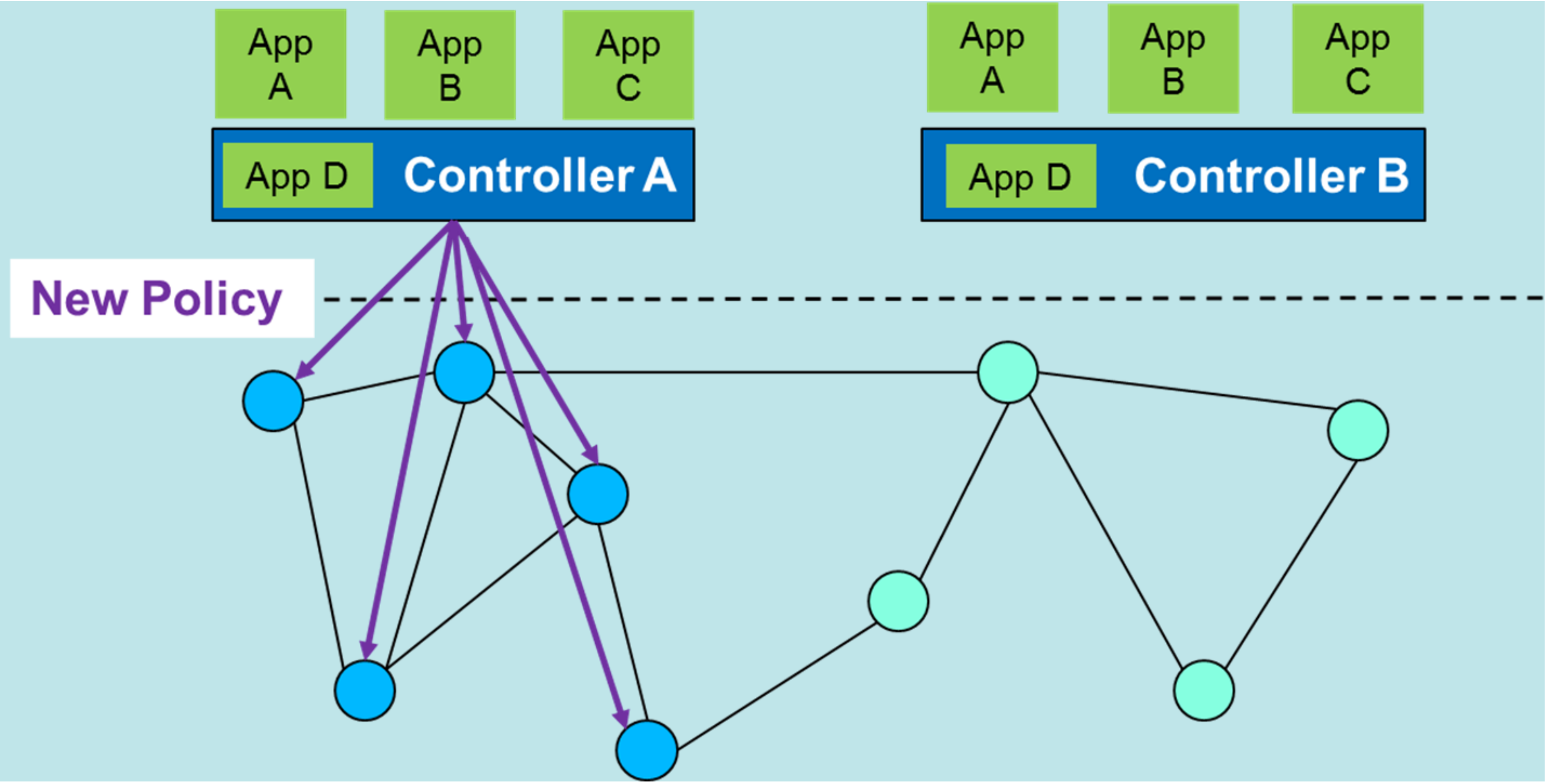
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

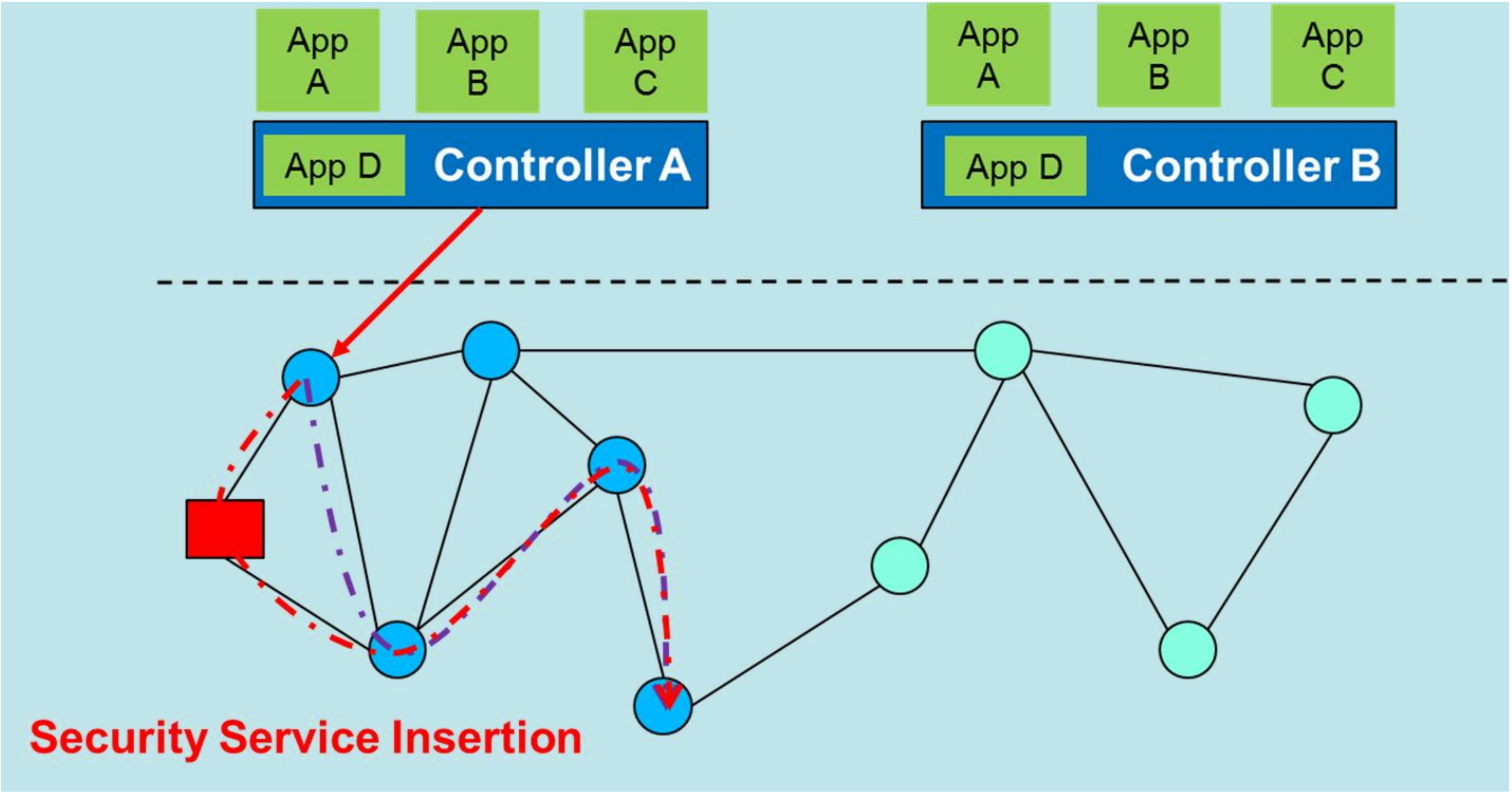
NETWORK SECURITY ENHANCEMENTS USING SDN

SDN Security Enhancements



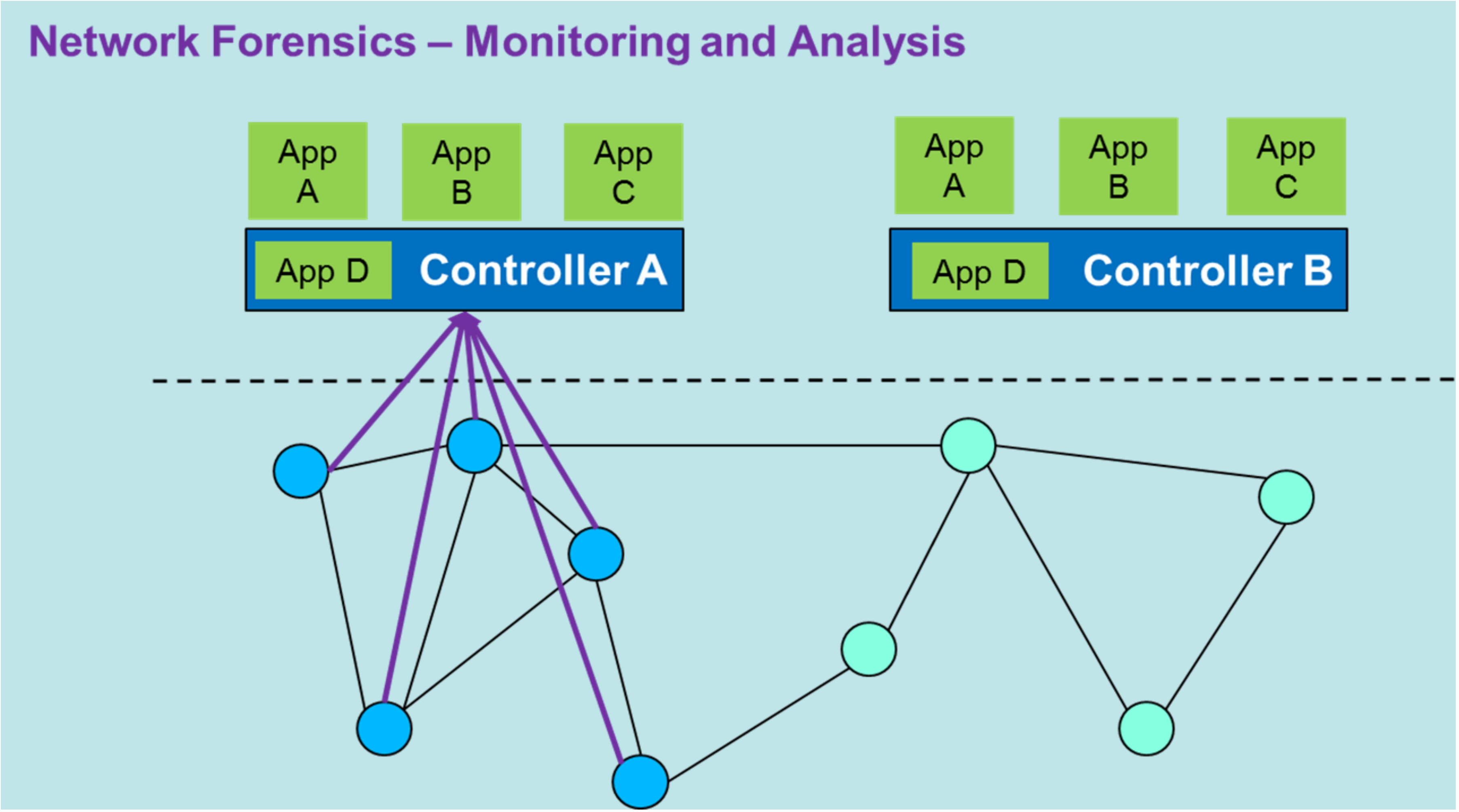
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

SDN Security Enhancements



CENTRE FOR SECURE INFORMATION TECHNOLOGIES

SDN Security Enhancements



CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Categorization of Security Enhancements

Security Enhancement	Research Work	SDN Layer/Interface				
		App	App-Ctl	Ctl	Ctl-Data	Data
Collect, Detect, Protect	Combining OpenFlow/sFlow [88], Active Security [89]	✓		✓	✓	✓
	Learning-IDS (L-IDS) [90], NetFuse [91], OrchSec [92]	✓		✓	✓	✓
	Cognition [93]	✓	✓	✓		
Traffic Analysis & Rule Updating	Resonance [94]	✓		✓	✓	✓
	AVANT-GUARD [55], Pedigree [95], OF-RHM [96]			✓	✓	✓
	SDN-MTD [97]	✓		✓	✓	✓
	NICE:NIDS [98], SnortFlow [99], SDNIPS [100], ScalableIDS [101]	✓		✓	✓	
	Revisiting Anomaly Detection [102]	✓		✓	✓	
	Fuzzy Logic SDN IDS [103]	✓		✓	✓	✓
DoS/DDoS Protection	Lightweight DDoS [104]	✓		✓	✓	
	CONA [105], DDoS Defender [106], DDoS Blocker [107]	✓		✓	✓	✓
Security Middleboxes - Architectures and Services	Slick [108], FlowTags [109]	✓	✓	✓	✓	✓
	SIMPLE-fying Middlebox [110]	✓		✓		✓
	OSTMA [111]			✓	✓	✓
	Covert Channel Protection [112]	✓		✓	✓	✓
	OpenSAFE [113], CloudWatcher [114]	✓	✓	✓	✓	
	Secure-TAS [115]				✓	✓
	Secure Forensics [116]			✓	✓	✓
AAA	AAA SDN [117]			✓	✓	✓
	C-BAS [118]	✓	✓	✓	✓	✓
Secure, Scalable Multi-Tenancy	vCNSMS [119], OpenvNMS [120], Tualatin [121]	✓		✓	✓	✓
	NetSecCloud [122]	✓		✓		

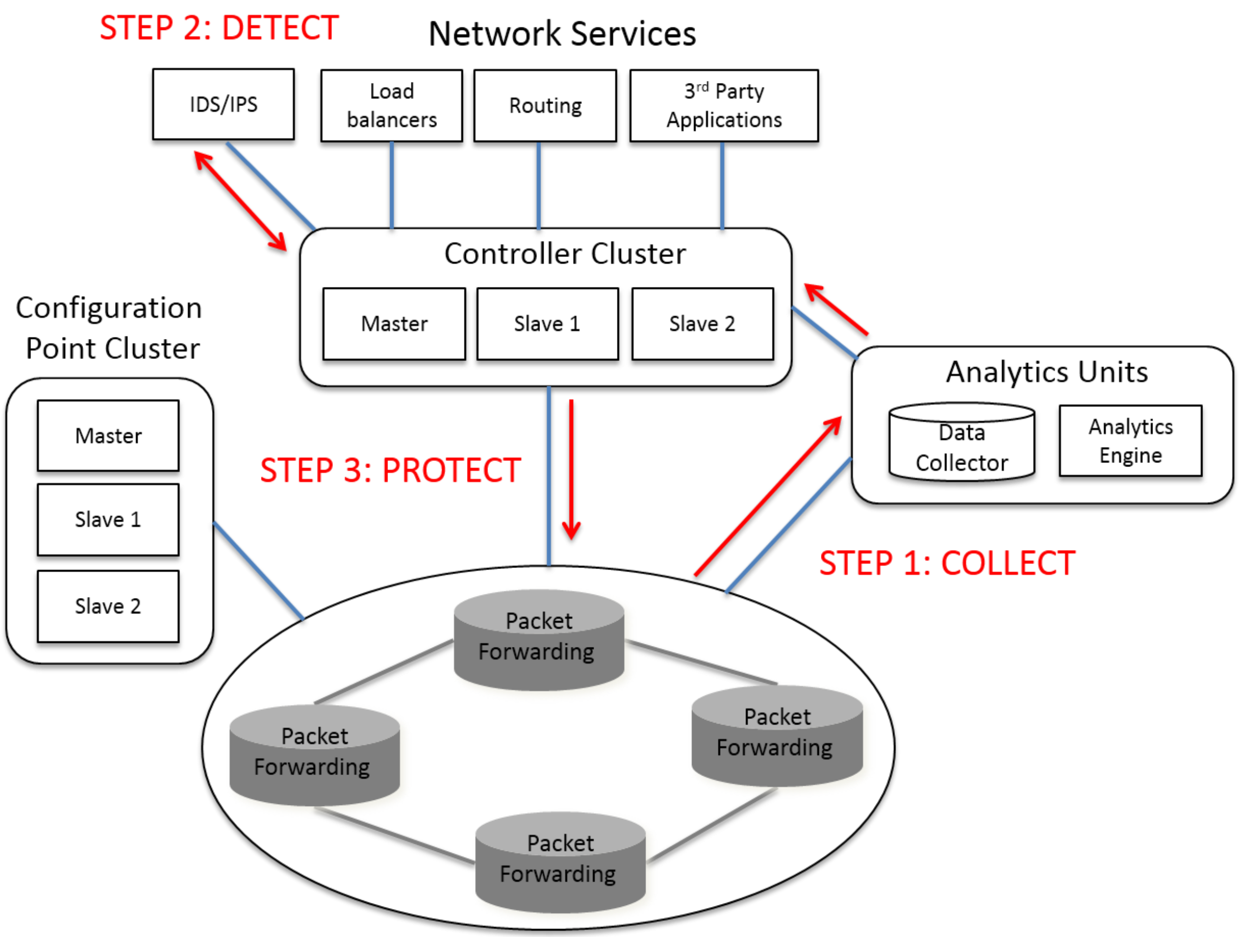
CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES

SDN Security Feedback Control

Step 1: Collect Network Statistics

Step 2: Detect anomalies or intrusions in the network

Step 3: Insert flow rules to protect the network



CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

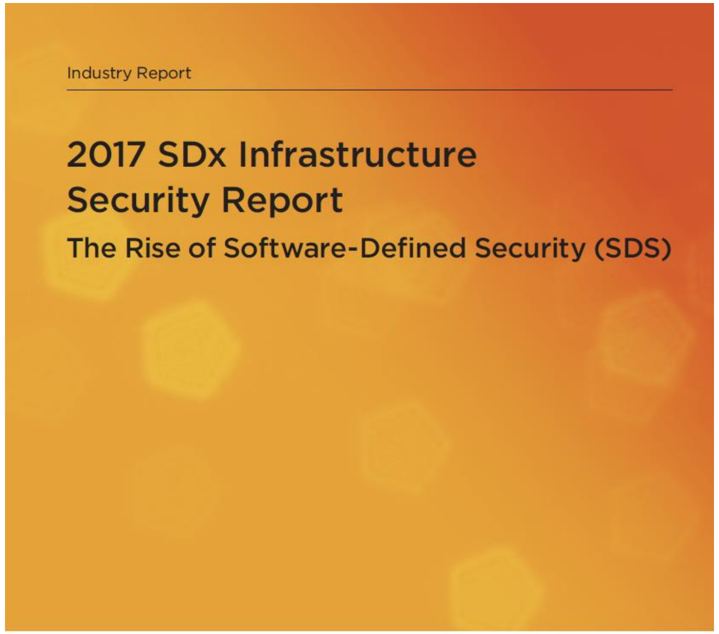
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

SDN MONITORING AND SECURITY APPLICATIONS

SDx Central Infrastructure Security Report (2017)

Four top security challenges:

- Effectiveness of security solutions at scale,
- Challenges in securing IoT devices,
- Lack of visibility, and
- Manageability of security solutions at scale.


Industry Report

2017 SDx Infrastructure Security Report

The Rise of Software-Defined Security (SDS)

sdx central®

The Trusted News and Resource Site for SDx, SDN, NFV, Cloud and Virtualization Infrastructure

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Distributed SDN Framework for Scalable Network Security

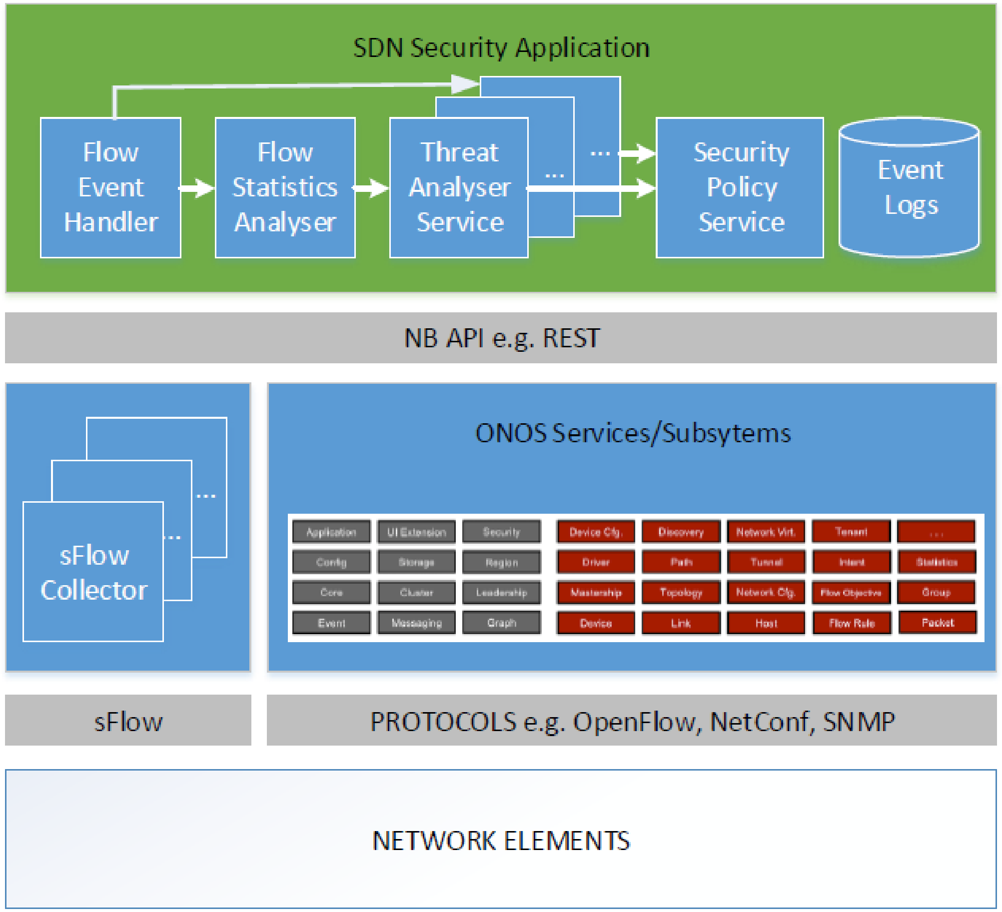
SecApp Project, 2016 - 2018

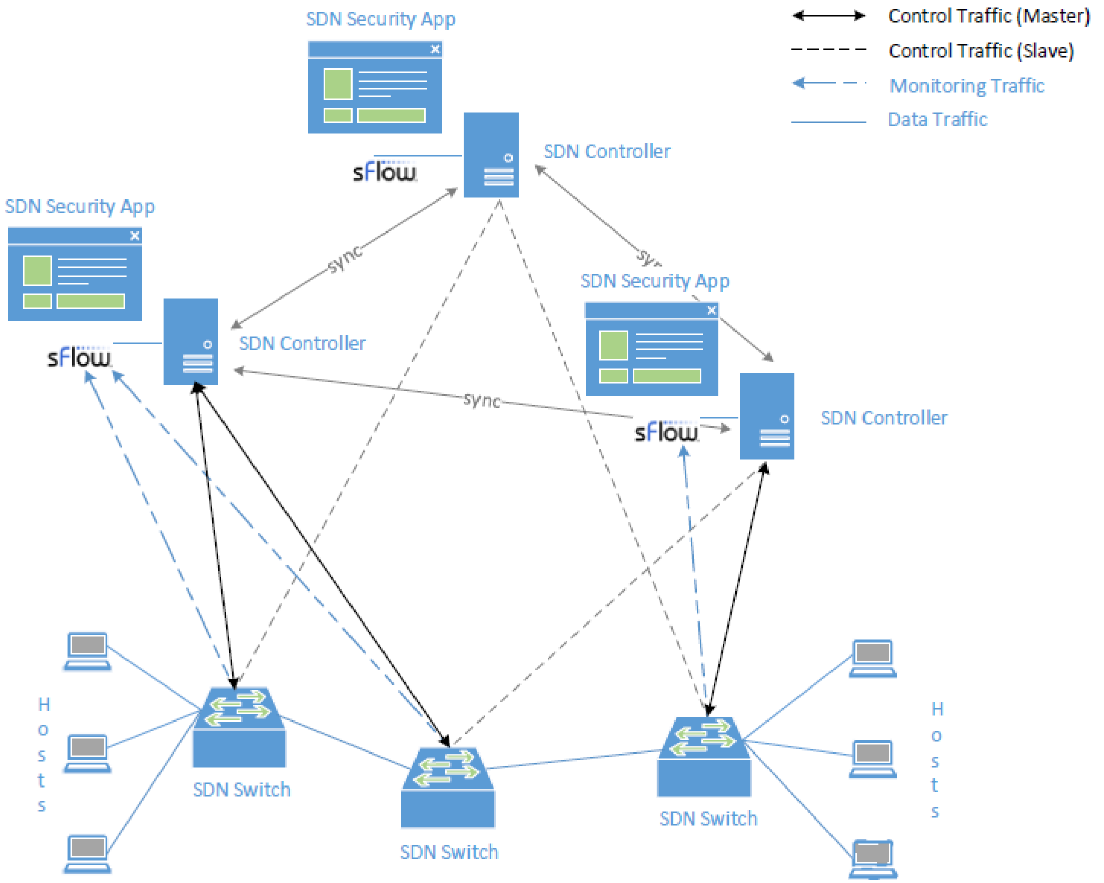
Objectives:

- To monitor and contribute to advancing the state-of-the-art in SDN-based monitoring and attack detection and protection.
- To design a SDN security application for traffic monitoring in an SDN combined with threat analysis and security policy generation.
- To exploit the full potential of the SDN framework to design and develop a distributed, controller-independent, scalable security application.

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

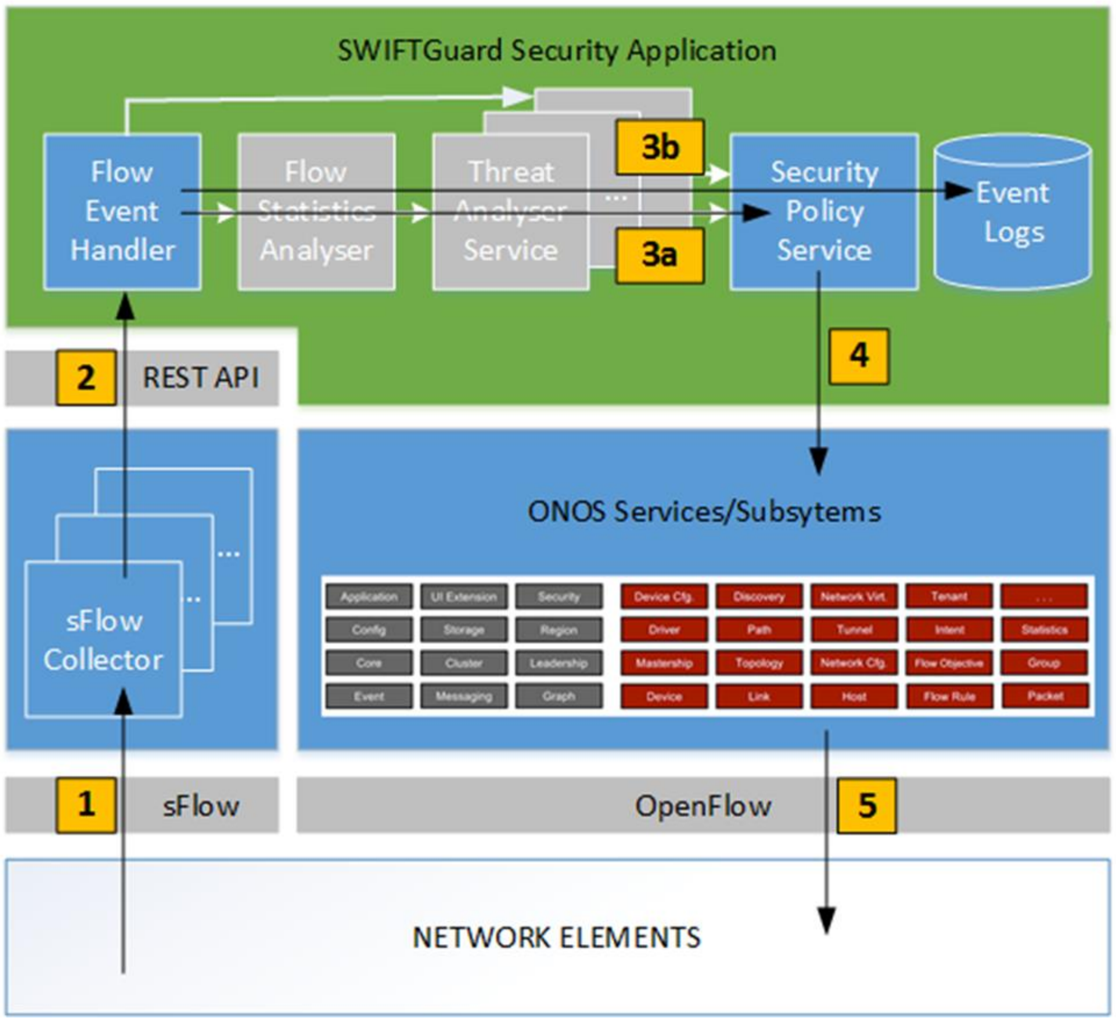
SWIFTGuard





CENTRE FOR SECURE INFORMATION TECHNOLOGIES

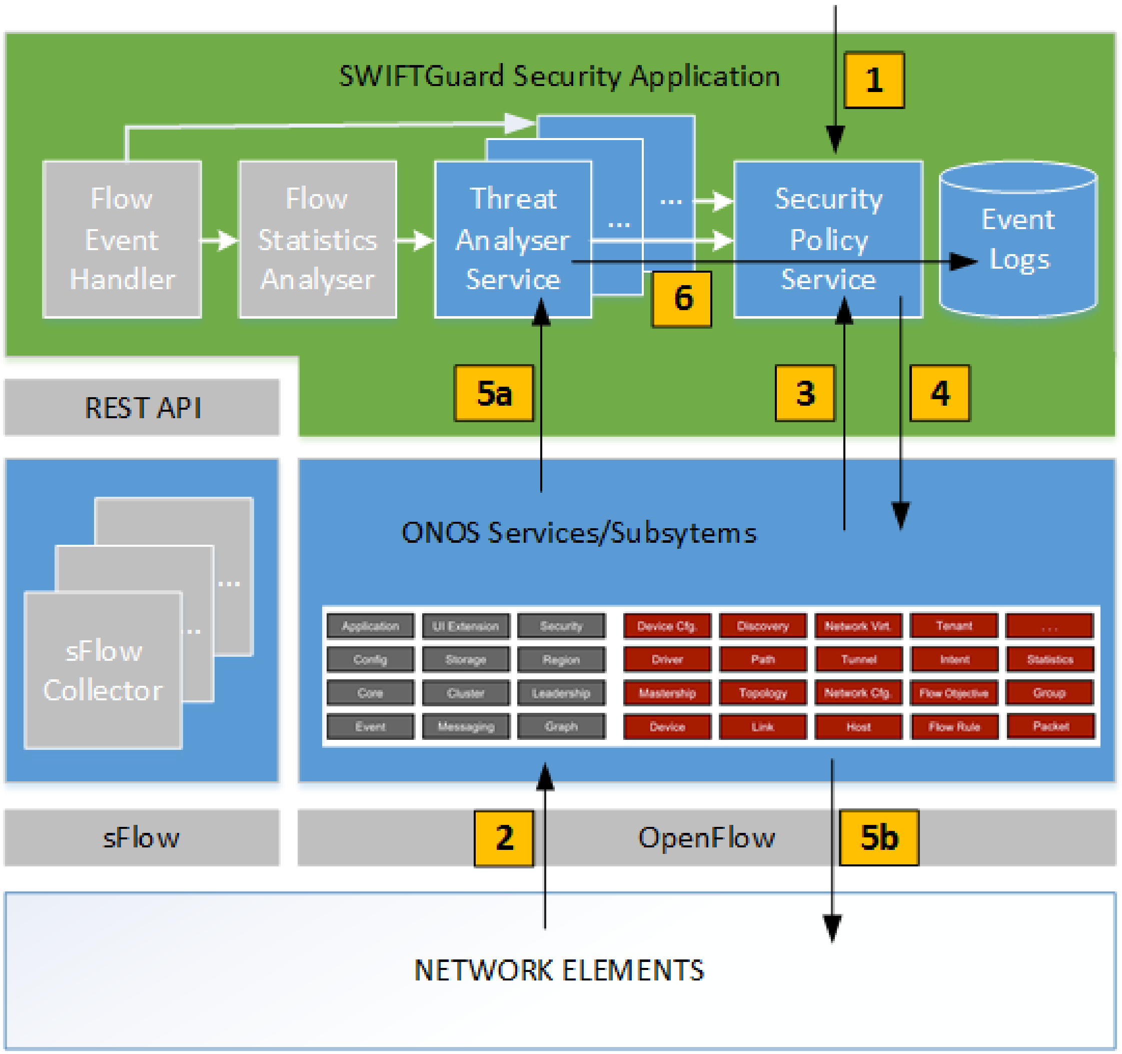
DDoS Detection/Protection



1. sFlow datagrams received by sFlowRT
2. DDoS event detected and sent to SWIFTGuard using RESTful API
3. Security policy generated by SWIFTGuard and event logged
4. Security policy received by ONOS flow rule subsystem
5. OpenFlow rules sent by ONOS to network elements

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

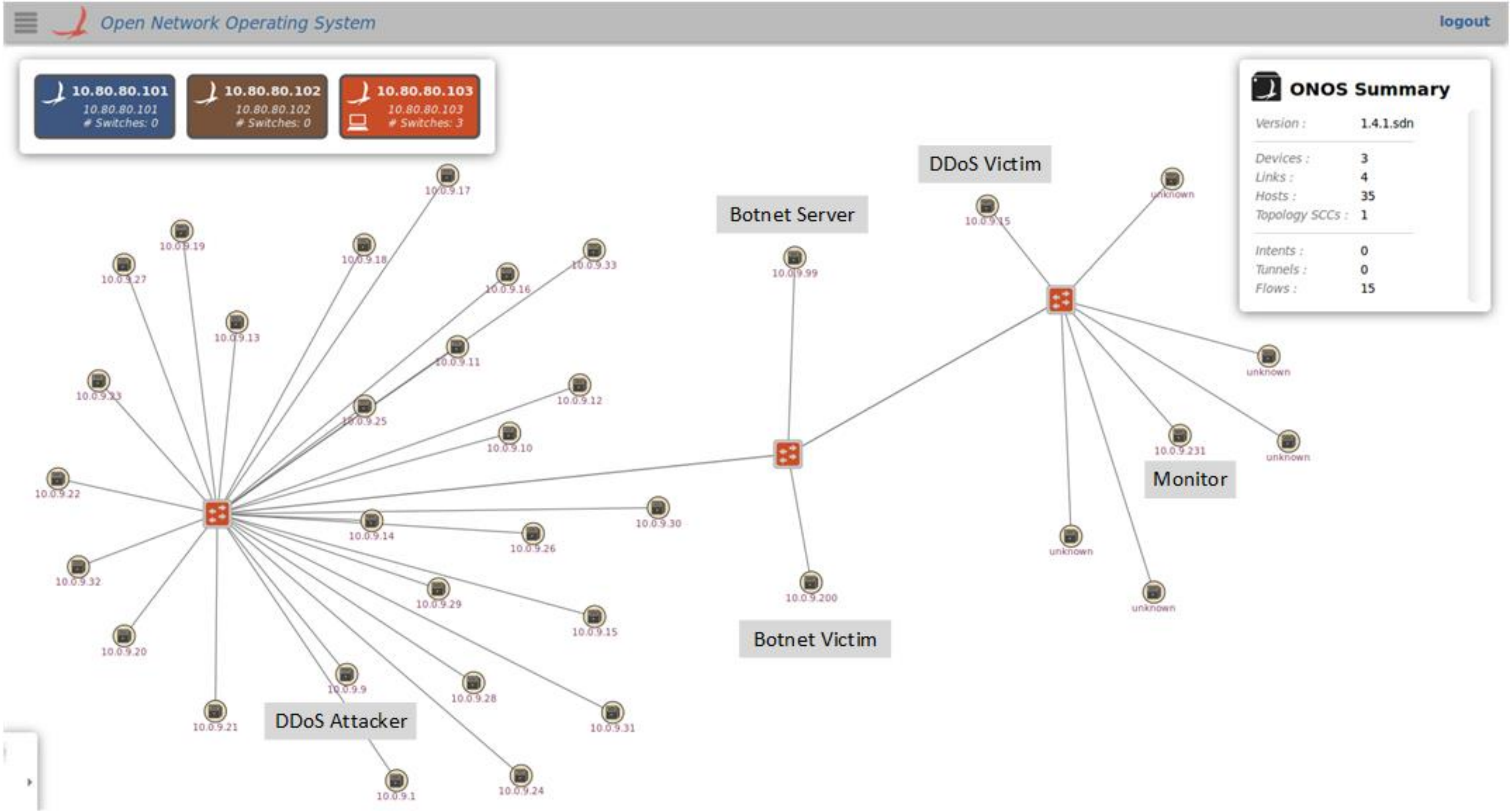
Malicious Host Detection/Traffic Mirroring



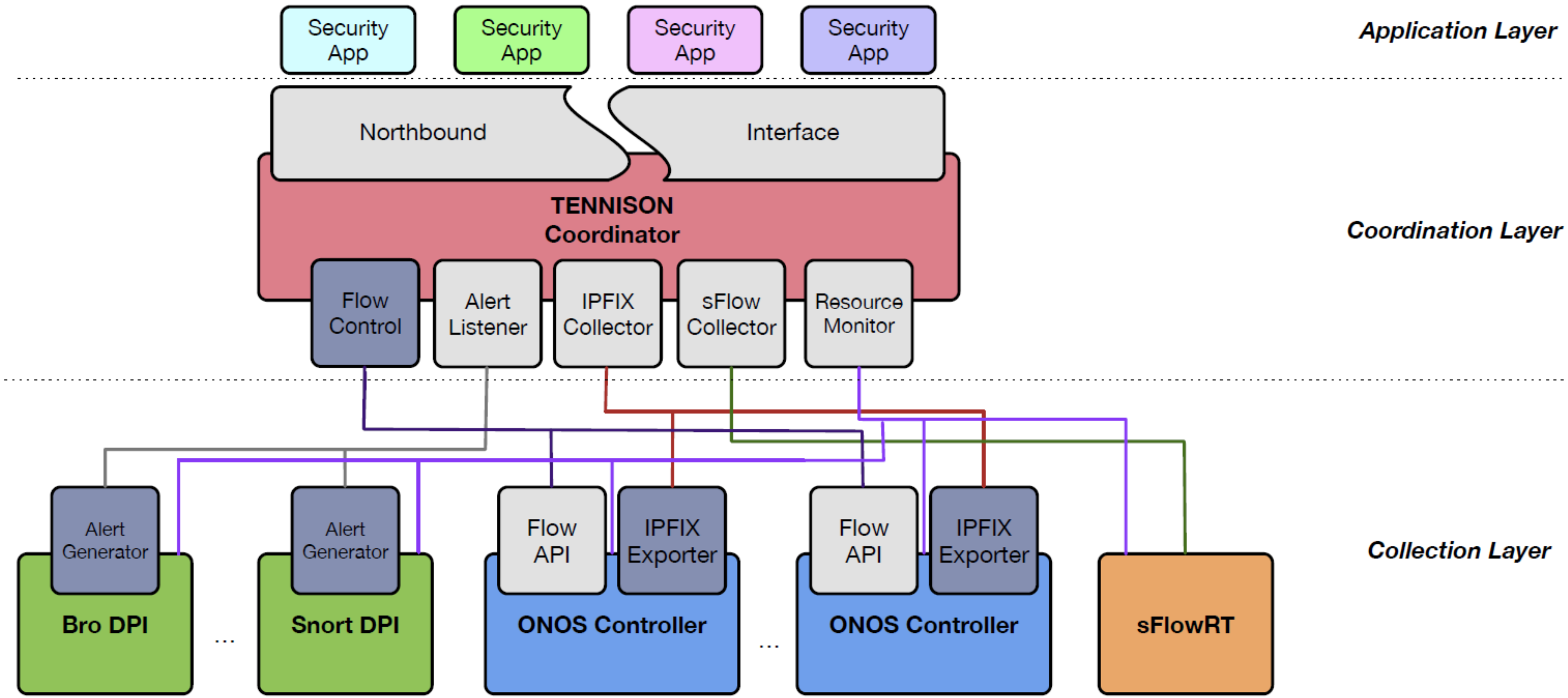
1. IP Monitor/Blacklist loaded to SWIFTGuard
2. Packet_In received by ONOS
3. Packet_In parsed and checked against SWIFTGuard security policy (e.g. monitor/blacklist)
4. Flow rule created to fwd/drop/mirror traffic
5. Packets of flow blocked/dropped/mirrored
6. Event of mirrored traffic logged

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

SWIFTGuard Test Topology



TENNISON monitoring and security framework



Fawcett, L., Scott-Hayward, S., Broadbent, M., Wright, A. and Race, N. "TENNISON: A distributed SDN framework for scalable network security", Submitted to: *IEEE JSAC Special Issue on Scalability Issues and Solutions for Software Defined Networks*, March 2018.

NFV SECURITY

ETSI NFV Security Documents

Work Item
SEC001 “NFV Security problem statement”
SEC002 “Openstack security”
SEC003 “NFV Security and Trust Guidelines”
SEC004 “Lawful interception report”
SEC005 “Certificate management report”
SEC006 “Security & regulation report”
SEC007 “NFV attestation report”
SEC008 “Security monitoring report”
SEC009 “Use cases for multi-layer host administration”
SEC010 “NFV retained data”
SEC011 “Lawful interception architecture report”
SEC012 “Architecture for sensitive components”
SEC013 “Security management & monitoring spec.”
SEC014 “MANO security spec.”

Access at: https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/

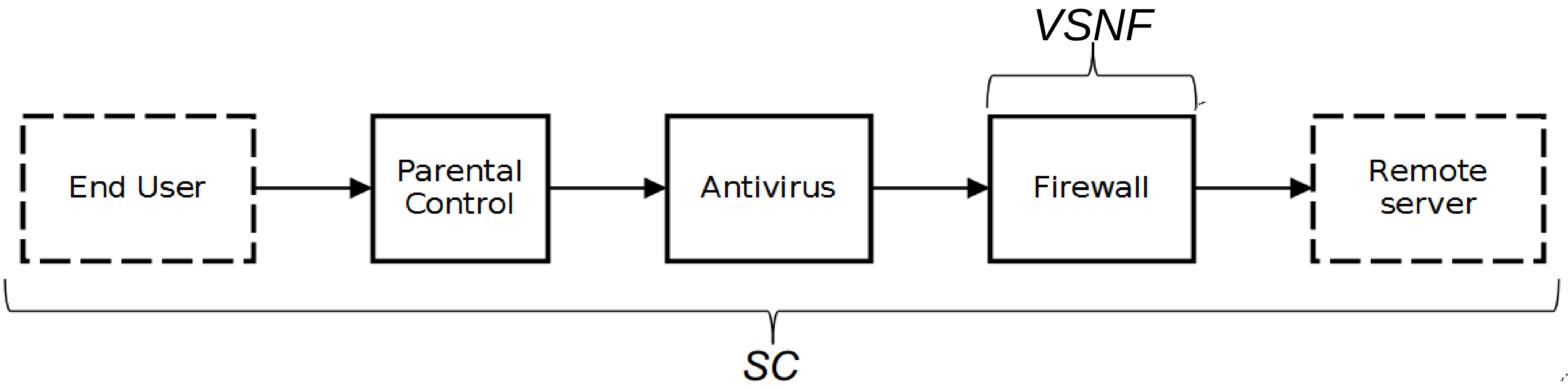
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

APPLICATION-AWARE PROVISIONING OF VIRTUAL SECURITY NETWORK FUNCTIONS

Context

Network security services can be provided to the users by means of chains of **<u>Virtual Security Network Functions (VSNF)</u>**

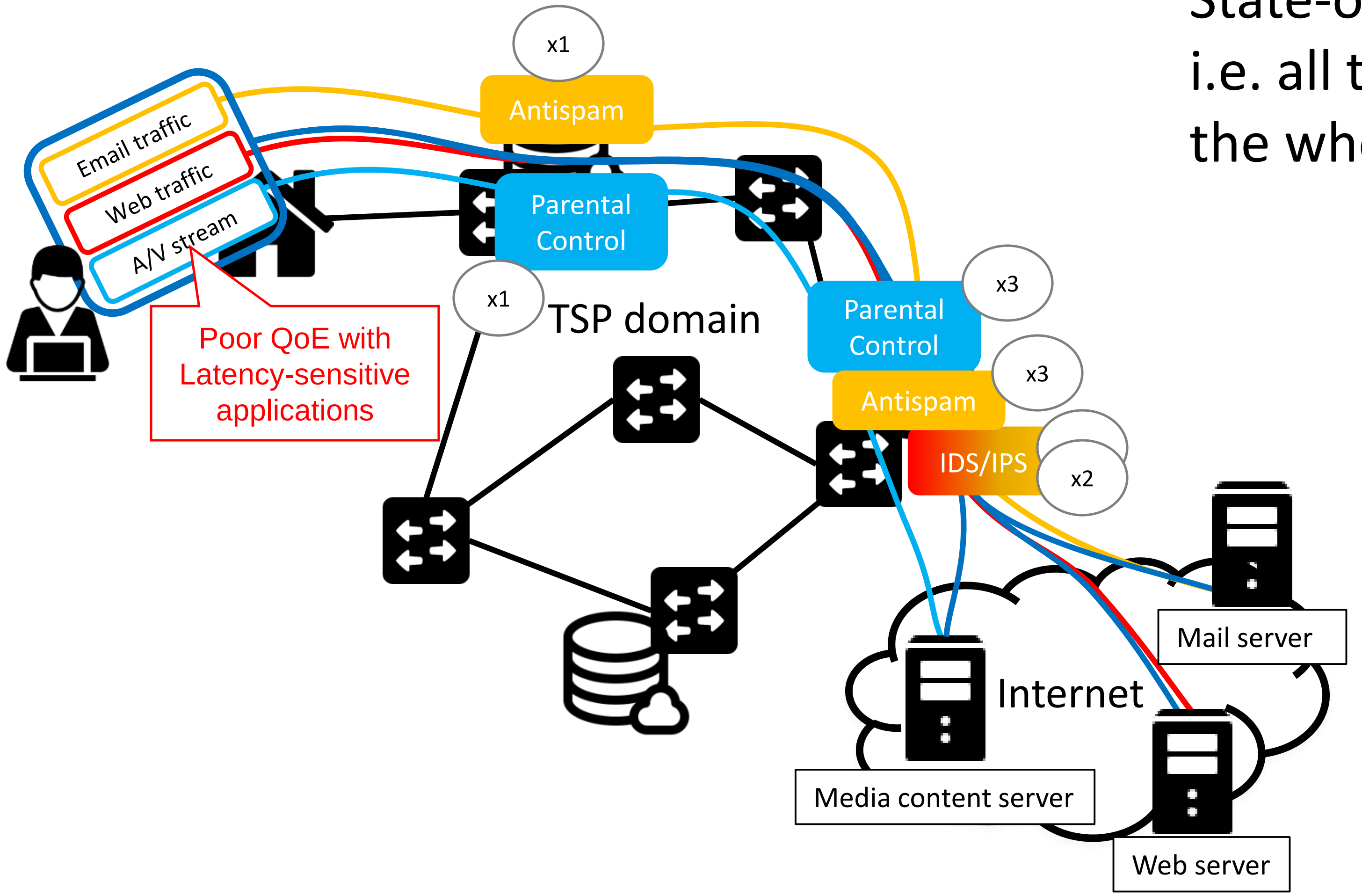


Example of VSNFs: Snort, Suricata, OpenDPI, DansGuardian, etc. running in virtual environments like VMs or containers

Progressive embedding of security services (PESS)

- Algorithm for the progressive placement of network security services
- The proposed ILP formulation comprises constraints to ensure that **application-specific** QoS and security requirements are met
- The objective is to increase the number of provisioned services:
    a) Reduced overall consumption of network resources
    b) Lower infeasibility percentage

Application-centric provisioning of virtual security network functions



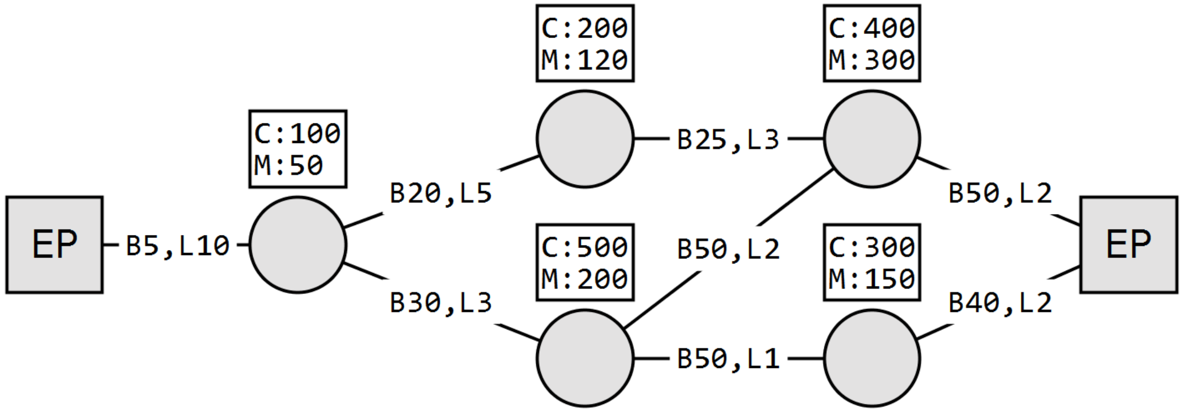
State-of-the-Art models are **user-centric** i.e. all the user traffic is forced to traverse the whole chain of security VNFs

1. User's QoE degradation
2. Waste of computational resources

Application-centric approach

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

System model (physical topology)



Physical topology model

Undirected and weighted graph

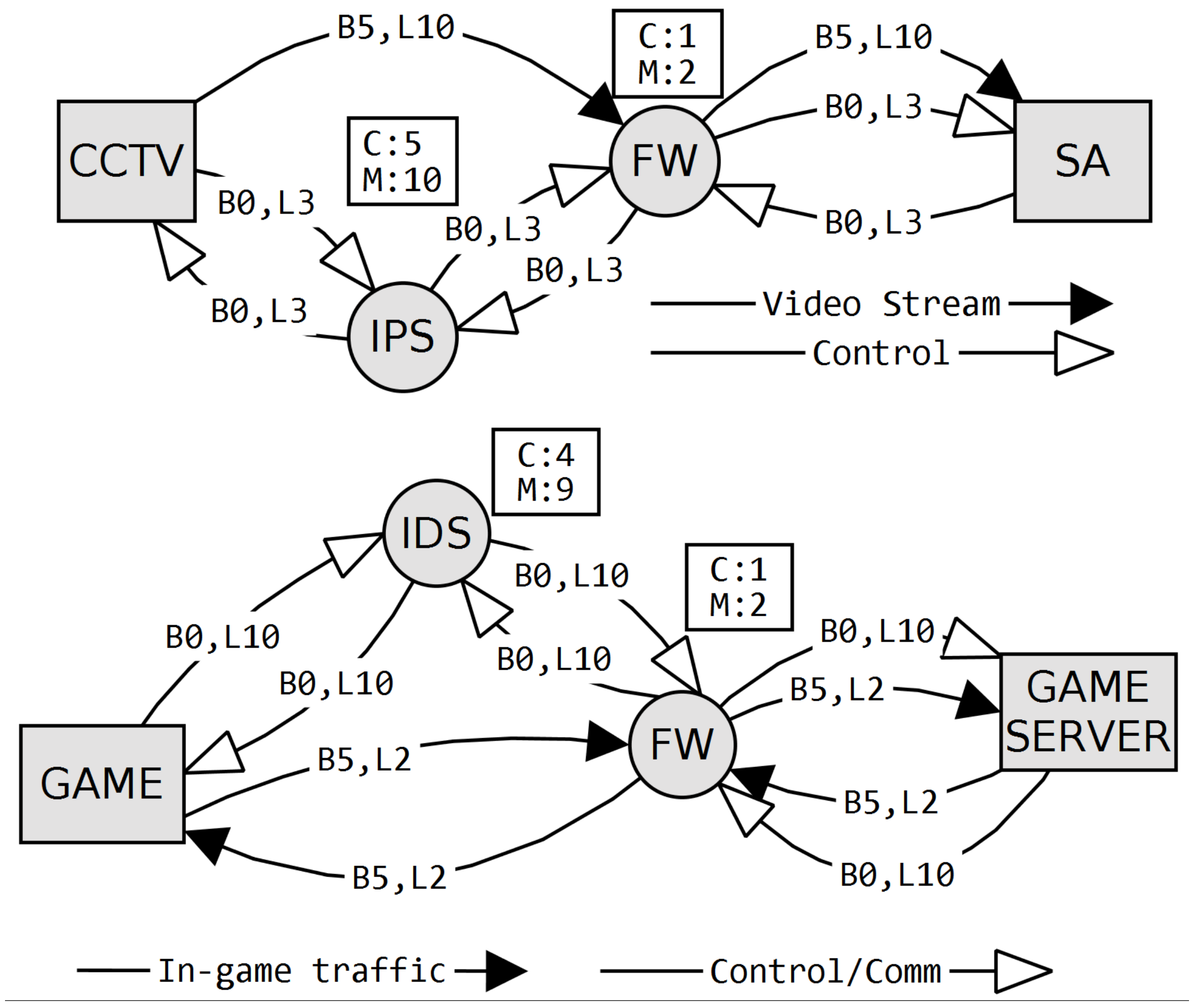
$$\mathcal{G} = (N, E)$$

Nodes: all of them are NFV nodes with CPU and memory resources

Links: characterized by their bandwidth and propagation delay

FONDAZIONE BRUNO KESSLER CREATE-NET CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

System model (security service request)



Security service request

$$\mathcal{G}_s = \{(U^c, U^c_{pairs}) : c \in C_s\}$$

- Each chain is characterized by security, min. bandwidth and max. latency requirements
- Nodes are characterized by CPU and memory requirements

Objective function (TSP use-case)

Minimization of used physical resources

Bandwidth resources

CPU and memory resources

$$\min \sum_{\substack{c \in C_s,\ i,j \in N, \\ (k,l) \in E, (u,v) \in U^c_{pairs}}} b_{k,l} \cdot \beta^c \cdot y^c_{k,l,i,j,u,v} + \sum_{c \in C_s, i \in N, u \in V^c} (c_i \cdot \gamma^c_u + m_i \cdot \mu^c_u) \cdot x^c_{i,u}$$

Penalty for resources with less residual capacity

where $$b_{k,l} = \frac{1}{\beta'_{k,l} + \delta} \quad c_i = \frac{1}{\gamma'_i + \delta} \quad m_i = \frac{1}{\mu'_i + \delta}$$

Constraints

Routing constraints build a path between the two end points of each chain

Resource constraints ensure that the resources requested by the security service are available

Latency constraint verifies the end-to-end latency requirements

Security constraint based on TSP's security policies and best practices

Recent achievements

Implementation of the ILP model with a commercial solver (Gurobi)

Implementation of a heuristic based on the Dijkstra algorithm

Evaluation:

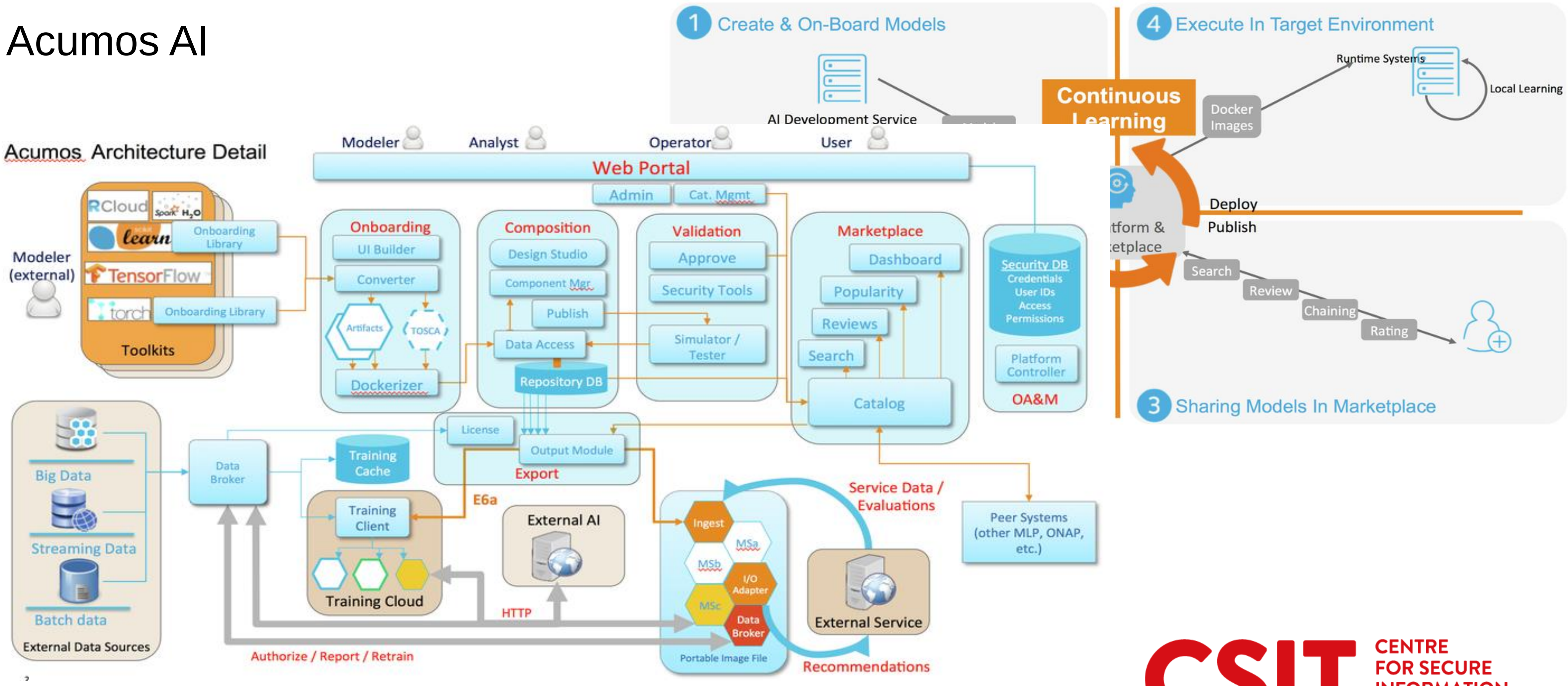
- Comparison between solver and heuristic
- Comparison between PESS approach and application-agnostic
- Scalability evaluation

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

MACHINE LEARNING FOR SECURITY IN SDN

Open Networking Summit (ONS) 2018

Acumos AI



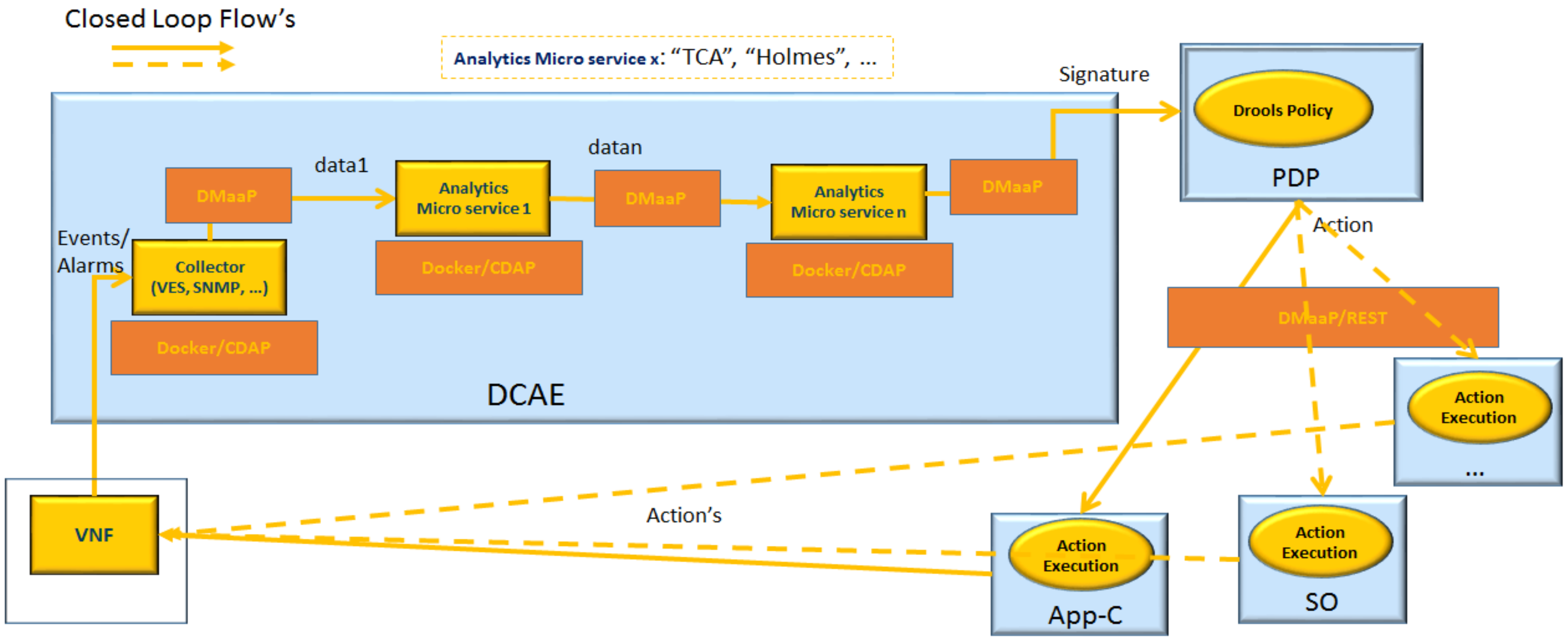
https://www.acumos.org/

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Open Networking Summit (ONS) 2018

ONAP (Open Network Orchestration Platform)

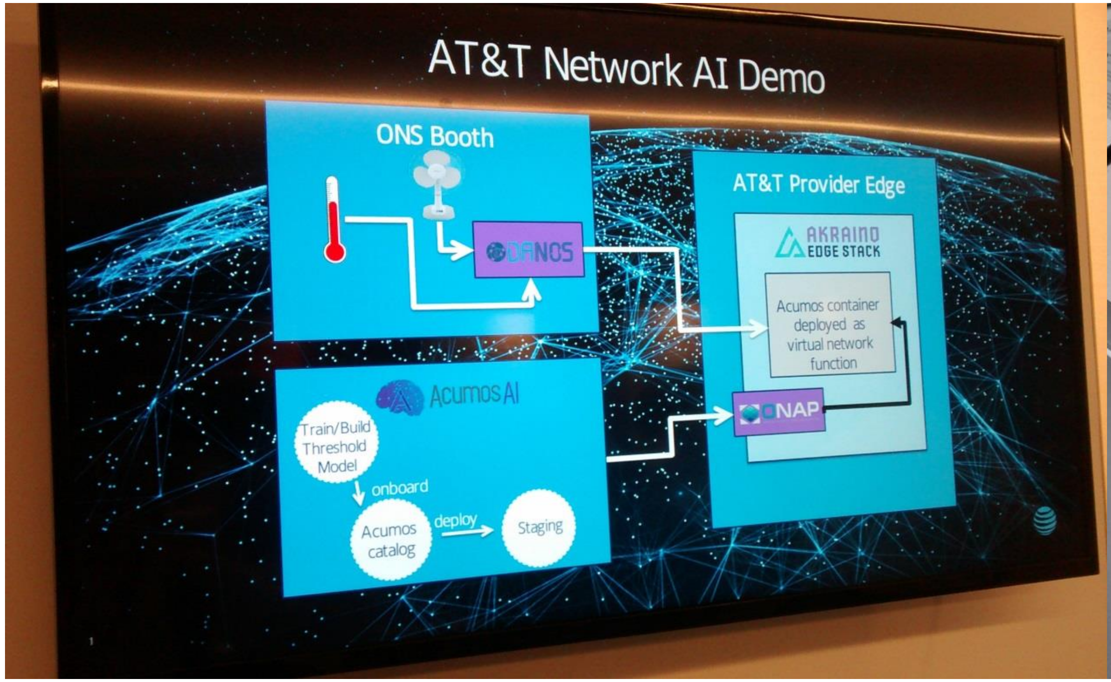
- Closed loop automation management platform
- ONAP policy engine (Data Collection, Analytics, and Events - DCAE)

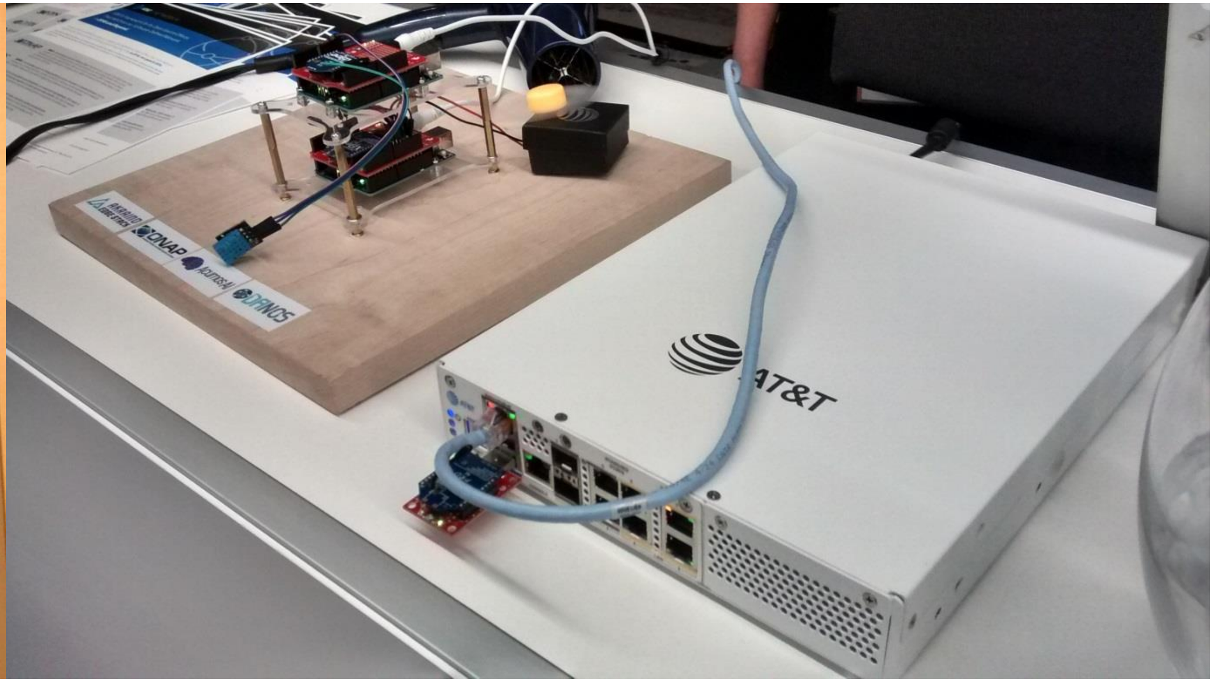


https://wiki.onap.org/pages/viewpage.action?pageId=4719898

Open Networking Summit (ONS) 2018

Akraino Edge Stack

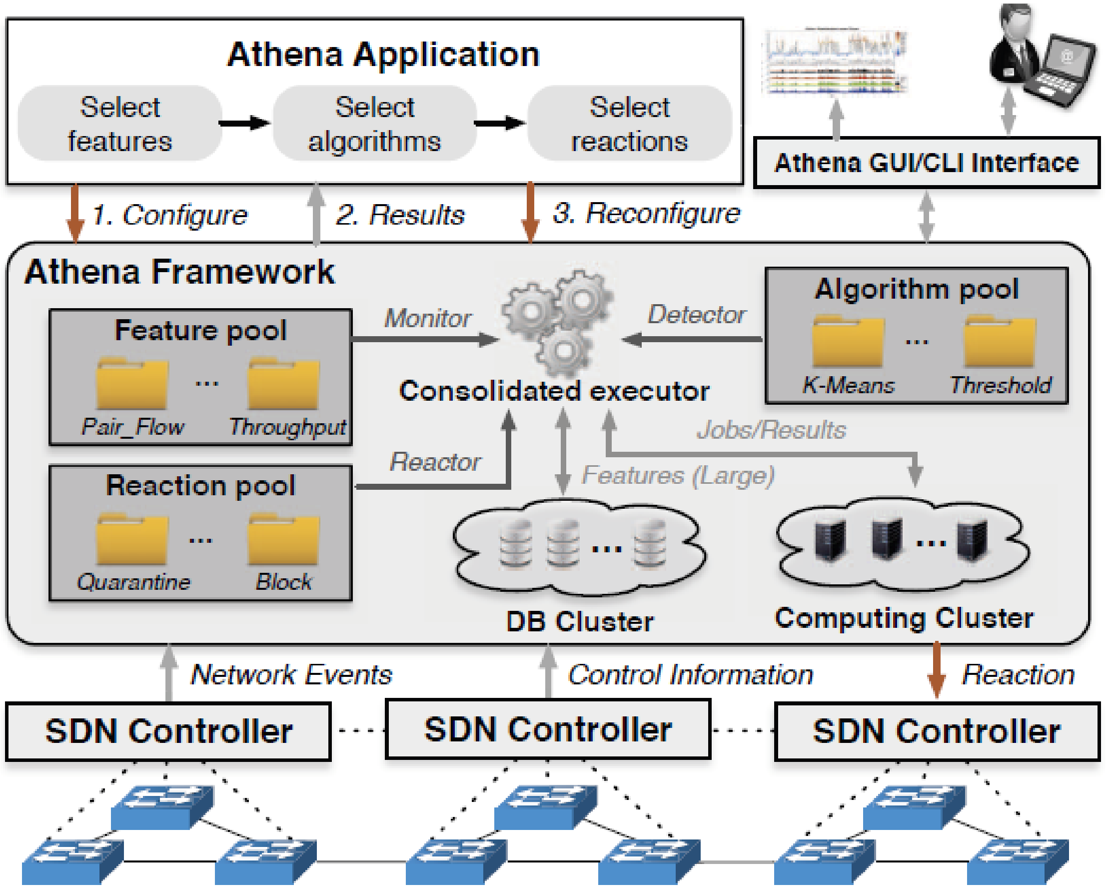




https://www.akraino.org/

Machine learning based security applications in SDN

- Example approach:
  - Athena



- Challenges in the network e.g.:
  - Volume of parameters
  - Non-stationary data

- Adversarial Examples

Lee, Seunghyeon, Jinwoo Kim, Seungwon Shin, Phillip Porras, and Vinod Yegneswaran. "Athena: A framework for scalable anomaly detection in software-defined networks." In *Dependable Systems and Networks (DSN), 2017 47th Annual IEEE/IFIP International Conference on*, pp. 249-260. IEEE, 2017.

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

BLOCKCHAIN IN SDN

Uses of Blockchain in SDN

- Authentication Solutions

  E.g. Securechain - http://www.reply.com/en/content/securechain

  Use-cases: Adding a device to the SDN, Rogue element rejection

  “Securechain brings security, scalability and auditability to Software-Defined Networks”

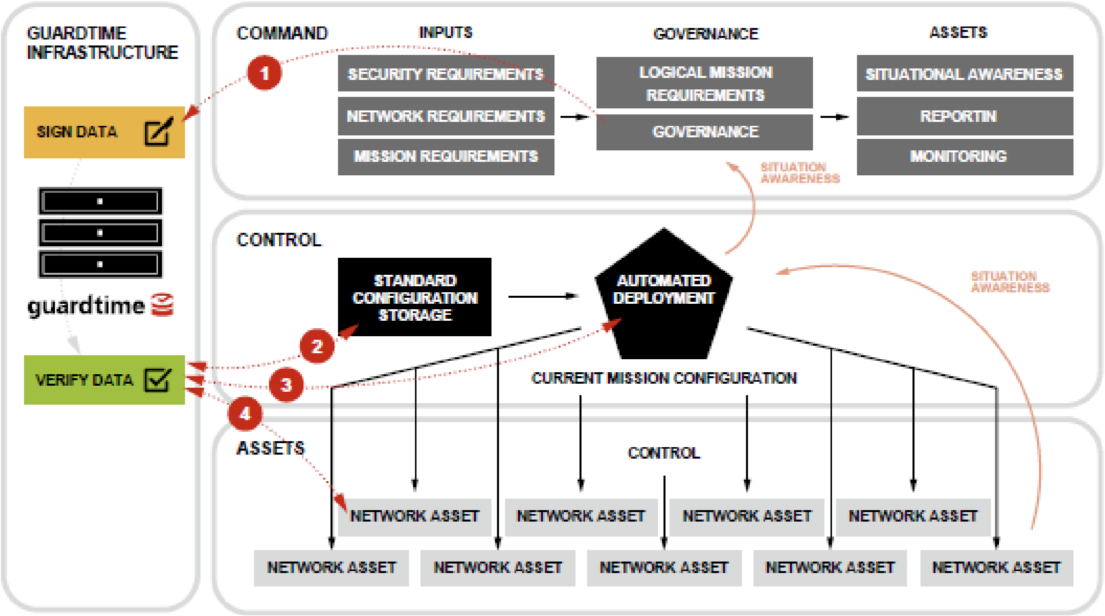
CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Uses of Blockchain in SDN

- Authentication Solutions

  E.g. Guardtime - http://www.ciosummits.com/Guardtime_KSI_Use_of_a_globally_distributed_blockchain_to_secure_SDN_whitepaper_1602.pdf

  Use-cases: Sign configuration data, Monitor verification data, Verify deployment inputs, Network asset continuous monitoring

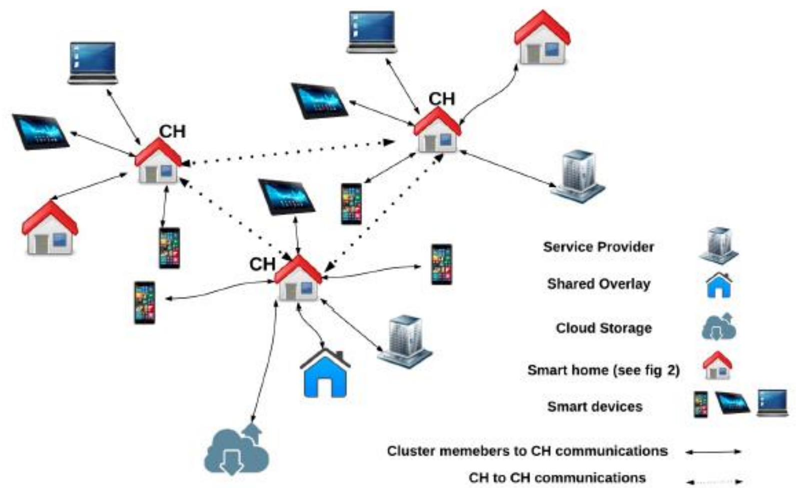


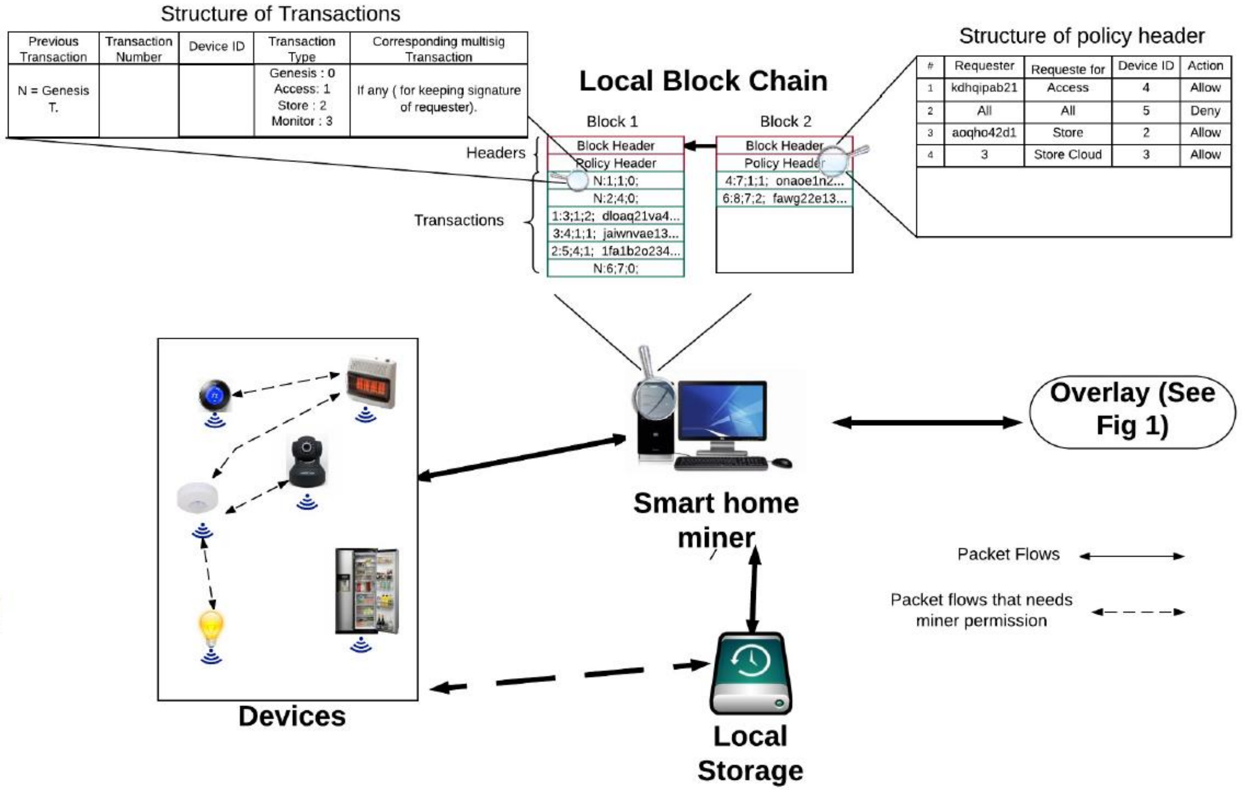
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Uses of Blockchain in SDN

- For IoT security and privacy

Use-case: Smart Home





Dorri, Ali, Salil S. Kanhere, Raja Jurdak, and Praveen Gauravaram. "Blockchain for IoT security and privacy: The case study of a smart home." In *Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on*, pp. 618-623. IEEE, 2017.

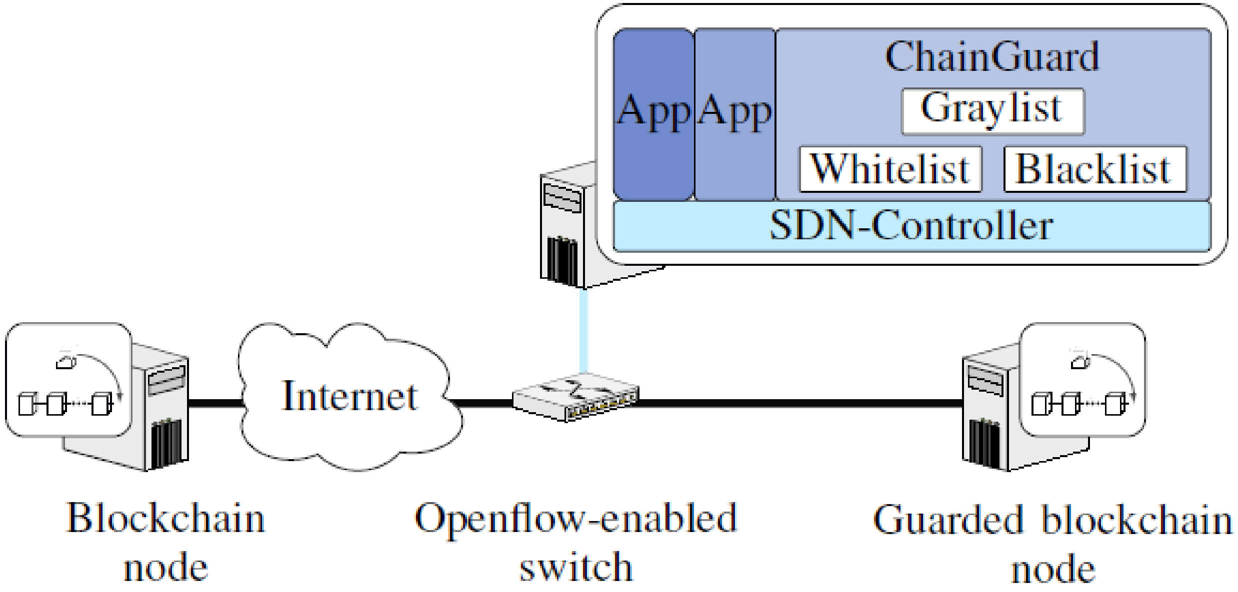
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Uses of Blockchain in SDN

- Guarding against blockchain attacks

  E.g. ChainGuard

  Use-case: Monitoring application to prevent DoS attack or abuse of the blockchain



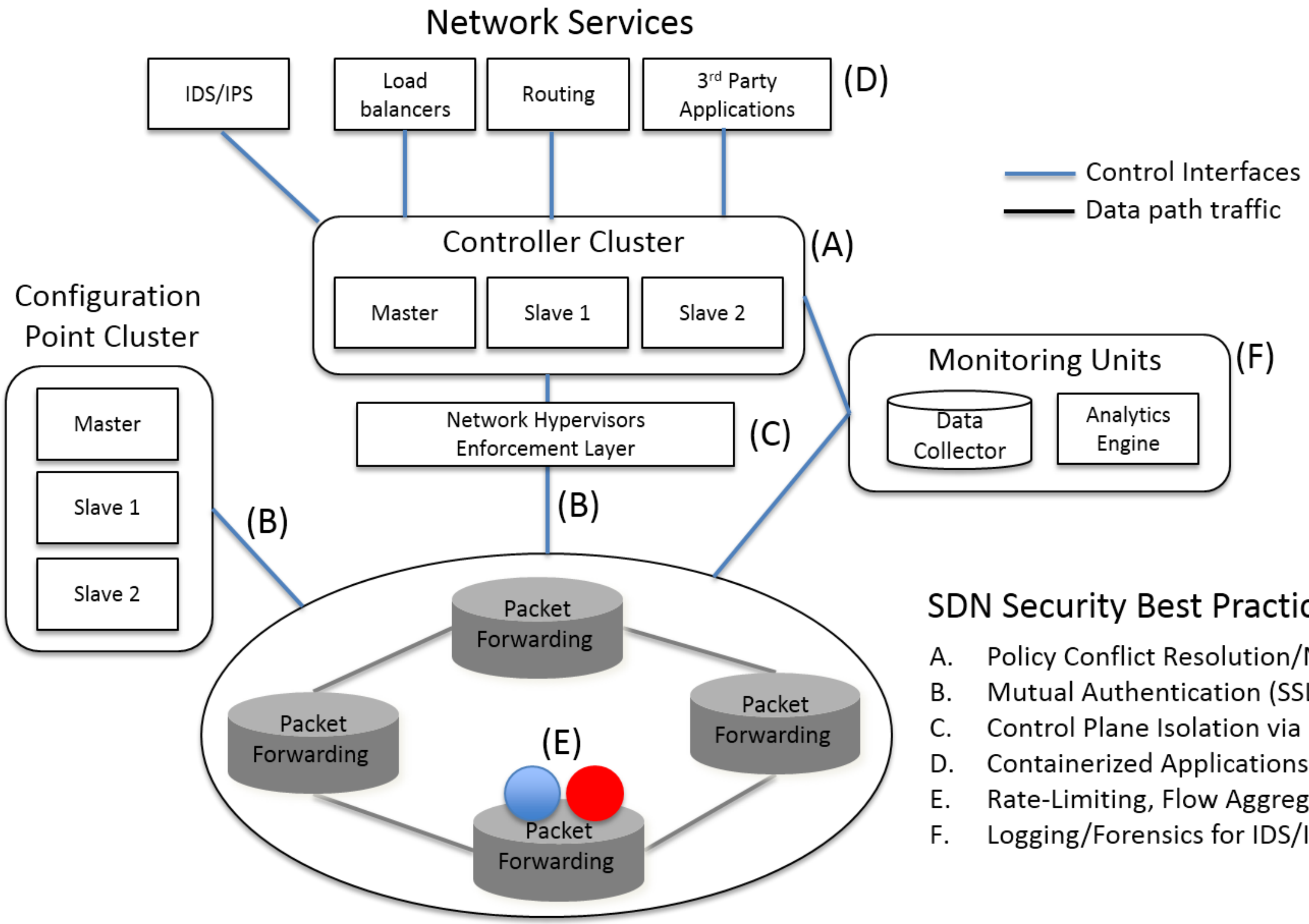
M. Steichen, S. Hommes, Radu State, "Chainguard – A firewall for blockchain applications using SDN with OpenFlow", *IEEE, Principles, Systems and Applications of IP Telecommunications (IPTComm),* 2017

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

SDN SECURITY RECOMMENDED BEST PRACTICES

Recommended Best Practices



SDN Security Best Practices

A. Policy Conflict Resolution/Network Invariant Detection
B. Mutual Authentication (SSL/TLS) – Access Control
C. Control Plane Isolation via Slicing
D. Containerized Applications - Access Control
E. Rate-Limiting, Flow Aggregation, Short Timeouts
F. Logging/Forensics for IDS/IPS

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Thank you

s.scott-hayward@qub.ac.uk

www.csit.qub.ac.uk

CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES