Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

Institute of Computer Science
Chair of Communication Networks
Prof. Dr.-Ing. P. Tran-Gia

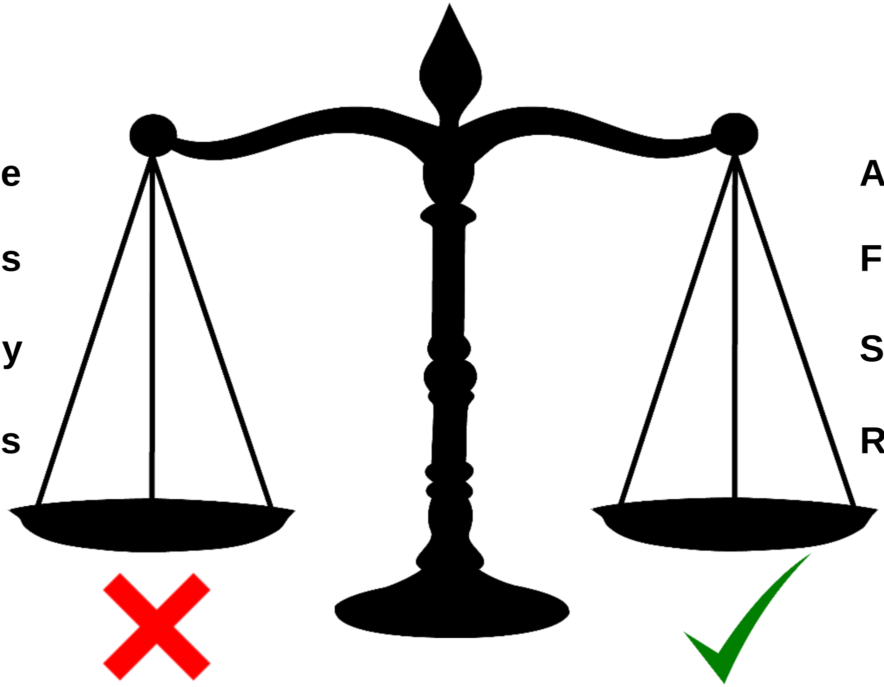
Security in Softwarized Networks: Prospects and Challenges

Nicholas Gray, Thomas Zinner, Phuoc Tran-Gia

comnet.informatik.uni-wuerzburg.de

sardine-project.org

Motivation



Complex Architecture

Fast development rates

New Technology

Large Software Projects

Advanced DDoS Mitigation

Fine-granular Flow Control

Scalable Security Solutions

Reduced Management Efforts

- Average cost of data breach $3.62 million (IBM)
- Cloud infrastructure is the next frontier for cyber crime (Symantec)
- Nation-state cyber attacks change the security game (Microsoft)

→ **Both sides of the scale need to be addressed**

Agenda

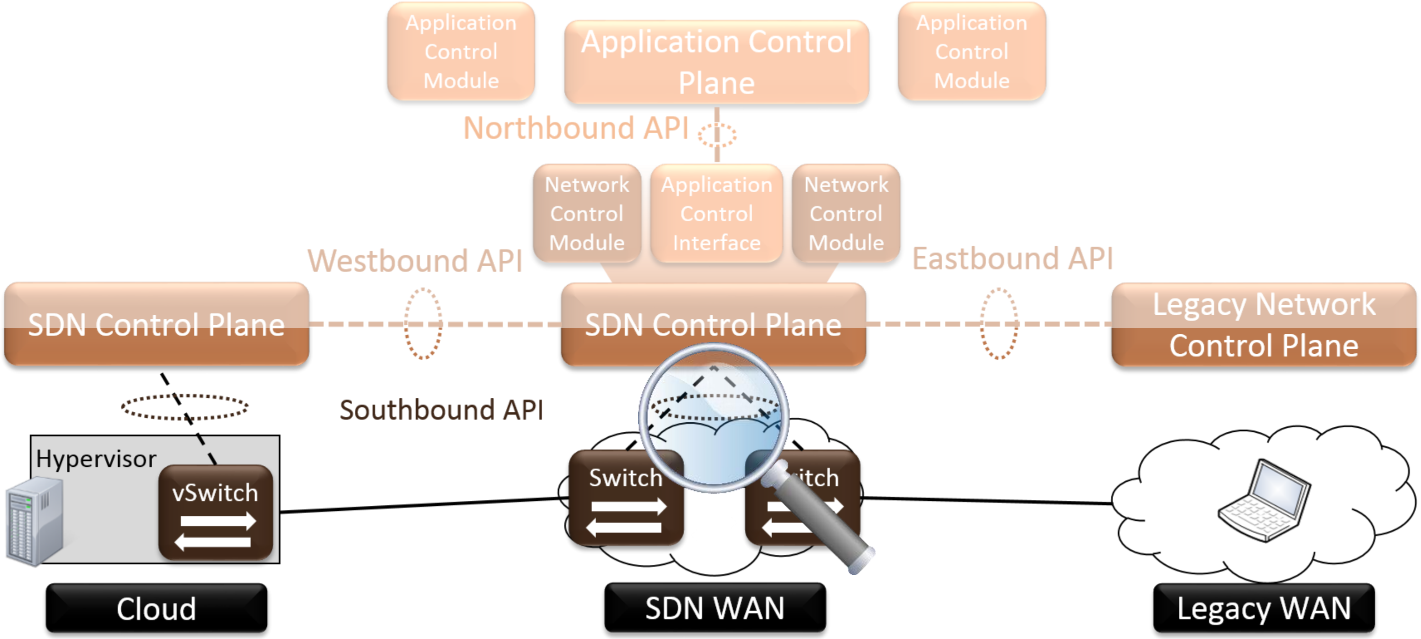
- Overview of the SDN Attack Surface
- Fuzzing as Quality Assurance Technique
- Omni-present SDN Firewall

OVERVIEW OF THE SDN ATTACK SURFACE

SDN Attack Surface

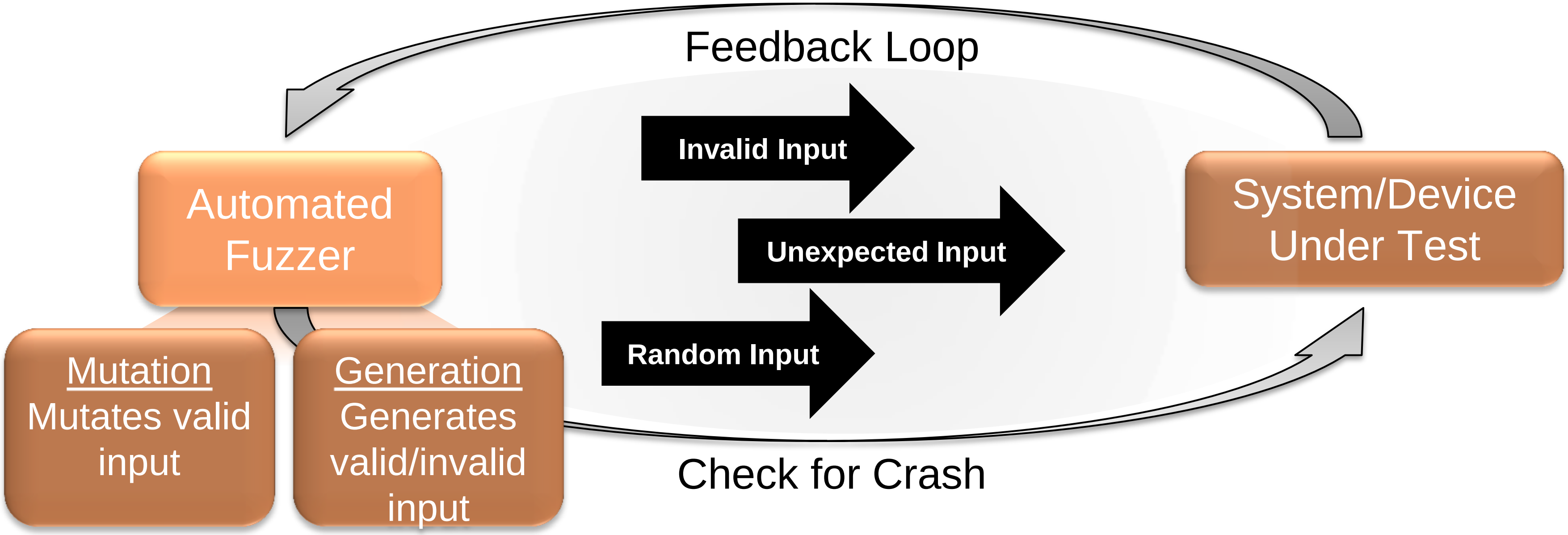
SDN Attack Surface

One compromised component is enough to take down the whole system



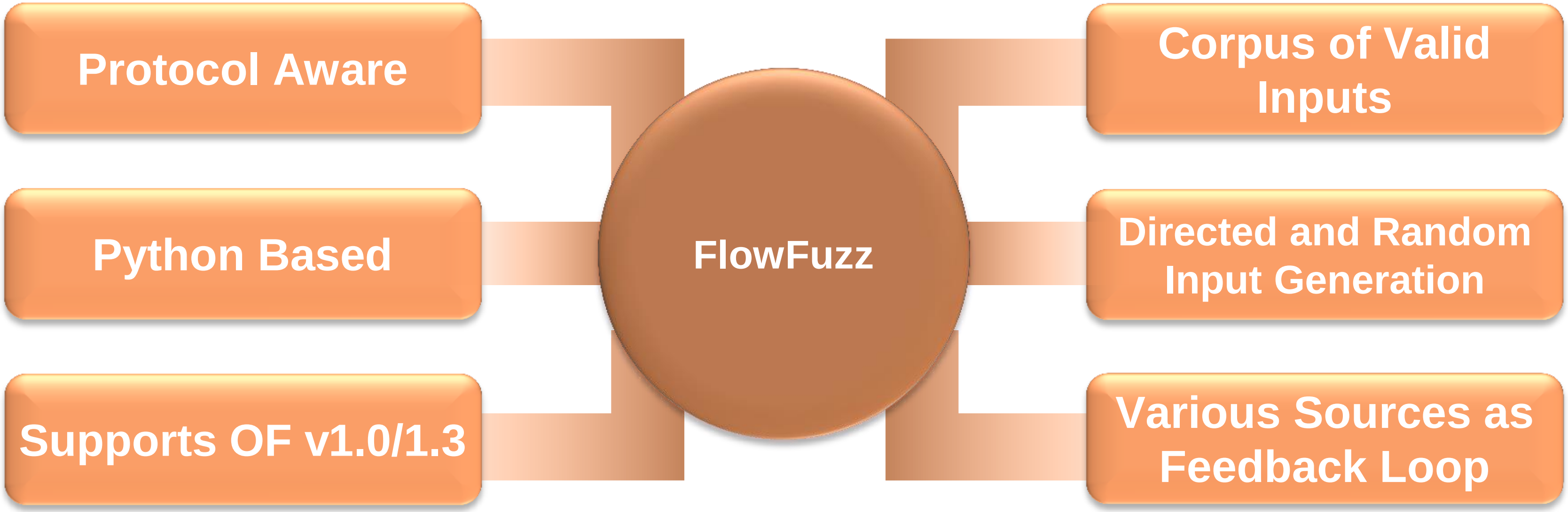
FUZZING AS QUALITY ASSURANCE TECHNIQUE

Fuzzing as Proactive Security Testing Technique



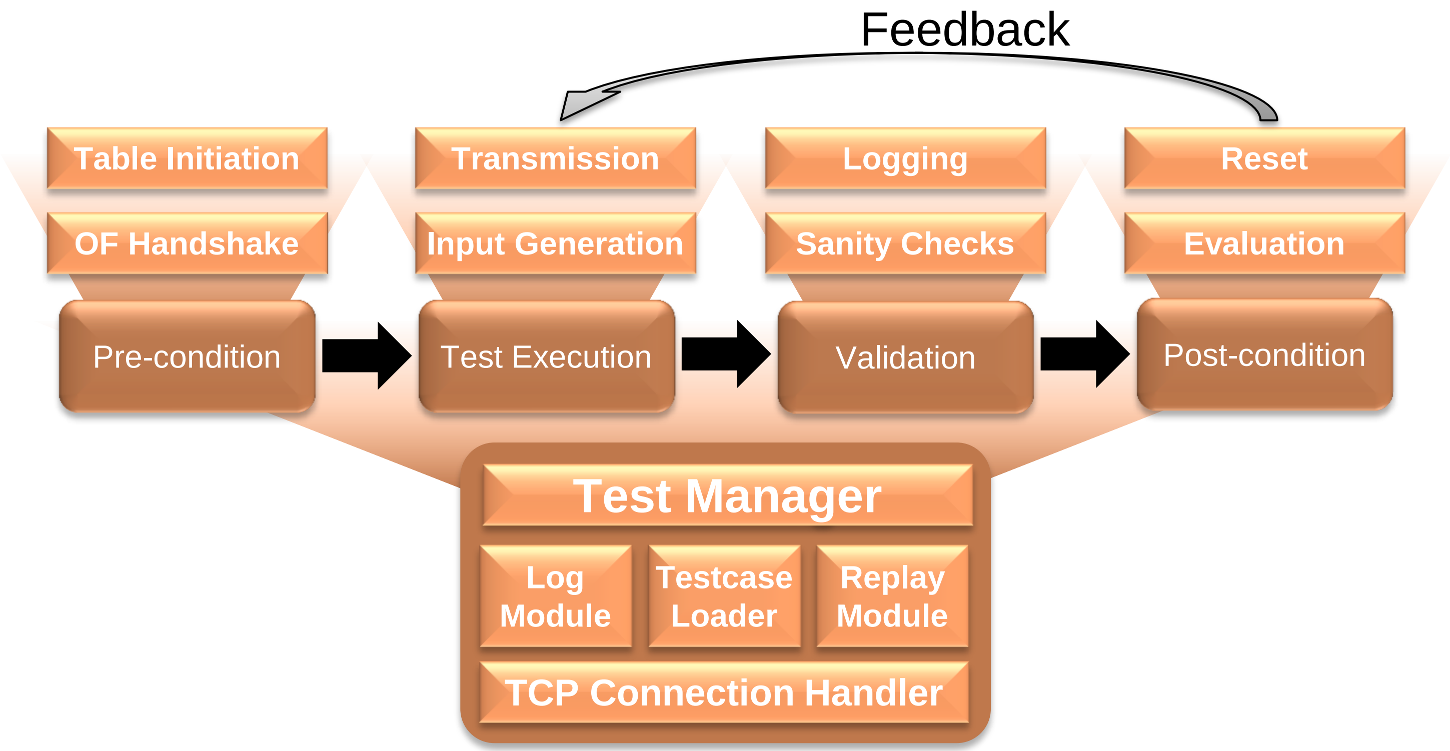
- Automated proactive software testing technique
- Proven method for uncovering unknown security vulnerabilities (Heartbleed, Crazy bad, Shellshock …)
- Feedback Loop is vital for efficient input generation

FlowFuzz – Core Features



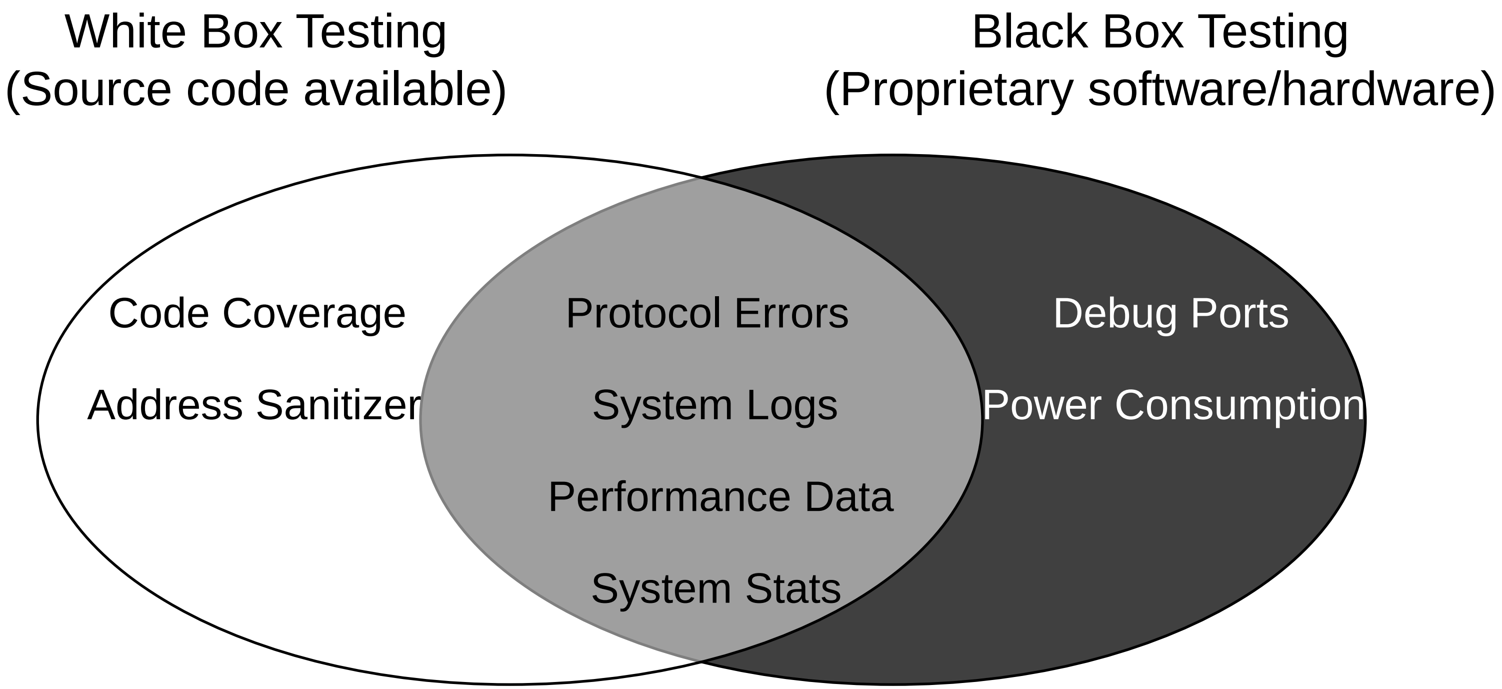
- Full featured fuzzing framework
- Specialized for OpenFlow-enabled software/hardware switches

FlowFuzz - Architecture



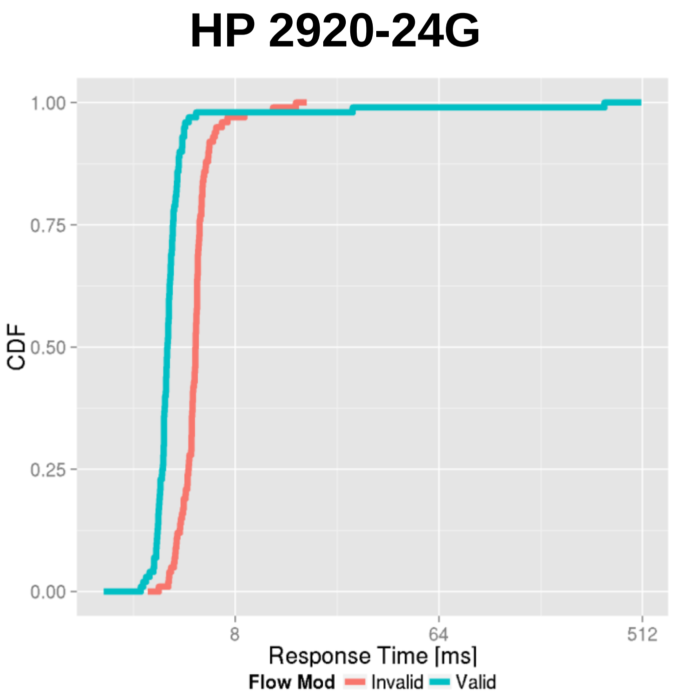
- Modular design allows for fast and custom adaptations
- Selection of modules is configurable to best fit the use case

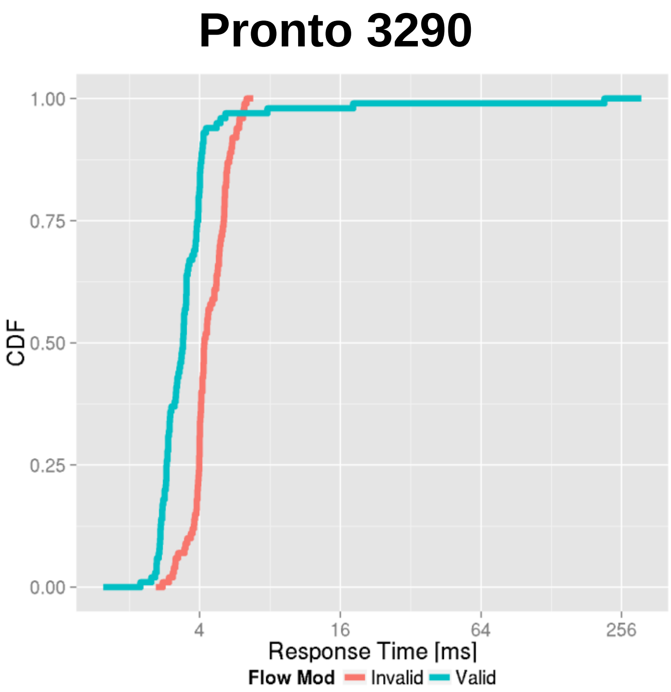
FlowFuzz - Feedback Sources



- Use case specific selection of feedback sources
- Adjustable weights of sources during the evaluation stage
- All sources are combined to fingerprints to reflect the test paths

Feedback Sources – Evaluation of Response Times

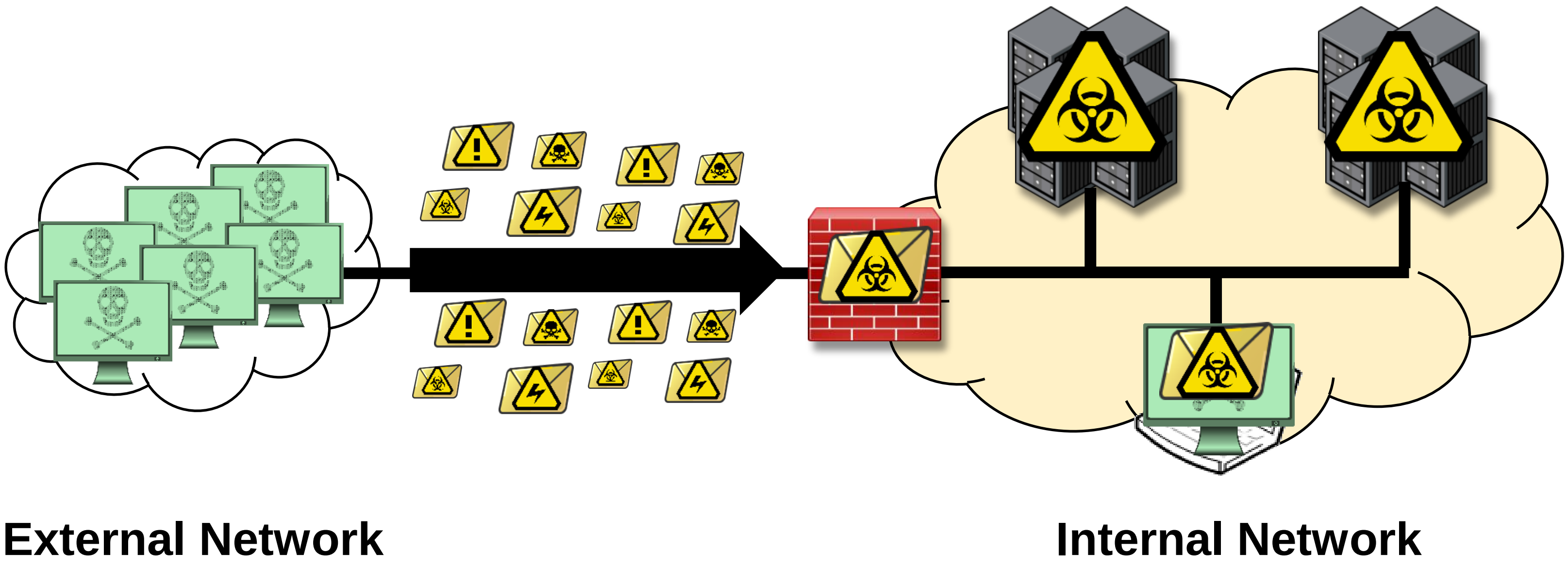




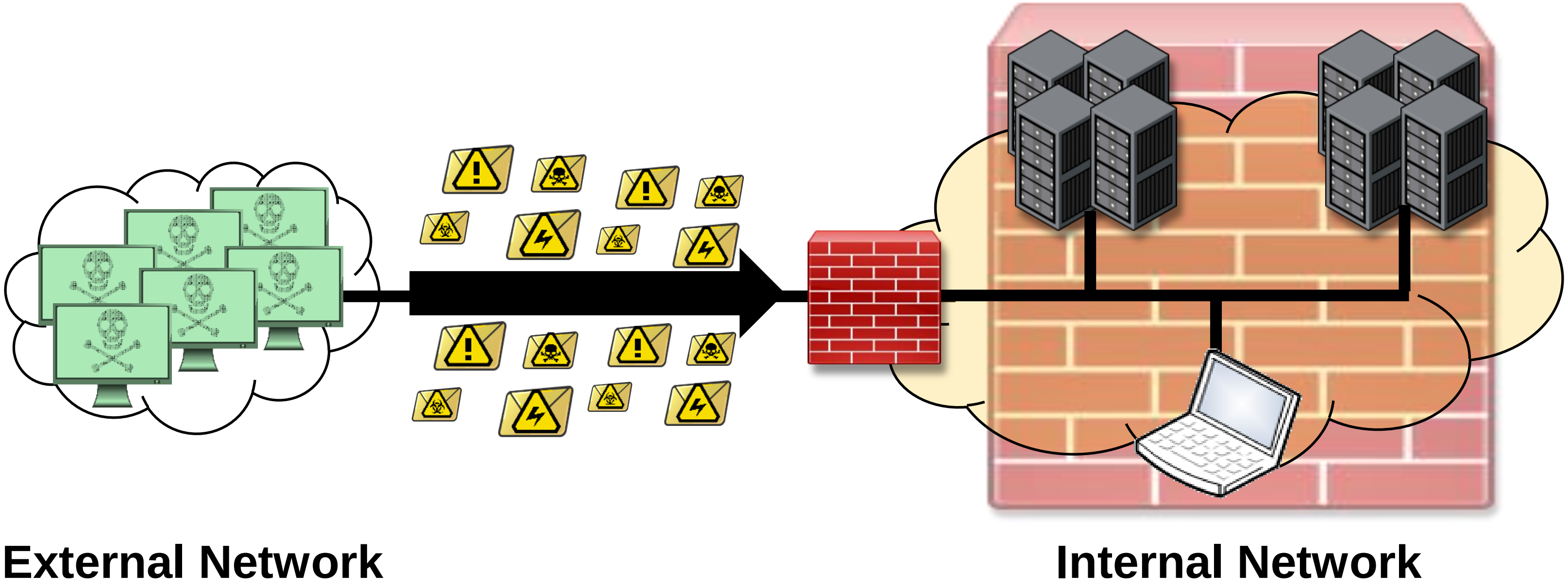
- Response times reflect execution of different code segments
- Baseline measurement is required per device and firmware

OMNI-PRESENT SDN FIREWALL

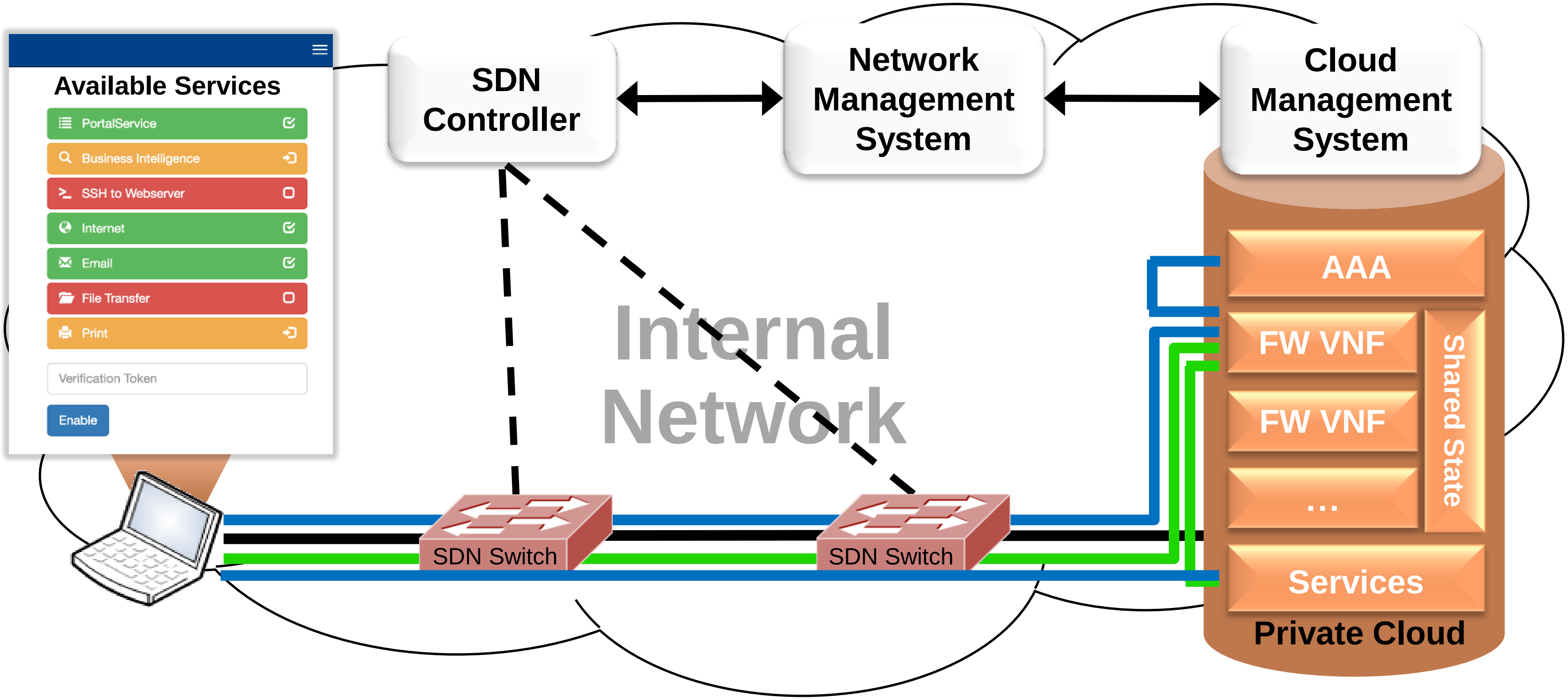
Can we enhance network security with SDN?



Can we enhance network security with SDN?



SDN Omni-present Firewall

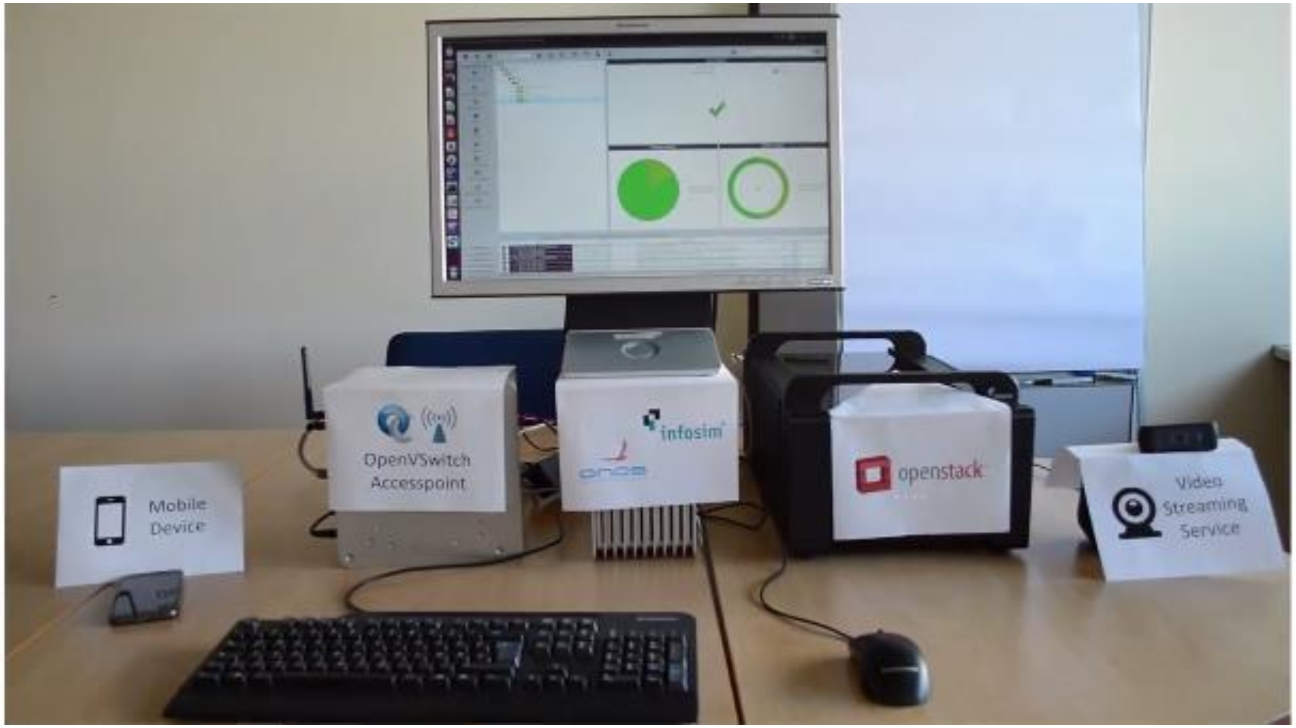


Available Services

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

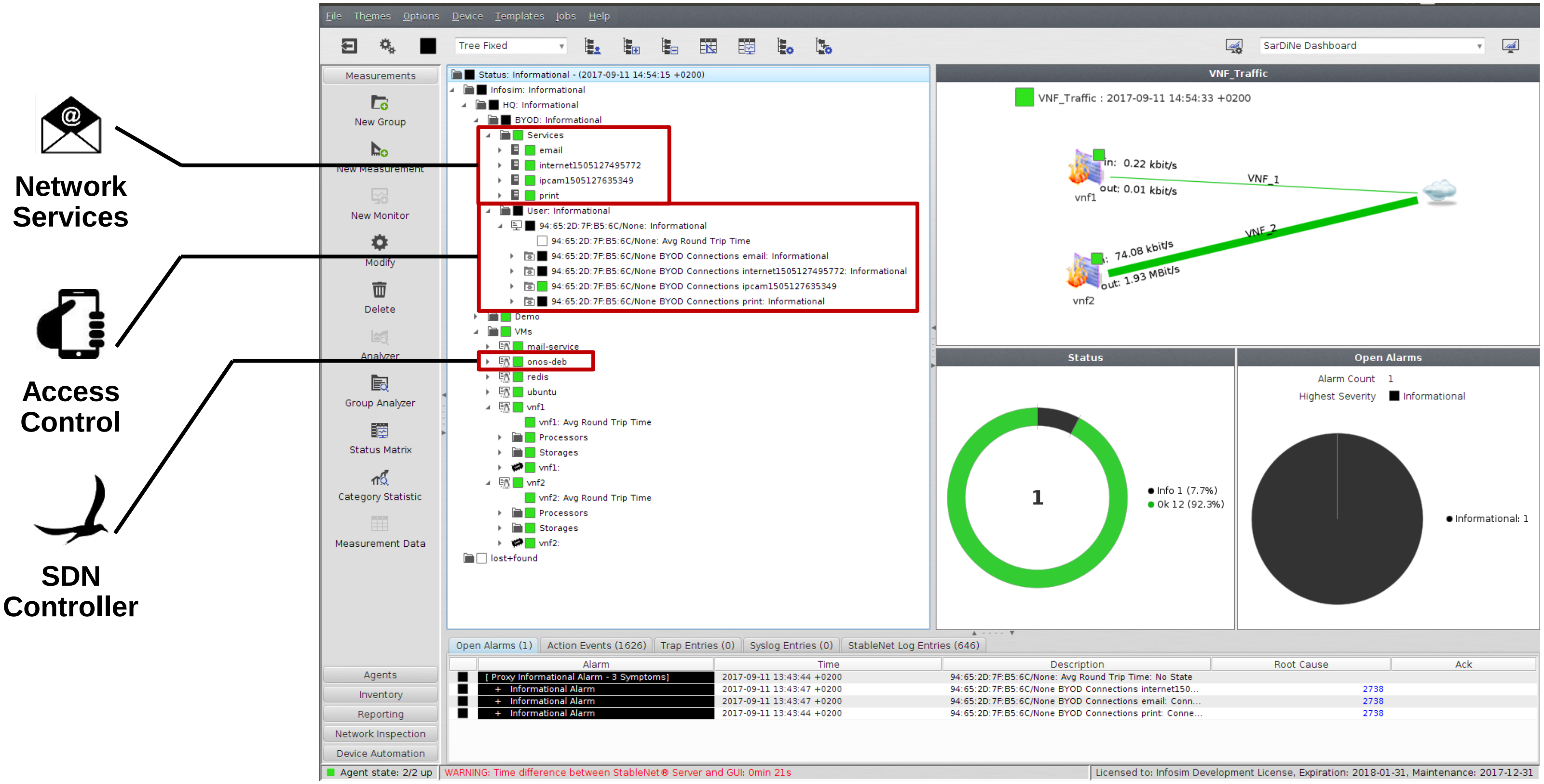
Verification Token

Demo Setup



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

Fine-granular Access Control



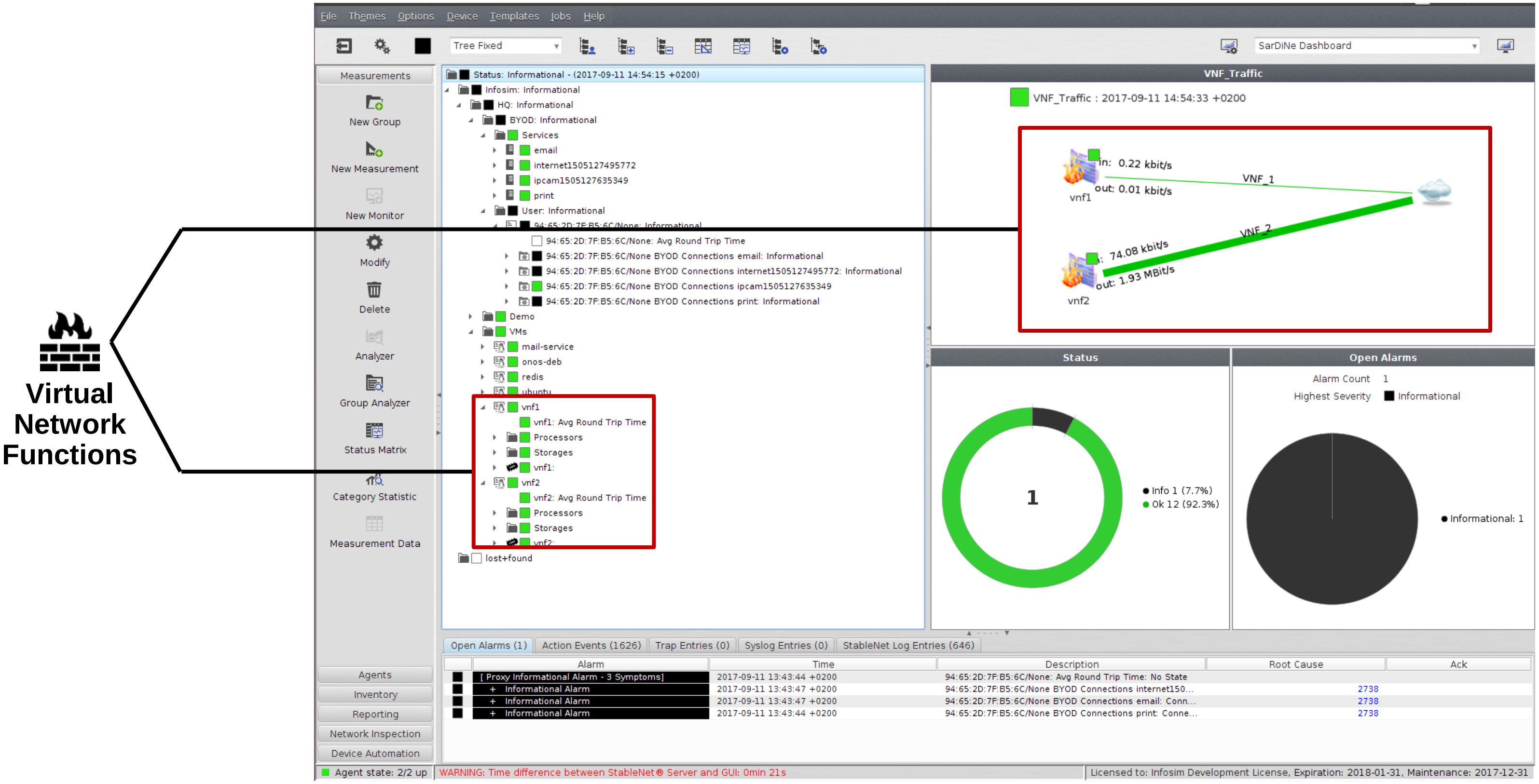
```
Status: Informational - (2017-09-11 14:54:15 +0200)
  Infosim: Informational
    HQ: Informational
      BYOD: Informational
        Services
          email
          internet1505127495772
          ipcam1505127635349
          print
        User: Informational
          94:65:2D:7F:B5:6C/None: 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
```

	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	

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
```

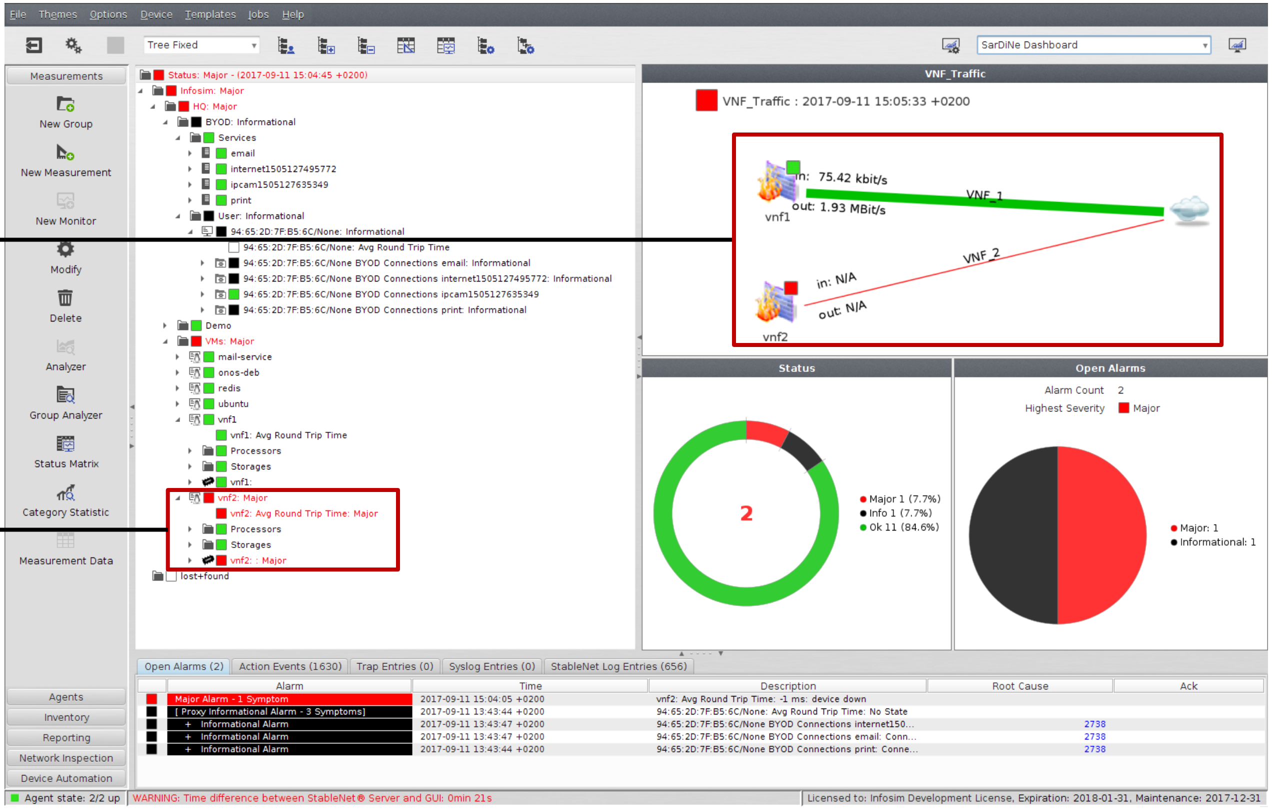
Open Alarms (1) | Action Events (1626) | Trap Entries (0) | Syslog Entries (0) | StableNet Log Entries (646)

	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)

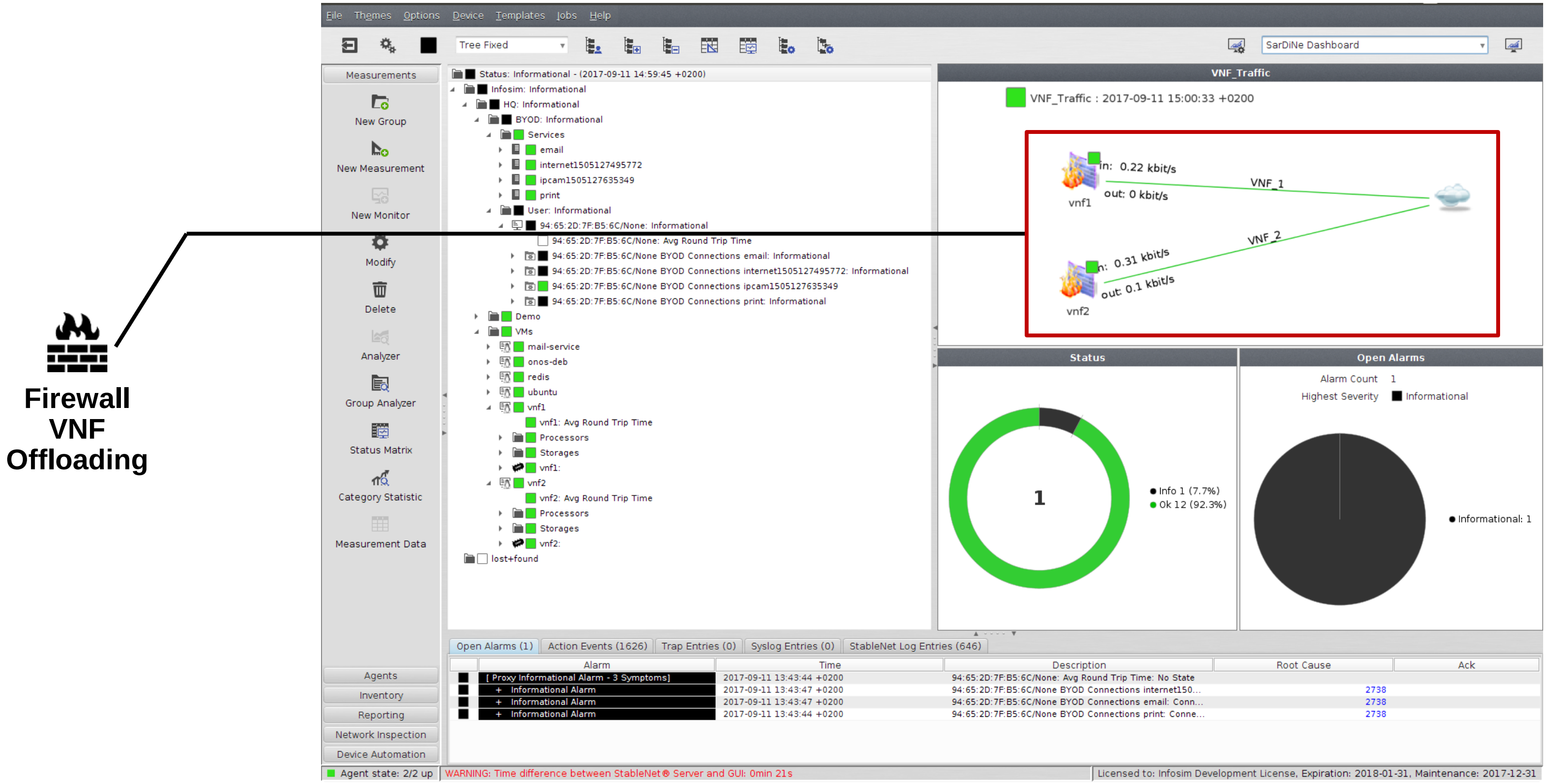
	Alarm	Time	Description	Root Cause	Ack
🟥	Major Alarm - 1 Symptom	2017-09-11 15:04:05 +0200	vnf2: Avg Round Trip Time: -1 ms: device down		
■	[Proxy Informational Alarm - 3 Symptoms]	2017-09-11 13:43:44 +0200	94:65:2D:7F:B5:6C/None: Avg Round Trip Time: No State		
■	+ Informational Alarm	2017-09-11 13:43:47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

- SDN provides new opportunities but also introduces new risks

- 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

- Related Talks and Publications
  - FlowFuzz - A Framework for Fuzzing OpenFlow-Enabled Software and Hardware Switches, Black Hat USA 2017
  - SDN/NFV-enabled Security Architecture for Fine-grained Policy Enforcement and Threat Mitigation for Enterprise Networks, SIGCOMM 2017