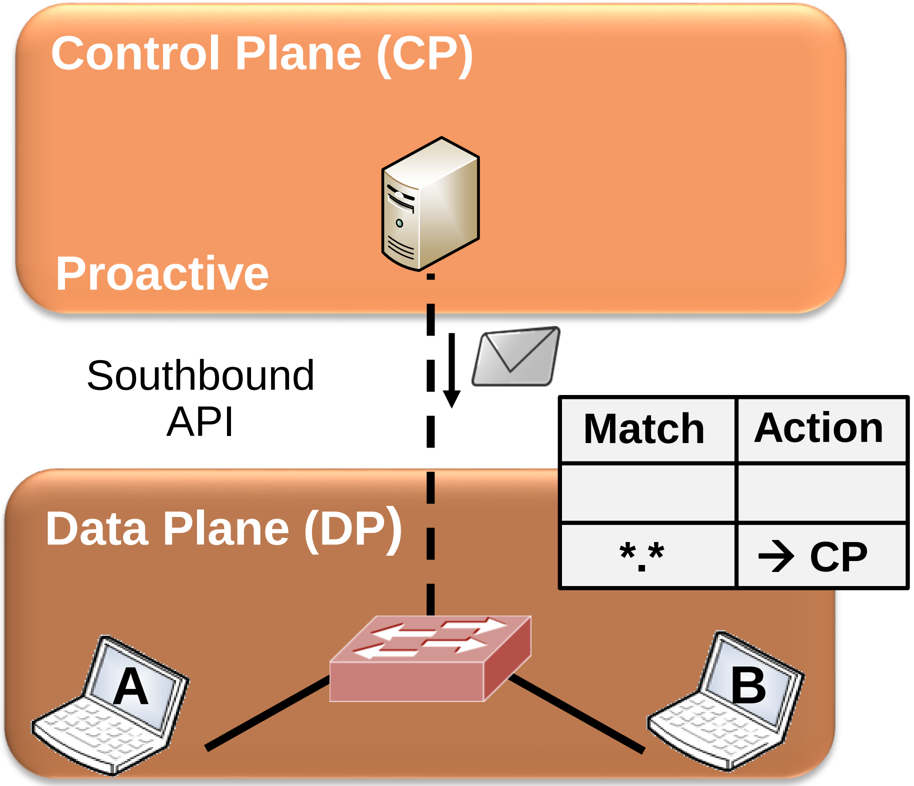


| Match | Action |
|---|---|
| | |
| *.* | → CP |

# SDN – Modes of Operation

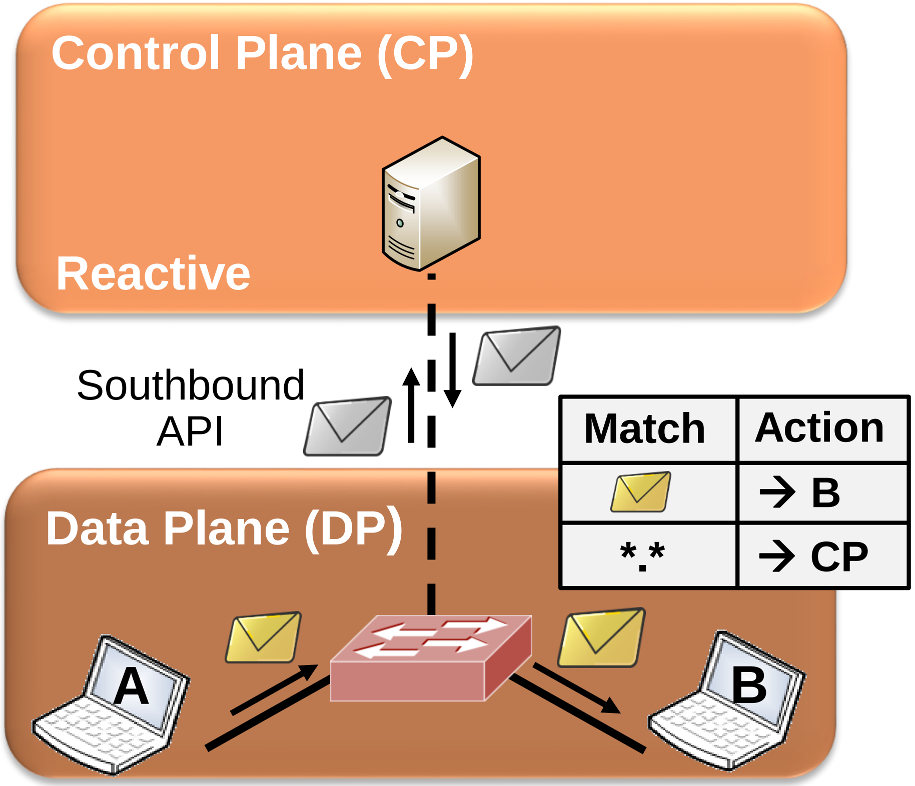


| Match | Action |
|---|---|
| ✉ | → B |
| *.* | → CP |

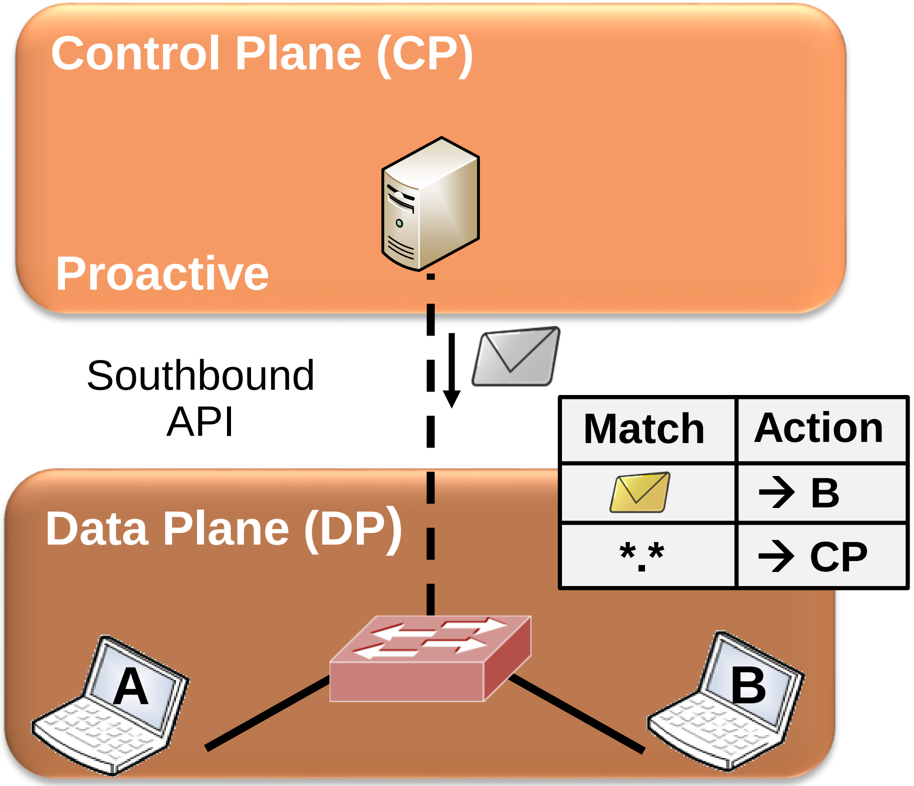


| Match | Action |
|---|---|
| | |
| *.* | → CP |

# SDN – Modes of Operation

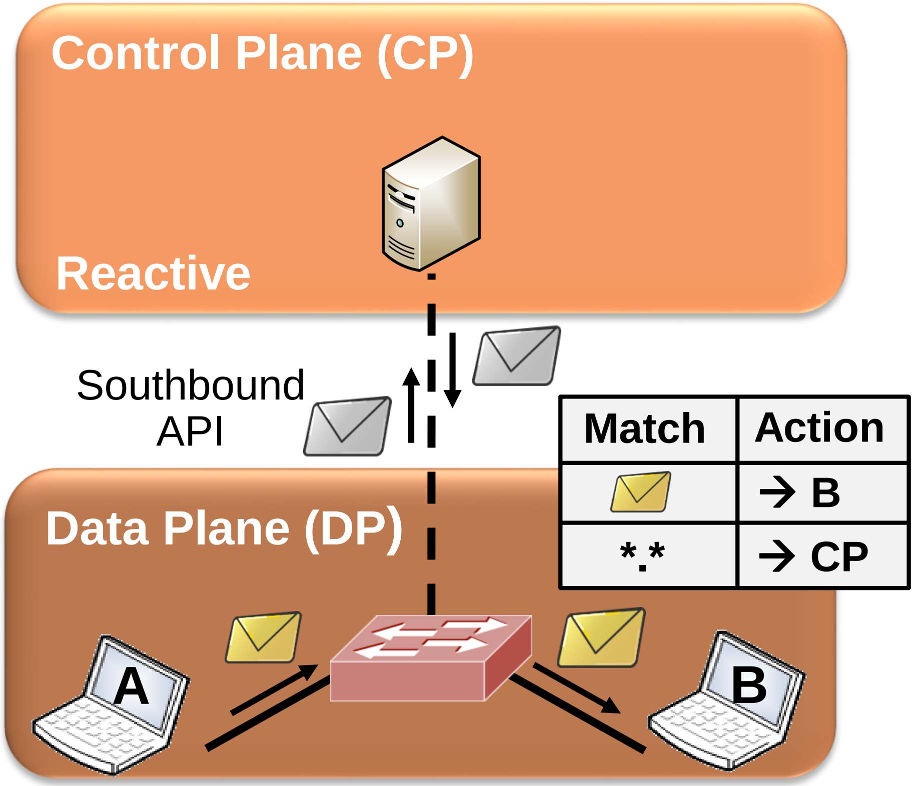


| Match | Action |
|---|---|
| ✉ | → B |
| *.* | → CP |

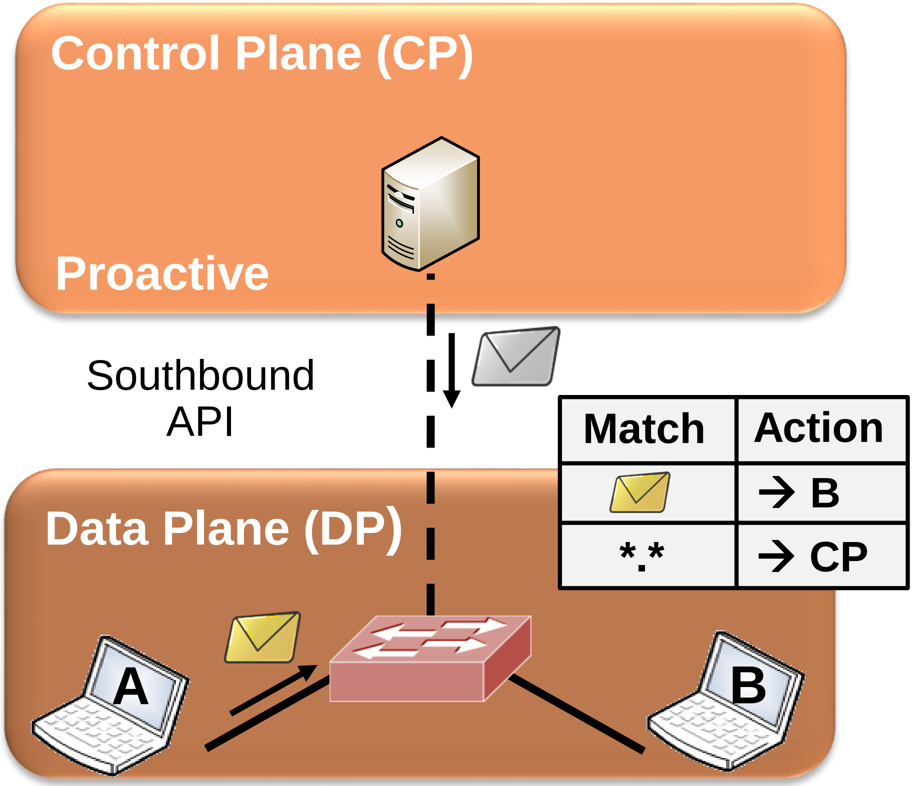


| Match | Action |
|---|---|
| ✉ | → B |
| *.* | → CP |

# SDN – Modes of Operation

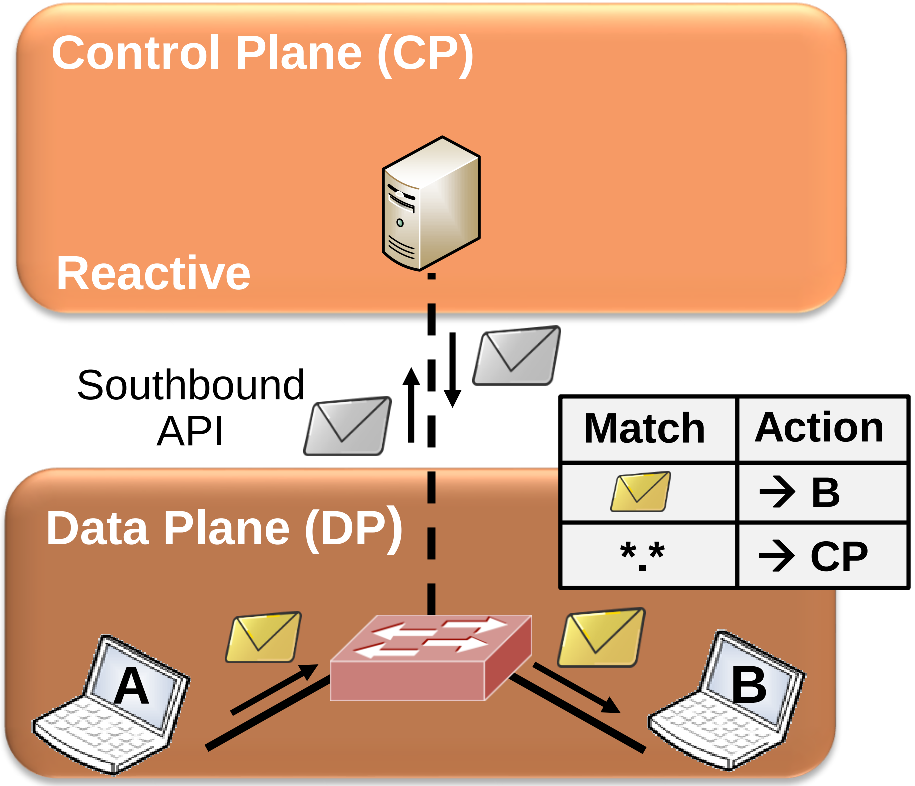


| Match | Action |
|---|---|
| ✉ | → B |
| *.* | → CP |

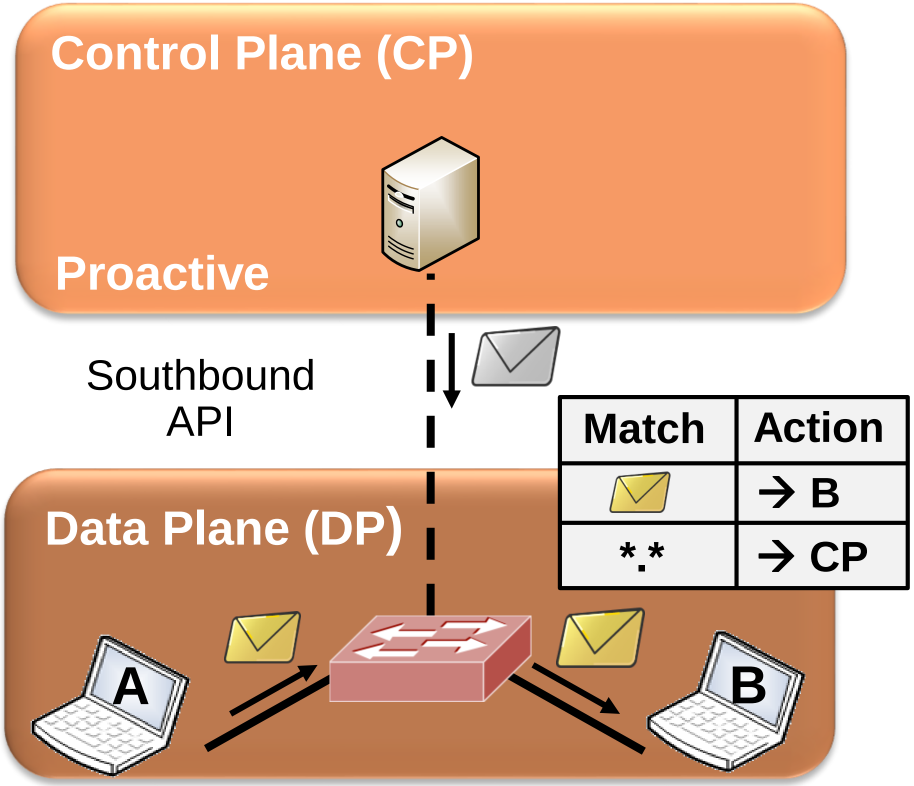


| Match | Action |
|---|---|
| ✉ | → B |
| *.* | → CP |

# SDN – Modes of Operation



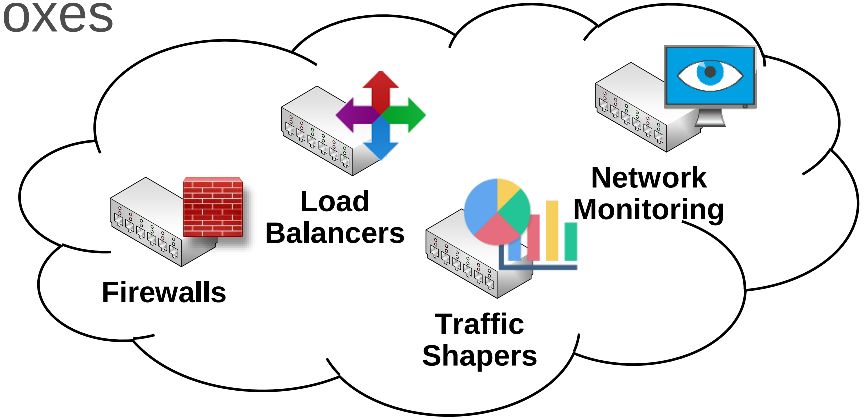
| Match | Action |
|---|---|
| ✉ | → B |
| *.* | → CP |



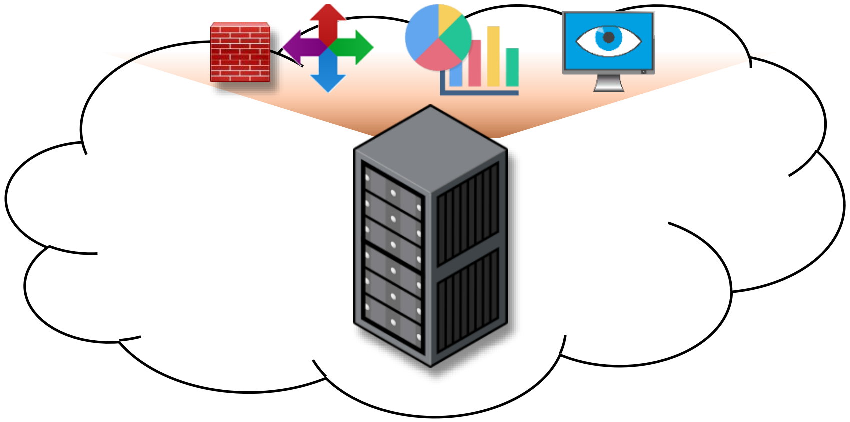
| Match | Action |
|---|---|
| ✉ | → B |
| *.* | → CP |

# Network Function Virtualization (NFV)

- Legacy networks are full of middle boxes
  - Specialized hardware
  - Deployed in the data path
  - Limited scalability



- Network Function Virtualization
  - Virtual applications
  - Executed on COTS servers
  - Cloud-ready

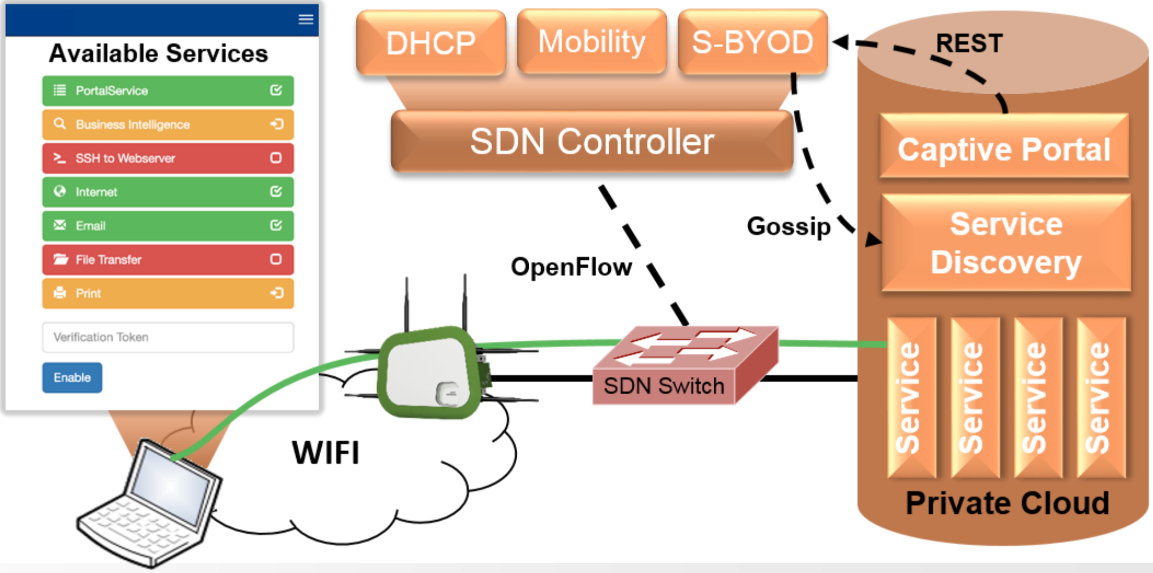


# OMNI-PRESENT SDN FIREWALL

# Fine-granular Access Control

- On-demand personalized virtual network
  - BYOD scenario
  - Strict flow isolation
  - Minimized attack surface

- Technical implementation
  - 2FA Authentication
  - No MDM required



Available Services

- PortalService
- Business Intelligence
- SSH to Webserver
- Internet
- Email
- File Transfer
- Print

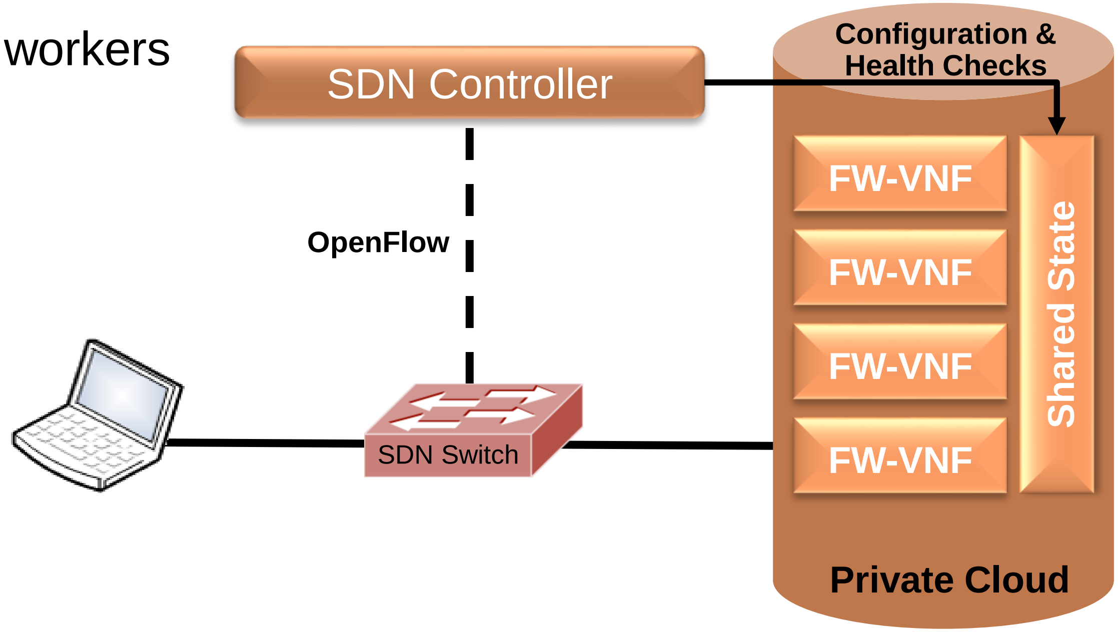
Verification Token

Enable

# Scalable & Resilient Stateful Firewalling

- NFV-based stateful firewall
  - Run as software in the cloud
  - Dynamic n+1 protection

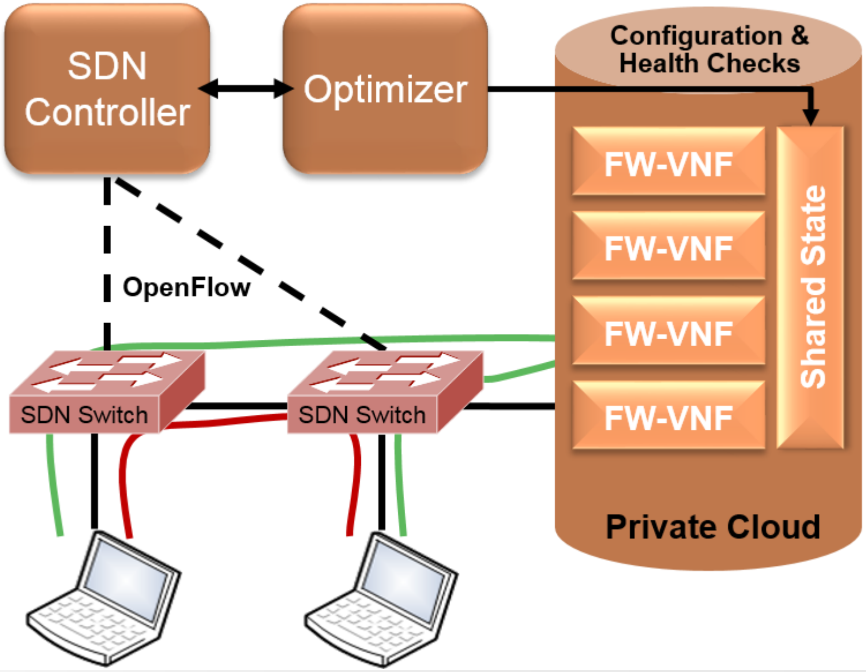
- Technical implementation
  - SDN switch as load balancer
  - State decoupled from workers



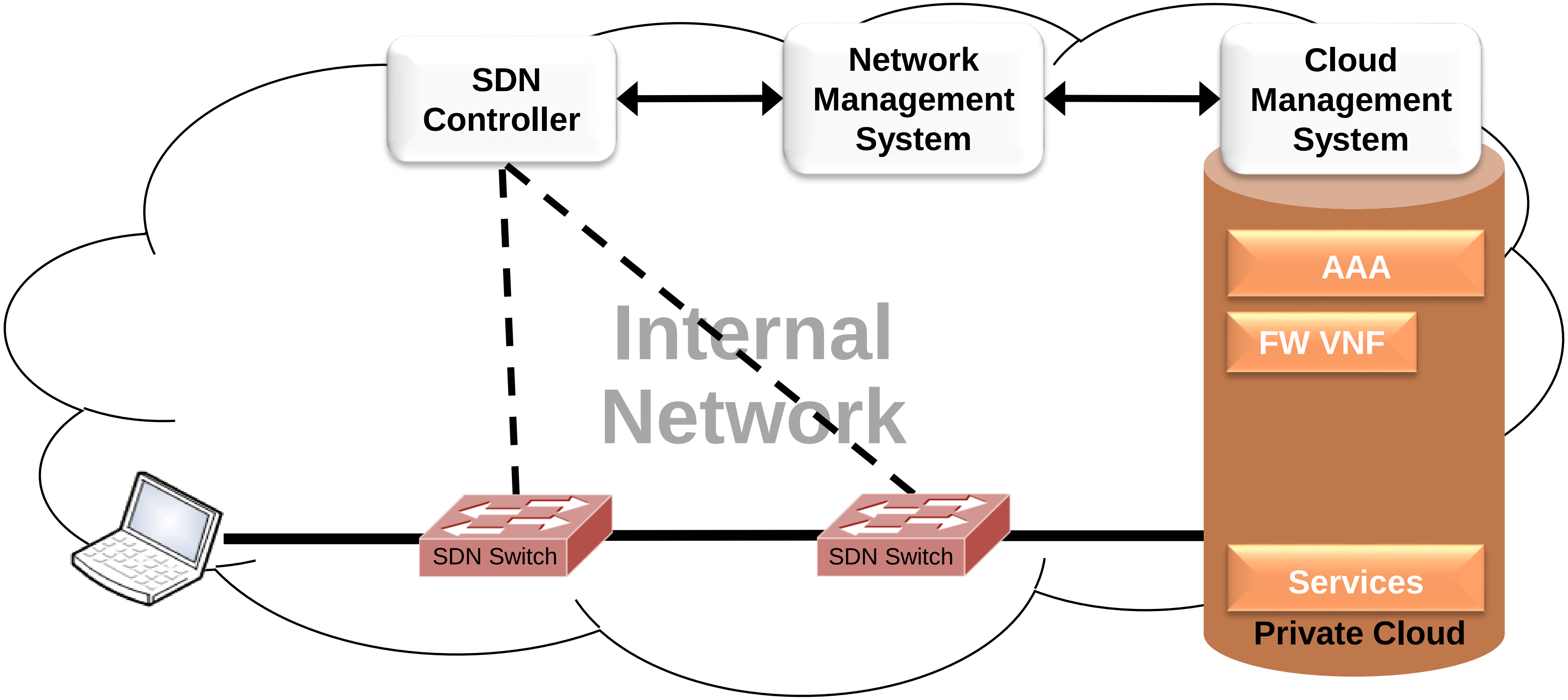
# Firewall Offloading

- Dynamic firewall offloading
  - Offload trusted flows to relief VNFs
  - No noticeable service degradation

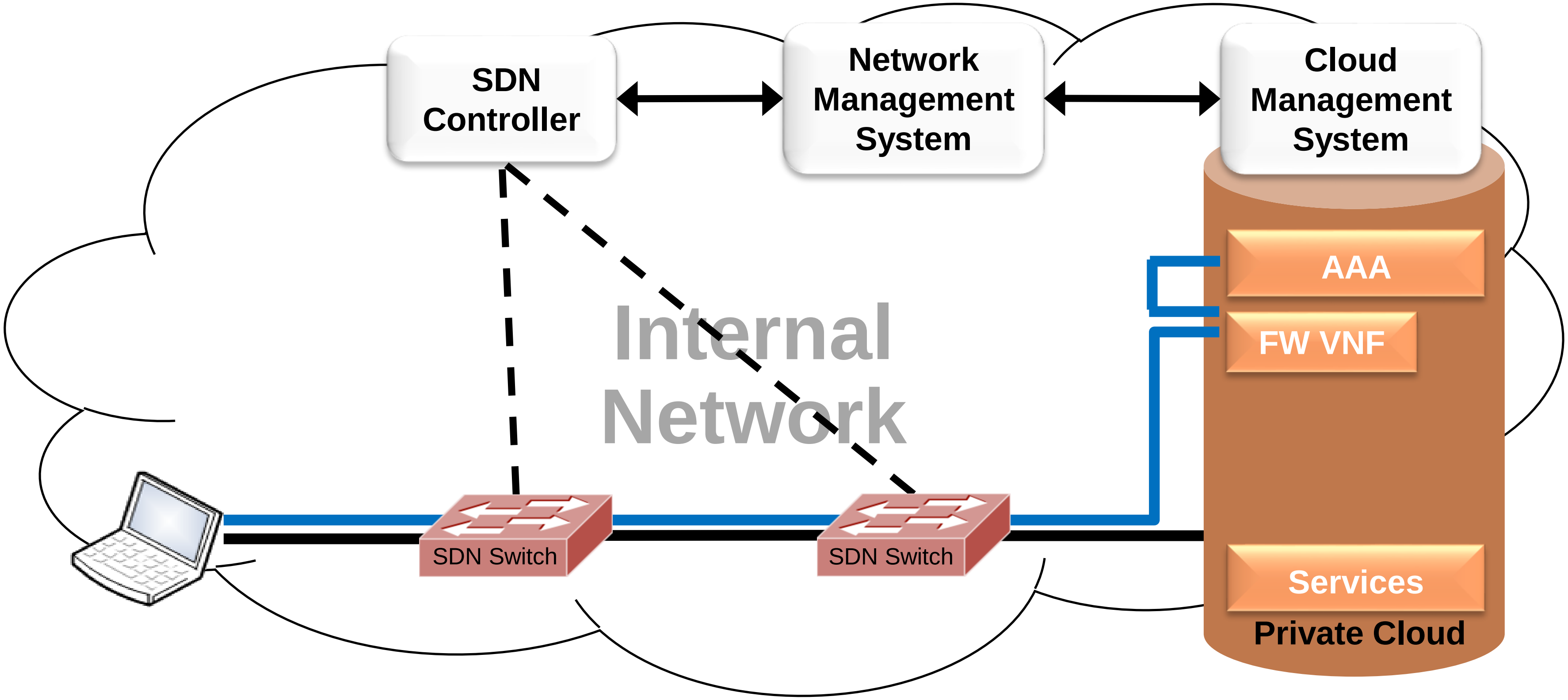
- Technical implementation
  - Optimizer selects flows with a high performance impact
  - Switches act as stateless packet filters
  - Performed in the fast path at line rate



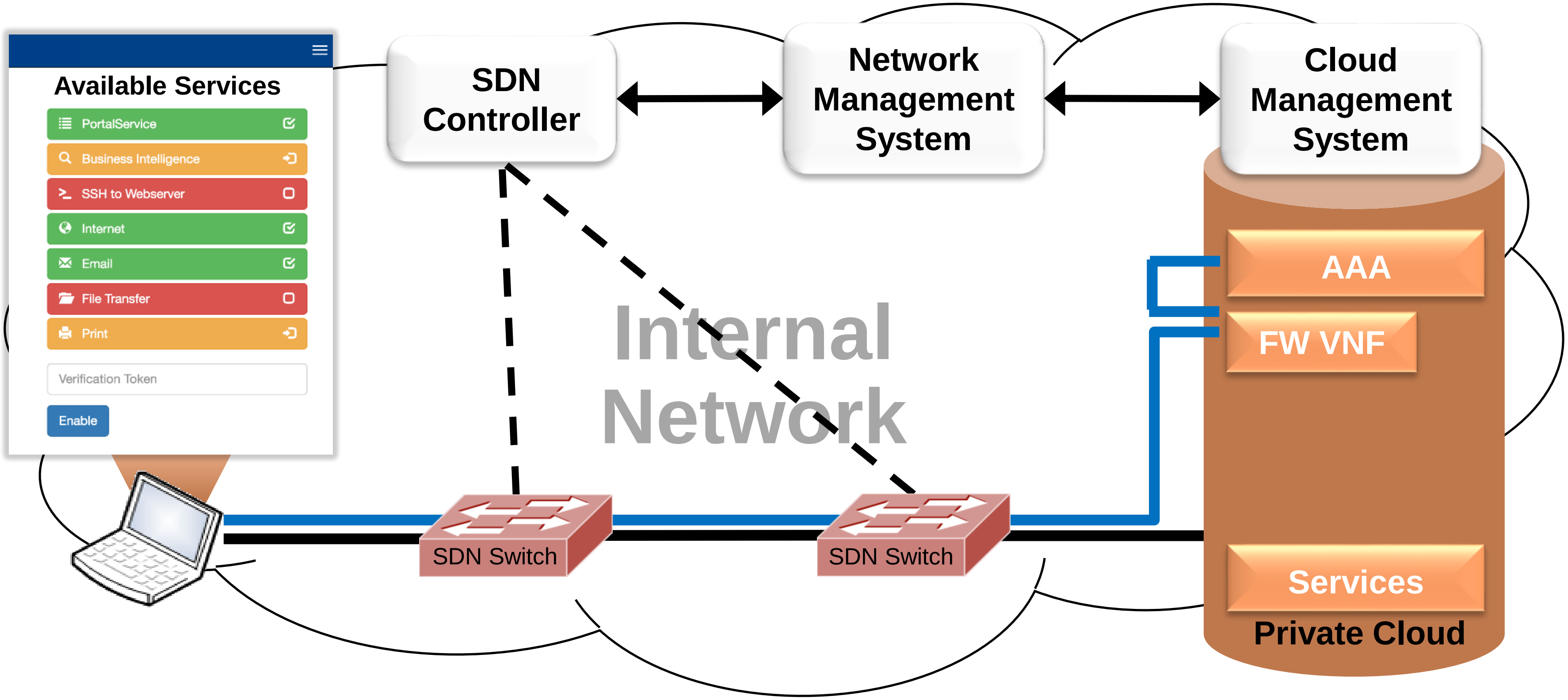
# Omni-present SDN Firewall



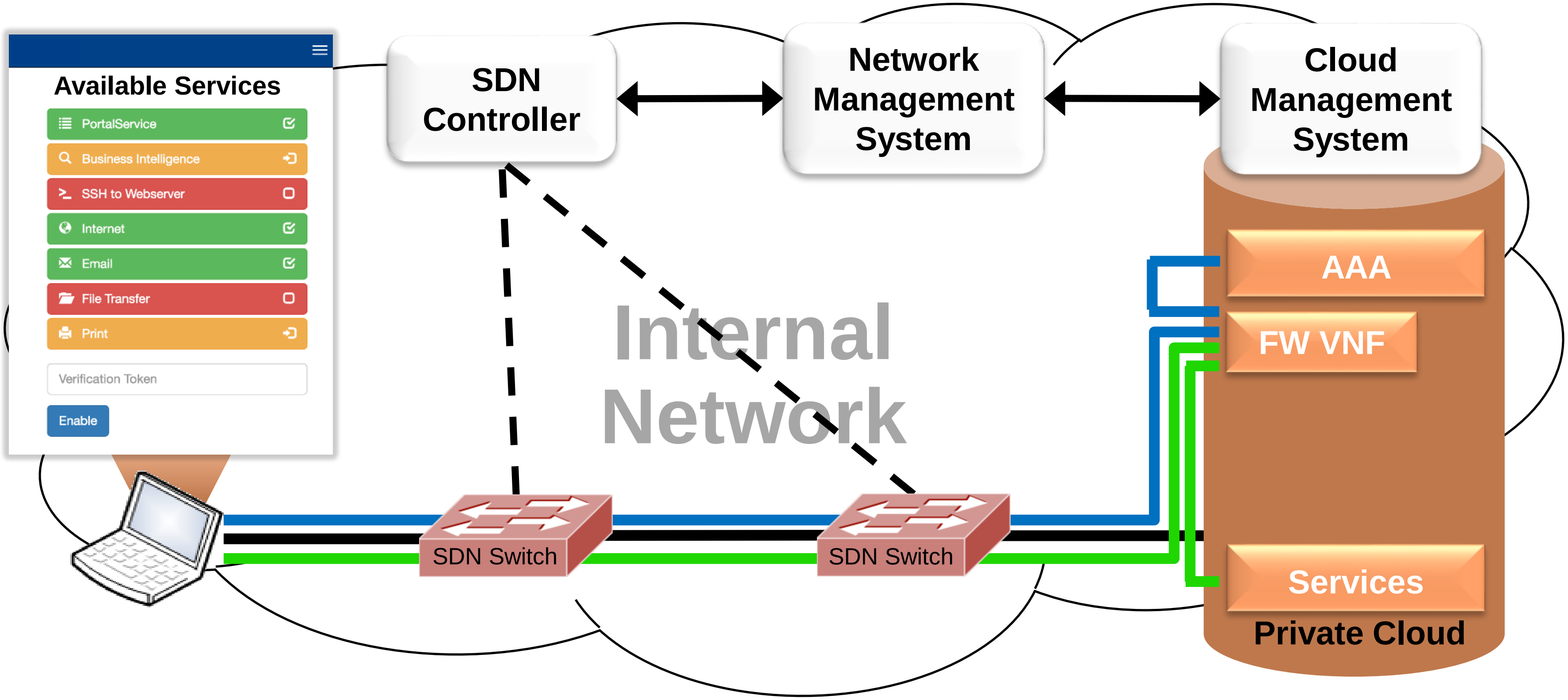
# Omni-present SDN Firewall



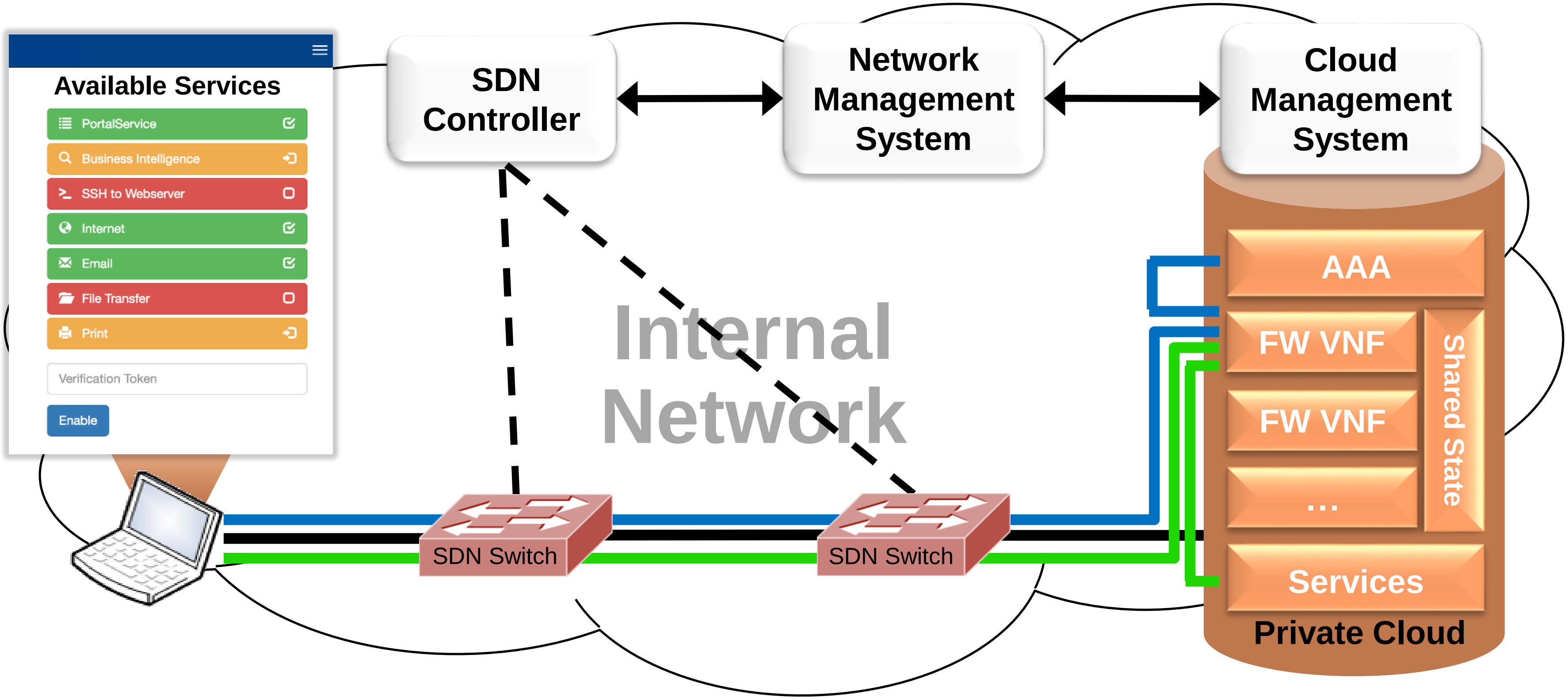
# Omni-present SDN Firewall



# Omni-present SDN Firewall



# Omni-present SDN Firewall



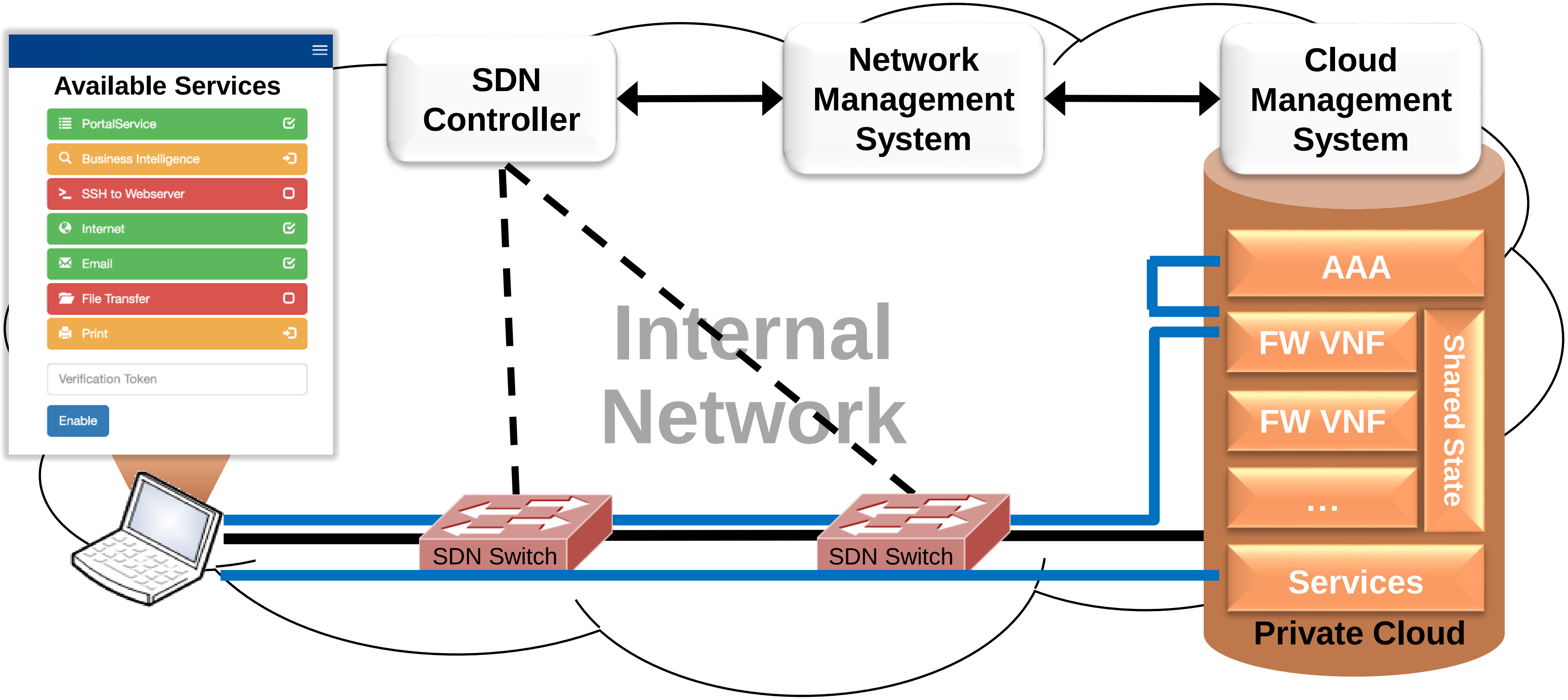
**Available Services**

- PortalService ☑
- Business Intelligence
- SSH to Webserver □
- Internet ☑
- Email ☑
- File Transfer □
- Print

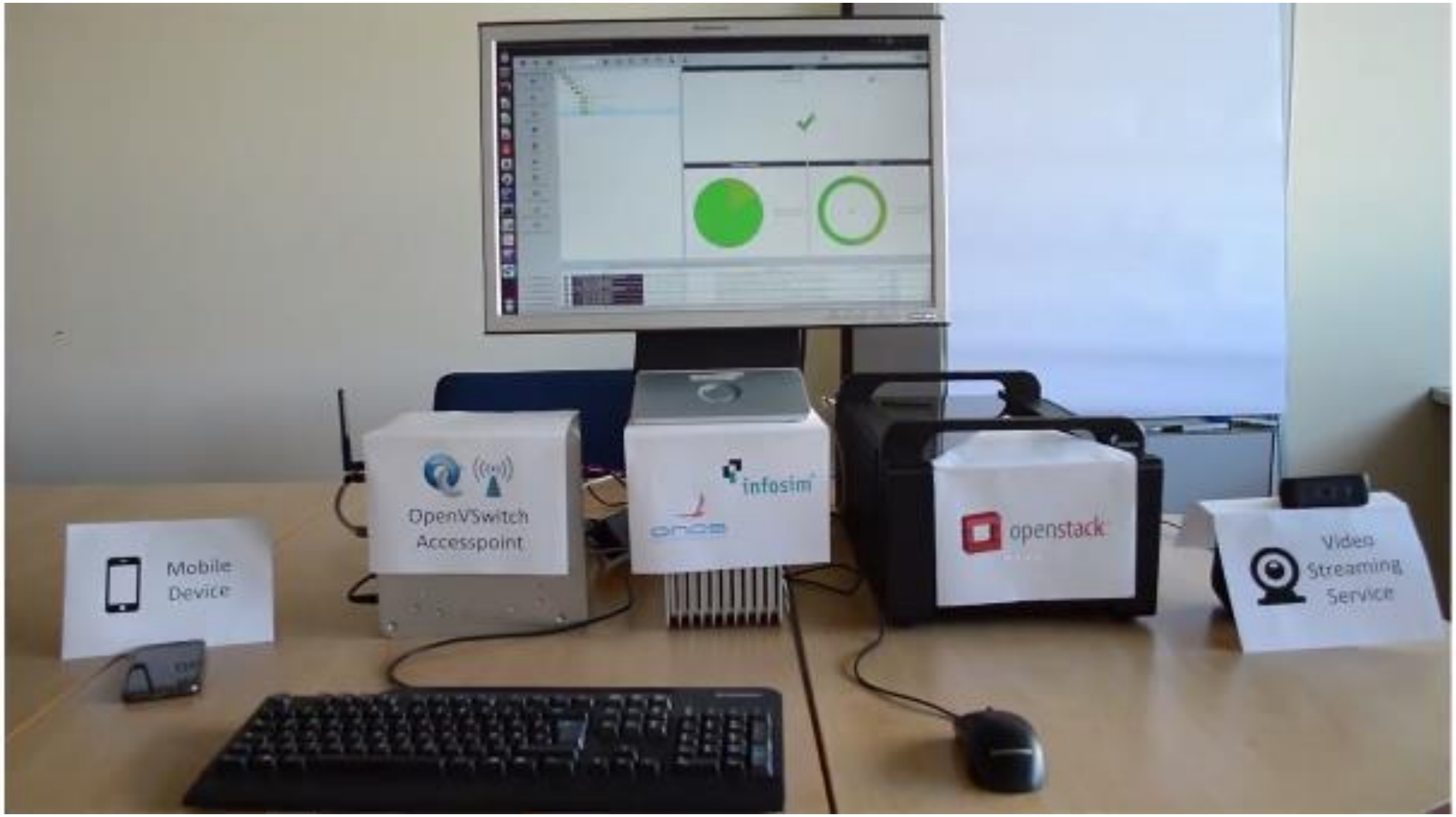
Verification Token

Enable

# Omni-present SDN Firewall

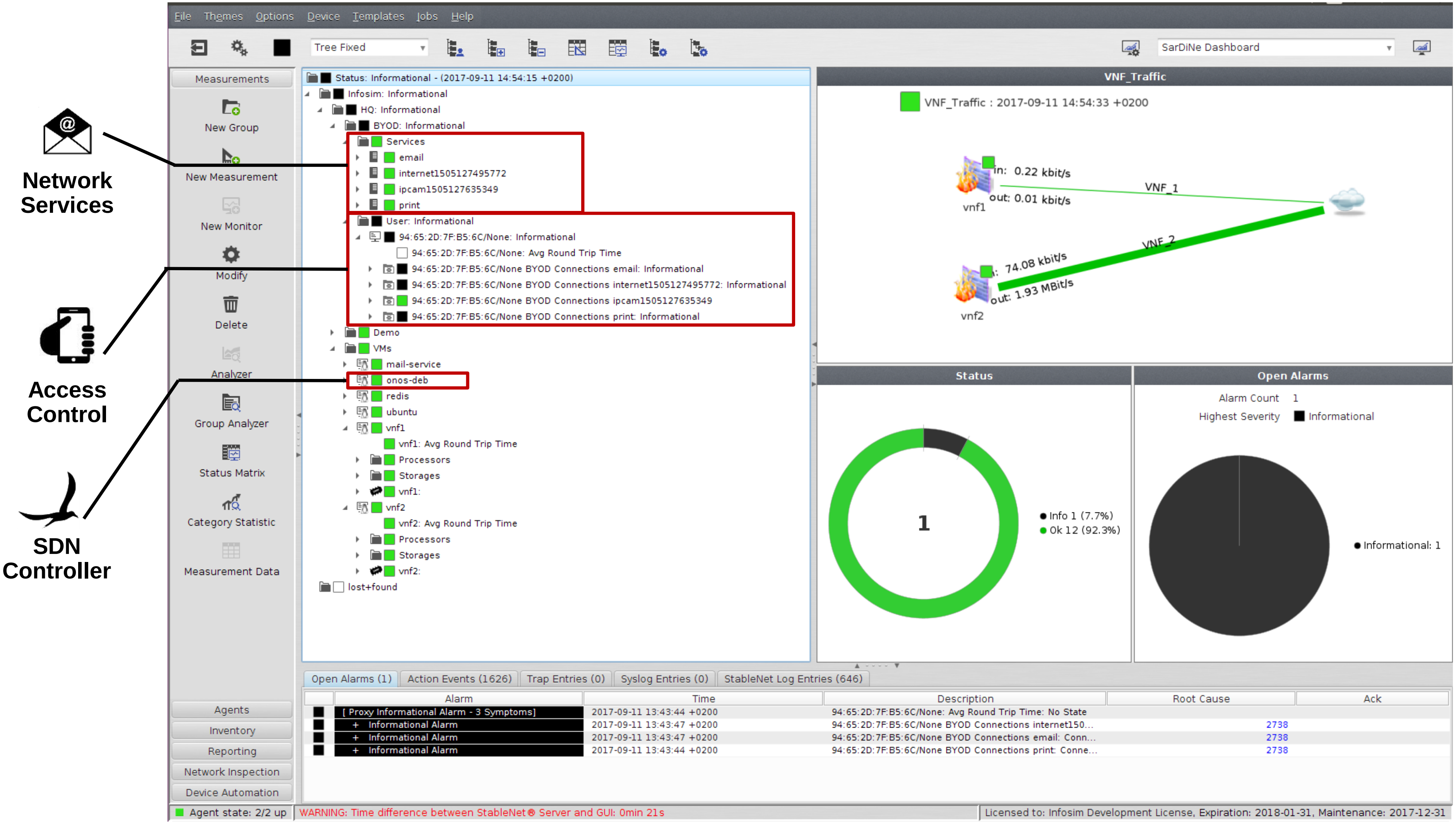


# Demo Setup



https://www.youtube.com/watch?v=e_CmcGPXJGY

# Fine-granular Access Control



Status: Informational - (2017-09-11 14:54:15 +0200)
- Infosim: Informational
  - HQ: Informational
    - BYOD: Informational
      - Services
        - email
        - internet1505127495772
        - ipcam1505127635349
        - print
      - User: Informational
        - 94:65:2D:7F:B5:6C/None: Informational
          - 94:65:2D:7F:B5:6C/None: Avg Round Trip Time
          - 94:65:2D:7F:B5:6C/None BYOD Connections email: Informational
          - 94:65:2D:7F:B5:6C/None BYOD Connections internet1505127495772: Informational
          - 94:65:2D:7F:B5:6C/None BYOD Connections ipcam1505127635349
          - 94:65:2D:7F:B5:6C/None BYOD Connections print: Informational
    - Demo
    - VMs
      - mail-service
      - onos-deb
      - redis
      - ubuntu
      - vnf1
        - vnf1: Avg Round Trip Time
        - Processors
        - Storages
        - vnf1:
      - vnf2
        - vnf2: Avg Round Trip Time
        - Processors
        - Storages
        - vnf2:
  - lost+found

VNF_Traffic : 2017-09-11 14:54:33 +0200

● Info 1 (7.7%)
● Ok 12 (92.3%)

Alarm Count 1
Highest Severity ■ Informational

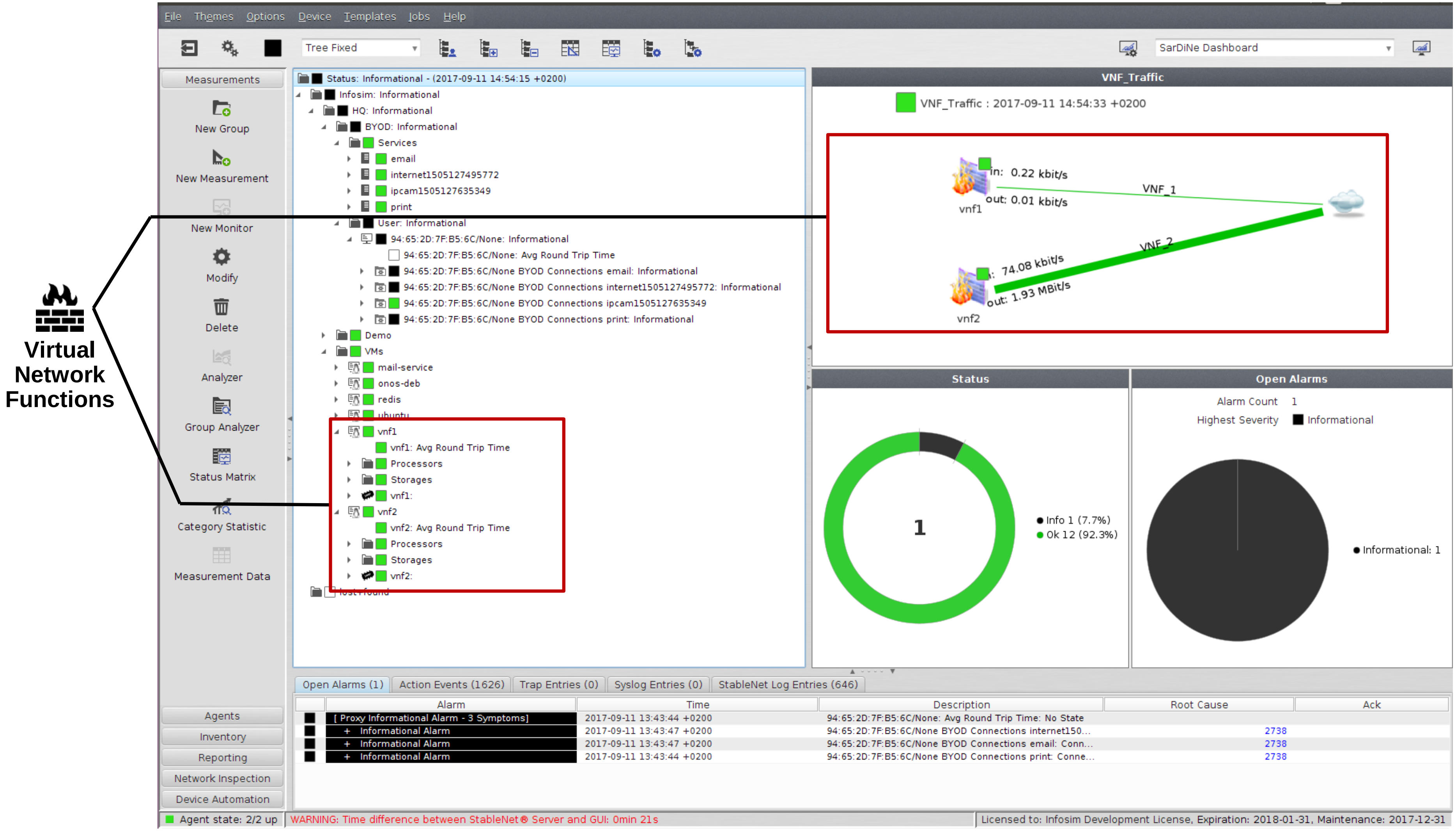
| | Alarm | Time | Description | Root Cause | Ack |
|---|---|---|---|---|---|
| ■ | [ Proxy Informational Alarm - 3 Symptoms] | 2017-09-11 13:43:44 +0200 | 94:65:2D:7F:B5:6C/None: Avg Round Trip Time: No State | | |
| ■ | + Informational Alarm | 2017-09-11 13:43:47 +0200 | 94:65:2D:7F:B5:6C/None BYOD Connections internet150... | 2738 | |
| ■ | + Informational Alarm | 2017-09-11 13:43:47 +0200 | 94:65:2D:7F:B5:6C/None BYOD Connections email: Conn... | 2738 | |
| ■ | + Informational Alarm | 2017-09-11 13:43:44 +0200 | 94:65:2D:7F:B5:6C/None BYOD Connections print: Conne... | 2738 | |

Agent state: 2/2 up

WARNING: Time difference between StableNet® Server and GUI: 0min 21s

Licensed to: Infosim Development License, Expiration: 2018-01-31, Maintenance: 2017-12-31

# NFV Monitoring



Virtual Network Functions

Status: Informational - (2017-09-11 14:54:15 +0200)
- Infosim: Informational
  - HQ: Informational
    - BYOD: Informational
      - 🟩 Services
        - 🟩 email
        - 🟩 internet1505127495772
        - 🟩 ipcam1505127635349
        - 🟩 print
      - User: Informational
        - 94:65:2D:7F:B5:6C/None: Informational
          - □ 94:65:2D:7F:B5:6C/None: Avg Round Trip Time
          - 94:65:2D:7F:B5:6C/None BYOD Connections email: Informational
          - 94:65:2D:7F:B5:6C/None BYOD Connections internet1505127495772: Informational
          - 94:65:2D:7F:B5:6C/None BYOD Connections ipcam1505127635349
          - 94:65:2D:7F:B5:6C/None BYOD Connections print: Informational
    - 🟩 Demo
    - 🟩 VMs
      - 🟩 mail-service
      - 🟩 onos-deb
      - 🟩 redis
      - 🟩 ubuntu
      - 🟩 vnf1
        - 🟩 vnf1: Avg Round Trip Time
        - 🟩 Processors
        - 🟩 Storages
        - 🟩 vnf1:
      - 🟩 vnf2
        - 🟩 vnf2: Avg Round Trip Time
        - 🟩 Processors
        - 🟩 Storages
        - 🟩 vnf2:
- lost+found

**VNF_Traffic**

🟩 VNF_Traffic : 2017-09-11 14:54:33 +0200

**Status**

**Open Alarms**

Alarm Count 1
Highest Severity ■ Informational

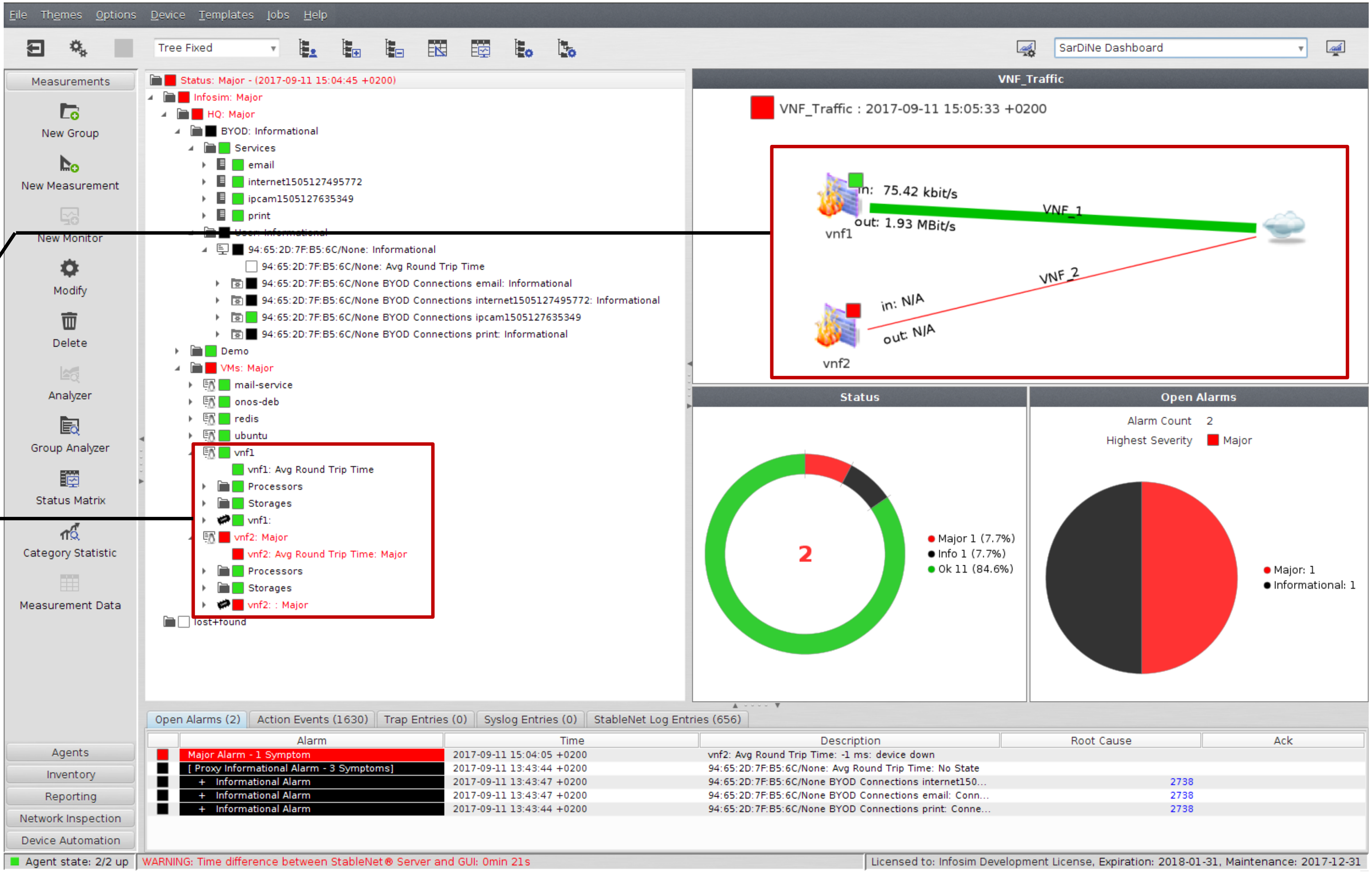
Open Alarms (1) | Action Events (1626) | Trap Entries (0) | Syslog Entries (0) | StableNet Log Entries (646)

| | Alarm | Time | Description | Root Cause | Ack |
|---|---|---|---|---|---|
| ■ | [ Proxy Informational Alarm - 3 Symptoms] | 2017-09-11 13:43:44 +0200 | 94:65:2D:7F:B5:6C/None: Avg Round Trip Time: No State | | |
| ■ | + Informational Alarm | 2017-09-11 13:43:47 +0200 | 94:65:2D:7F:B5:6C/None BYOD Connections internet150... | 2738 | |
| ■ | + Informational Alarm | 2017-09-11 13:43:47 +0200 | 94:65:2D:7F:B5:6C/None BYOD Connections email: Conn... | 2738 | |
| ■ | + Informational Alarm | 2017-09-11 13:43:44 +0200 | 94:65:2D:7F:B5:6C/None BYOD Connections print: Conne... | 2738 | |

🟩 Agent state: 2/2 up | WARNING: Time difference between StableNet® Server and GUI: 0min 21s | Licensed to: Infosim Development License, Expiration: 2018-01-31, Maintenance: 2017-12-31

# Fast Failover

**Firewall VNF Resiliency**



Status: Major - (2017-09-11 15:04:45 +0200)
- Infosim: Major
  - HQ: Major
    - BYOD: Informational
      - Services
        - email
        - internet1505127495772
        - ipcam1505127635349
        - print
      - User: Informational
        - 94:65:2D:7F:B5:6C/None: Informational
          - 94:65:2D:7F:B5:6C/None: Avg Round Trip Time
          - 94:65:2D:7F:B5:6C/None BYOD Connections email: Informational
          - 94:65:2D:7F:B5:6C/None BYOD Connections internet1505127495772: Informational
          - 94:65:2D:7F:B5:6C/None BYOD Connections ipcam1505127635349
          - 94:65:2D:7F:B5:6C/None BYOD Connections print: Informational
    - Demo
    - VMs: Major
      - mail-service
      - onos-deb
      - redis
      - ubuntu
      - vnf1
        - vnf1: Avg Round Trip Time
        - Processors
        - Storages
        - vnf1:
      - vnf2: Major
        - vnf2: Avg Round Trip Time: Major
        - Processors
        - Storages
        - vnf2: : Major
  - lost+found

**VNF_Traffic**

VNF_Traffic : 2017-09-11 15:05:33 +0200

**Status**

**Open Alarms**

Alarm Count 2

Highest Severity 🟥 Major

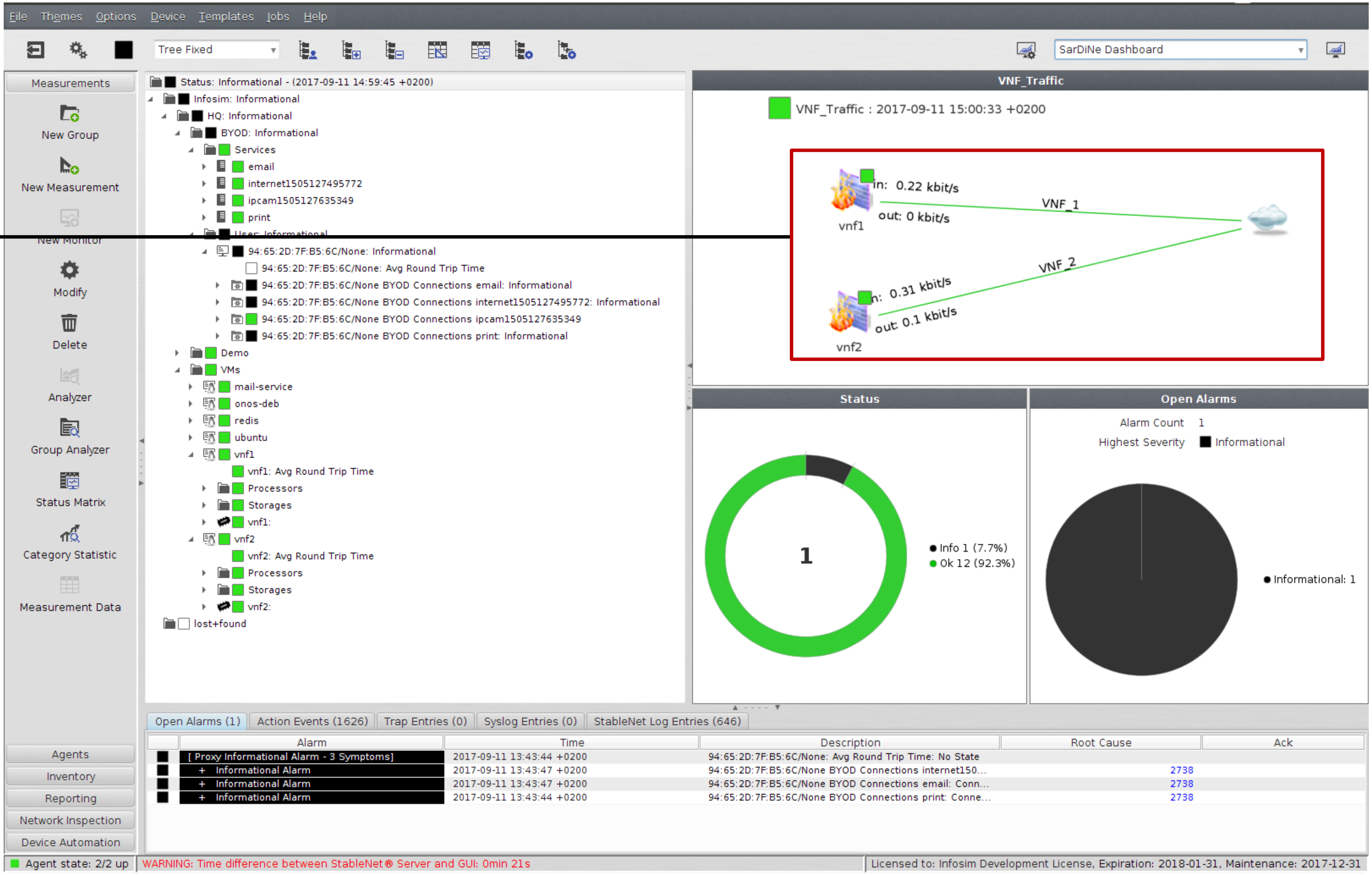
Open Alarms (2) | Action Events (1630) | Trap Entries (0) | Syslog Entries (0) | StableNet Log Entries (656)

| | Alarm | Time | Description | Root Cause | Ack |
|---|---|---|---|---|---|
| 🟥 | Major Alarm - 1 Symptom | 2017-09-11 15:04:05 +0200 | vnf2: Avg Round Trip Time: -1 ms: device down | | |
| ■ | [ Proxy Informational Alarm - 3 Symptoms] | 2017-09-11 13:43:44 +0200 | 94:65:2D:7F:B5:6C/None: Avg Round Trip Time: No State | | |
| ■ | + Informational Alarm | 2017-09-11 13:43:47 +0200 | 94:65:2D:7F:B5:6C/None BYOD Connections internet150... | 2738 | |
| ■ | + Informational Alarm | 2017-09-11 13:43:47 +0200 | 94:65:2D:7F:B5:6C/None BYOD Connections email: Conn... | 2738 | |
| ■ | + Informational Alarm | 2017-09-11 13:43:44 +0200 | 94:65:2D:7F:B5:6C/None BYOD Connections print: Conne... | 2738 | |

Agent state: 2/2 up | WARNING: Time difference between StableNet® Server and GUI: 0min 21s | Licensed to: Infosim Development License, Expiration: 2018-01-31, Maintenance: 2017-12-31

# Offloading of Trusted Flows

Firewall
VNF
Offloading



```
Status: Informational - (2017-09-11 14:59:45 +0200)
  Infosim: Informational
    HQ: Informational
      BYOD: Informational
        Services
          email
          internet1505127495772
          ipcam1505127635349
          print
        User: Informational
          94:65:2D:7F:B5:6C/None: Informational
            94:65:2D:7F:B5:6C/None: Avg Round Trip Time
            94:65:2D:7F:B5:6C/None BYOD Connections email: Informational
            94:65:2D:7F:B5:6C/None BYOD Connections internet1505127495772: Informational
            94:65:2D:7F:B5:6C/None BYOD Connections ipcam1505127635349
            94:65:2D:7F:B5:6C/None BYOD Connections print: Informational
      Demo
      VMs
        mail-service
        onos-deb
        redis
        ubuntu
        vnf1
          vnf1: Avg Round Trip Time
          Processors
          Storages
          vnf1:
        vnf2
          vnf2: Avg Round Trip Time
          Processors
          Storages
          vnf2:
  lost+found
```

VNF_Traffic : 2017-09-11 15:00:33 +0200

Alarm Count 1

Highest Severity ■ Informational

Open Alarms (1) | Action Events (1626) | Trap Entries (0) | Syslog Entries (0) | StableNet Log Entries (646)

| | Alarm | Time | Description | Root Cause | Ack |
|---|---|---|---|---|---|
| ■ | [ Proxy Informational Alarm - 3 Symptoms] | 2017-09-11 13:43:44 +0200 | 94:65:2D:7F:B5:6C/None: Avg Round Trip Time: No State | | |
| ■ | + Informational Alarm | 2017-09-11 13:43:47 +0200 | 94:65:2D:7F:B5:6C/None BYOD Connections internet150... | 2738 | |
| ■ | + Informational Alarm | 2017-09-11 13:43:47 +0200 | 94:65:2D:7F:B5:6C/None BYOD Connections email: Conn... | 2738 | |
| ■ | + Informational Alarm | 2017-09-11 13:43:44 +0200 | 94:65:2D:7F:B5:6C/None BYOD Connections print: Conne... | 2738 | |

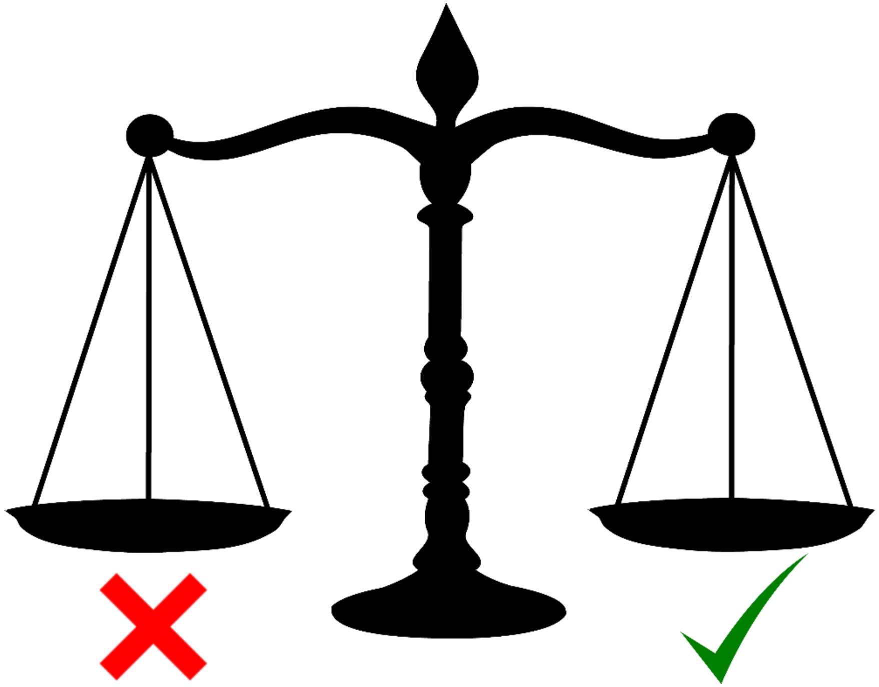
Agent state: 2/2 up

WARNING: Time difference between StableNet® Server and GUI: 0min 21s

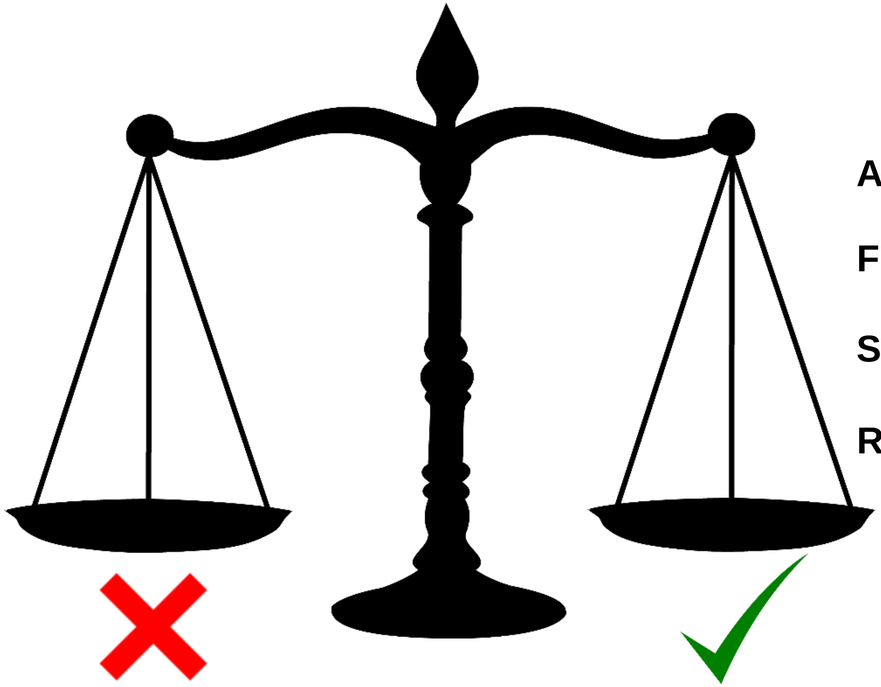
Licensed to: Infosim Development License, Expiration: 2018-01-31, Maintenance: 2017-12-31

# CONCLUSION

# Conclusion



# Conclusion



Advanced DDoS Mitigation

Fine-granular Flow Control

Scalable Security Solutions

Reduced Management Efforts

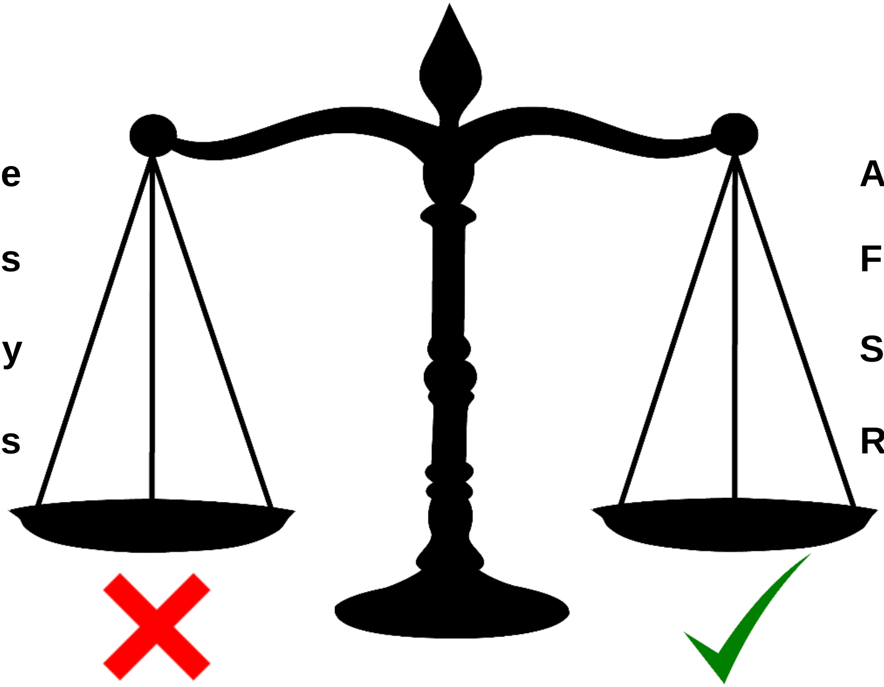
# Conclusion

Complex Architecture

Fast development rates

New Technology

Large Software Projects



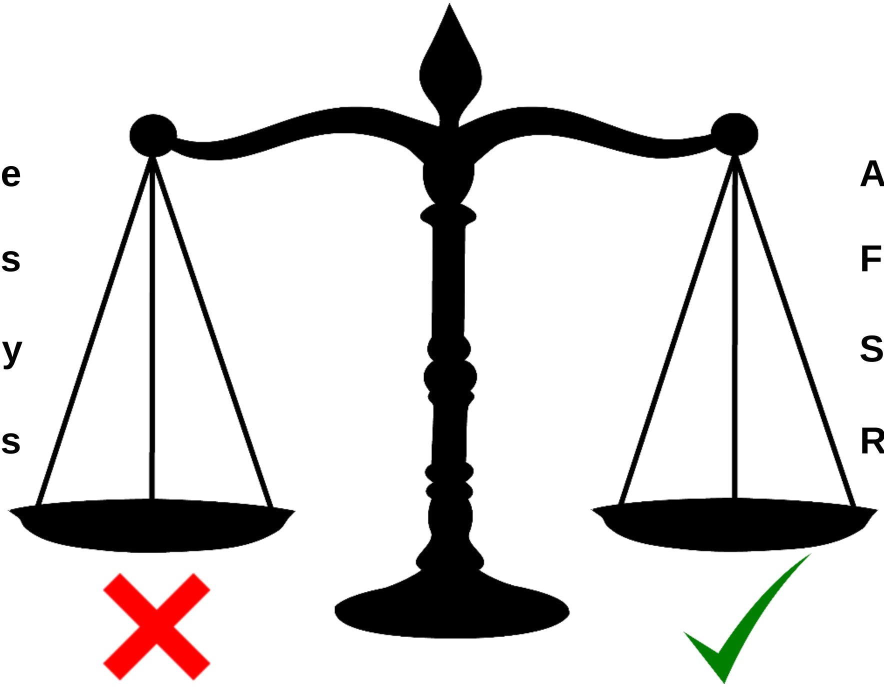
Advanced DDoS Mitigation

Fine-granular Flow Control

Scalable Security Solutions

Reduced Management Efforts

# Conclusion



Complex Architecture

Fast development rates

New Technology

Large Software Projects

Advanced DDoS Mitigation

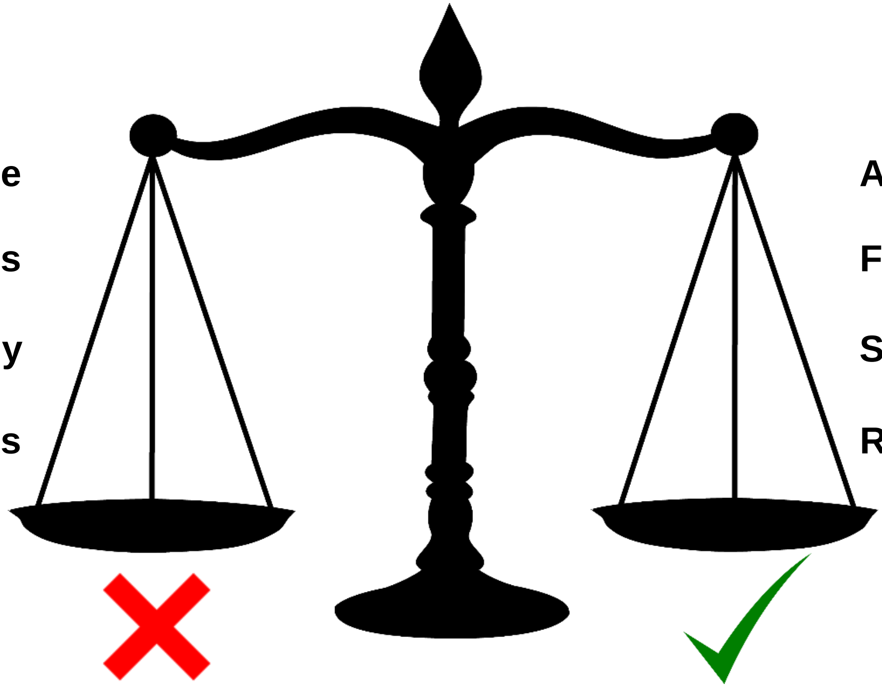
Fine-granular Flow Control

Scalable Security Solutions

Reduced Management Efforts

- Both sides of the scale need to be addressed

# Conclusion



Complex Architecture

Fast development rates

New Technology

Large Software Projects

Advanced DDoS Mitigation

Fine-granular Flow Control

Scalable Security Solutions

Reduced Management Efforts

- Both sides of the scale need to be addressed
- In our opinion the benefits will outweigh the challenges
  - Tight integration of quality assurance in the deployment stage
  - Adaptation of software testing methods to the networking domain

# Sources

- Michael Jarschel, Thomas Zinner, Tobias Hoßfeld, Phuoc Tran-Gia, Wolfgang Kellerer,
  **Interfaces, Attributes, and Use Cases: A Compass for SDN**,
  *IEEE Communications Magazine, 52, 2014*
- Gebert, S., Zinner, T., Gray, N., Durner, R., Lorenz, C., Lange, S.,
  **Demonstrating a Personalized Secure-By-Default Bring Your Own Device Solution Based on Software Defined Networking,**
  *International Teletraffic Congress (ITC 28), 2016*
- Lorenz, C., Hock, D., Scherer, J., Durner, R., Kellerer, W., Gebert, S., Gray, N., Zinner, T., Tran-Gia, P.,
  **An SDN/NFV-enabled Enterprise Network Architecture Offering Fine-Grained Security Policy Enforcement,**
  *IEEE Communications Magazine. 55, 217 - 223 (2017)*
- Gray, N., Lorenz, C., Müssig, A., Gebert, S., Zinner, T., Tran-Gia, P.,
  **A Priori State Synchronization for Fast Failover of Stateful Firewall VNFs,**
  *Workshop on Software-Defined Networking and Network Function Virtualization for Flexible Network Management, SDNFlex 2017*
- Pfaff B., Scherer J., Hock D., Gray N., Zinner T., Tran-Gia P., Durner R., Kellerer R., Lorenz C.,
  **SDN/NFV-enabled Security Architecture for Fine-grained Policy Enforcement and Threat Mitigation for Enterprise,**
  *ACM SIGCOMM Computer Communication Review*, *2017*