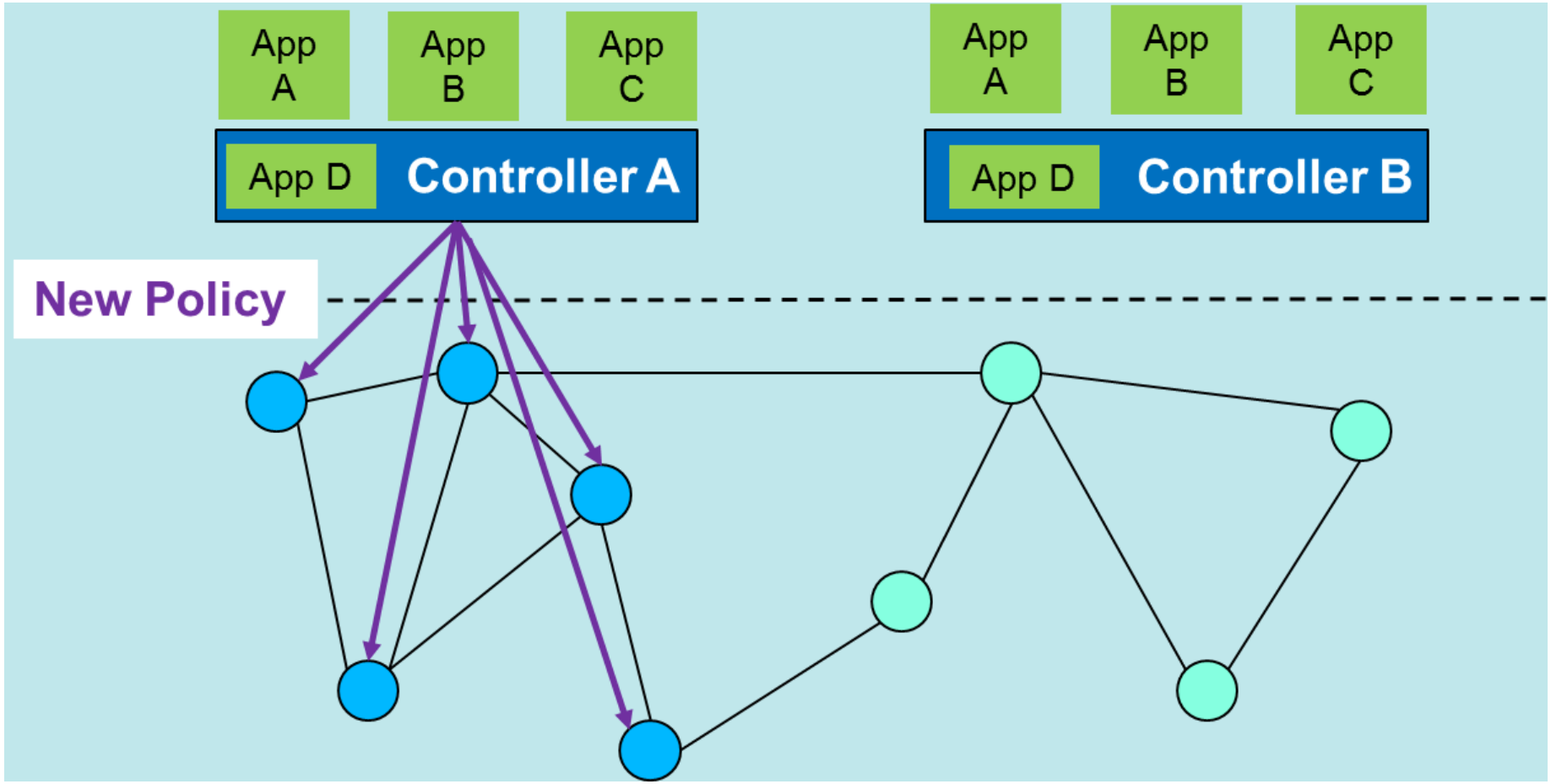
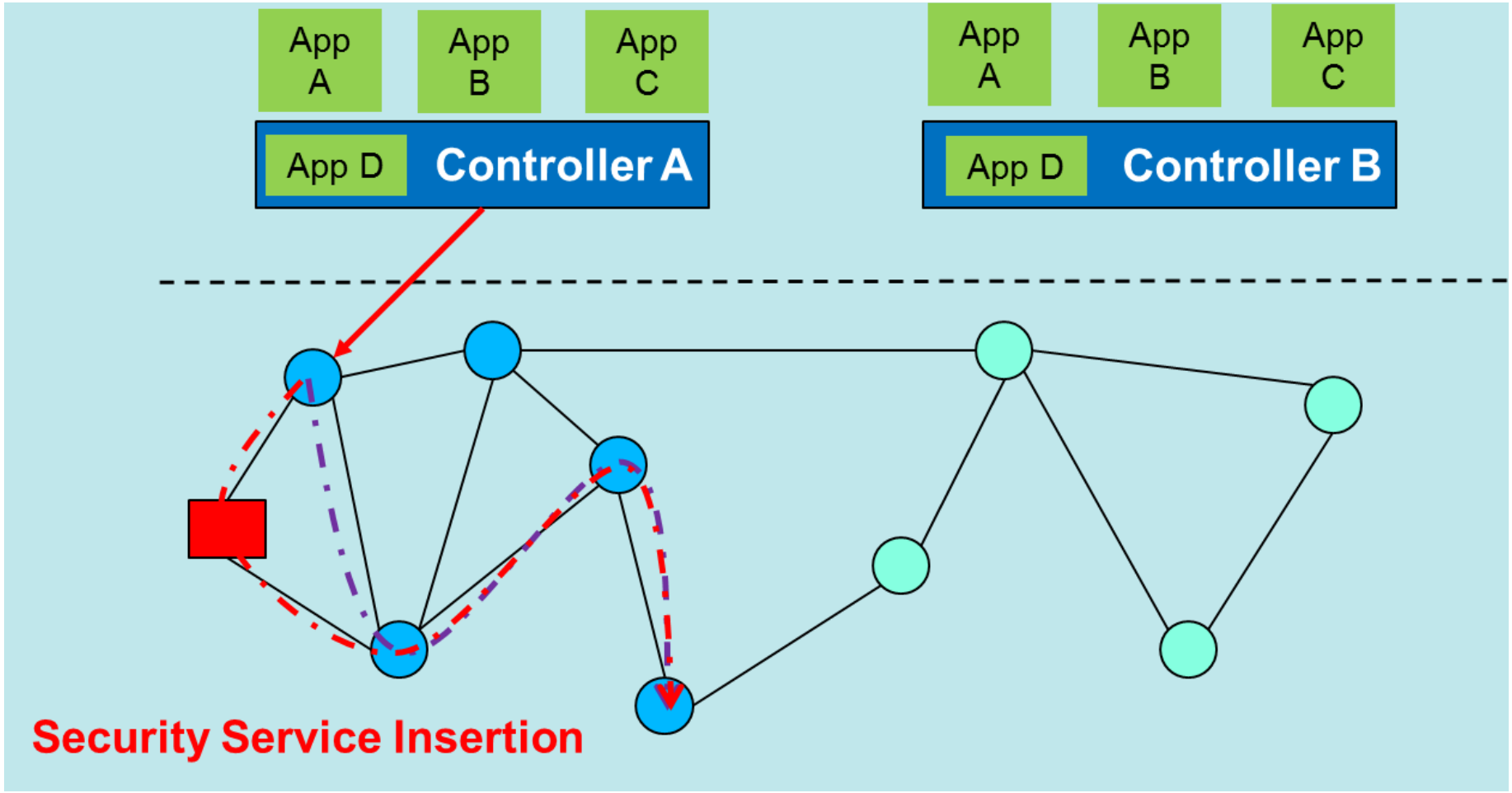
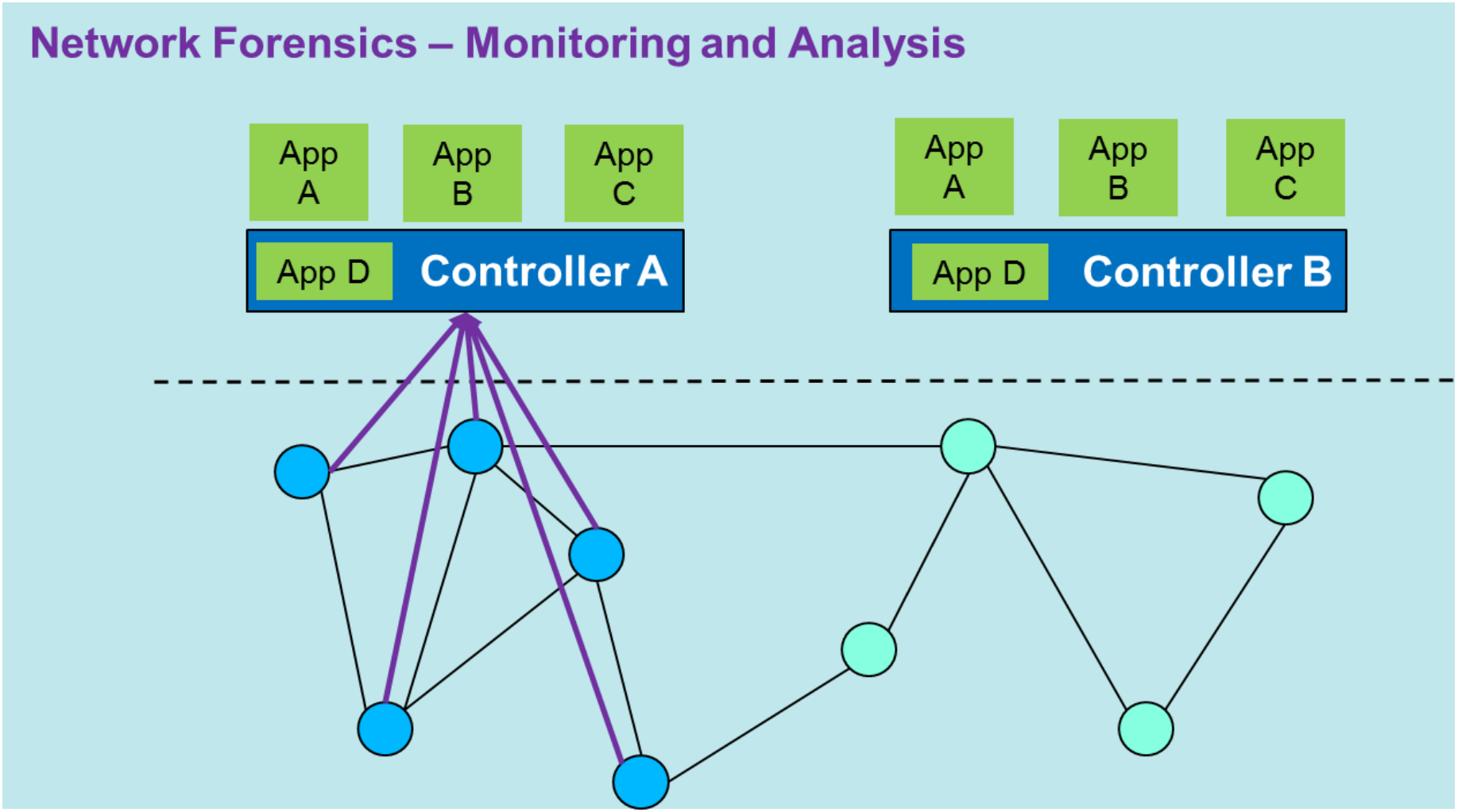

CSIT
CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES
Queen's University
Belfast
SDN Security
COINS Summer School
Dr. Sandra Scott-Hayward
23 August 2015
@CSIT_QUB

Network Security Enhancements using SDN


App A
App B
App C
App D
Controller A
App A
App B
App C
App D
Controller B
New Policy


App A
App B
App C
App D
Controller A
App A
App B
App C
App D
Controller B
Security Service Insertion

Network Forensics – Monitoring and Analysis



Categorization of Security Enhancements

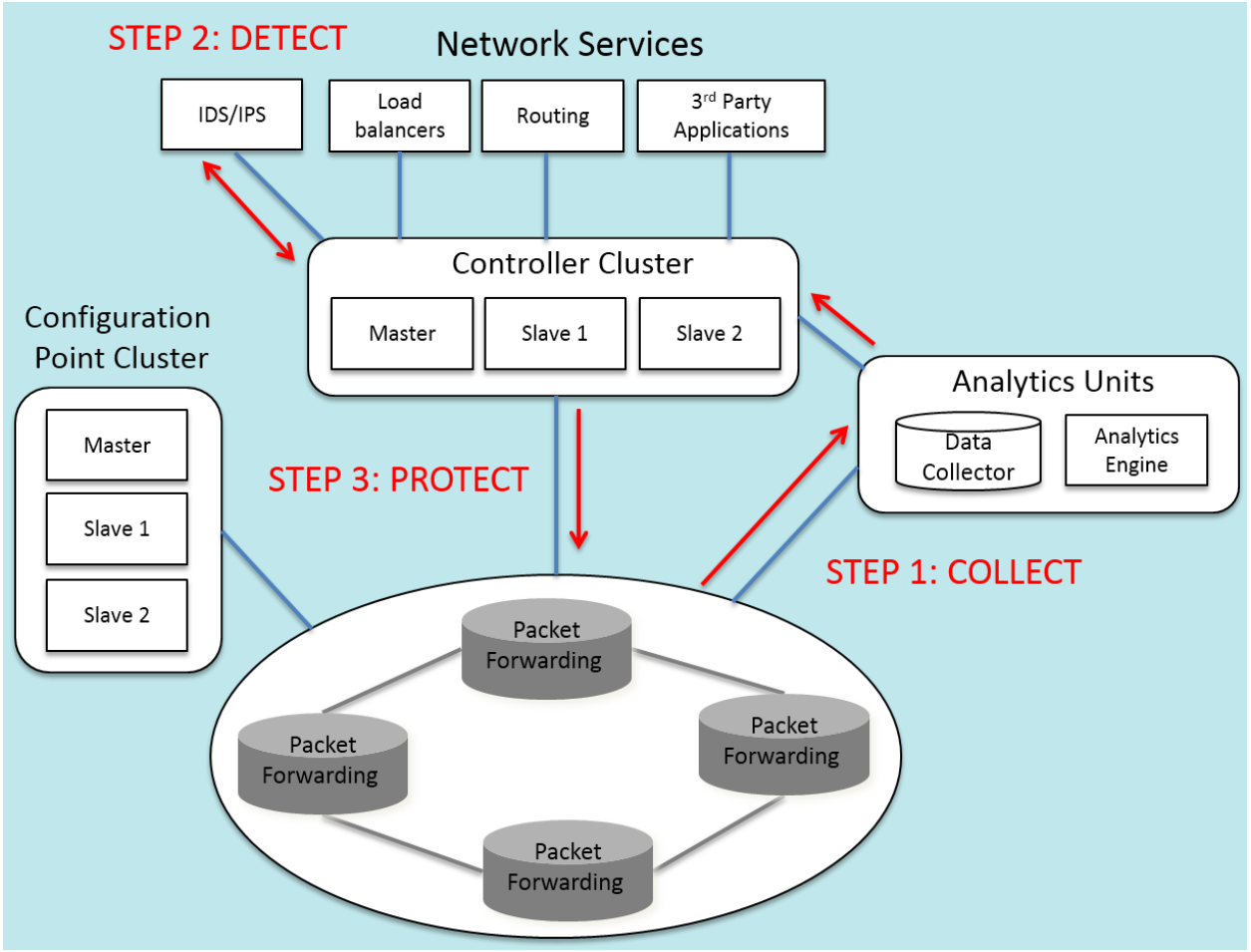
Security Enhancement	Research Work	SDN Layer/Interface				
		App	App-Ctl	Ctl	Ctl-Data	Data
Collect, Detect, Protect	Combining OpenFlow/sFlow [88], Active Security [89]	✓		✓	✓	✓
	Learning-IDS (L-IDS) [90], NetFuse [91], OrchSec [92]	✓		✓	✓	✓
	Cognition [93]	✓	✓	✓		
Traffic Analysis & Rule Updating	Resonance [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]	✓		✓		

SDN Security Feedback Control

Step 1: Collect Network Statistics

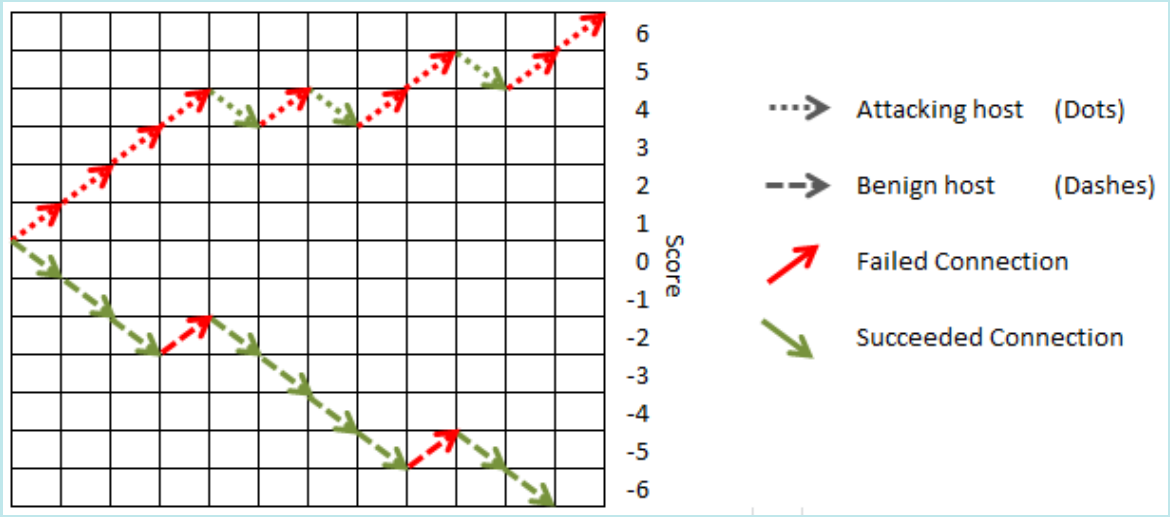
Step 2: Detect anomalies or intrusions in the network

Step 3: Insert flow rules to protect the network



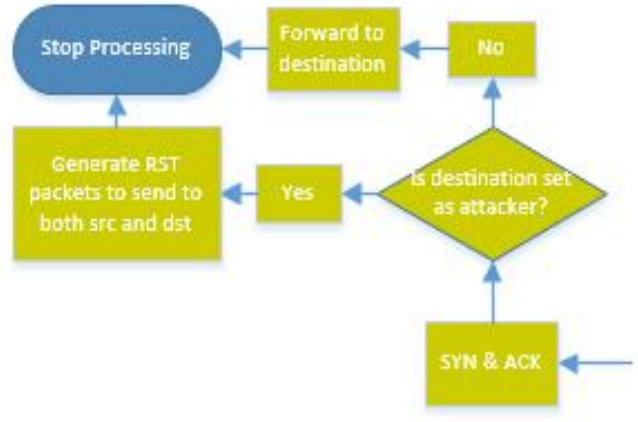
Algorithm Decisions:

- Count attempted connection rate (use TRW);
- Detect illegal TCP Flag combinations;
- Periodically review restrictions;



Port Scan Protection

ACK Scan



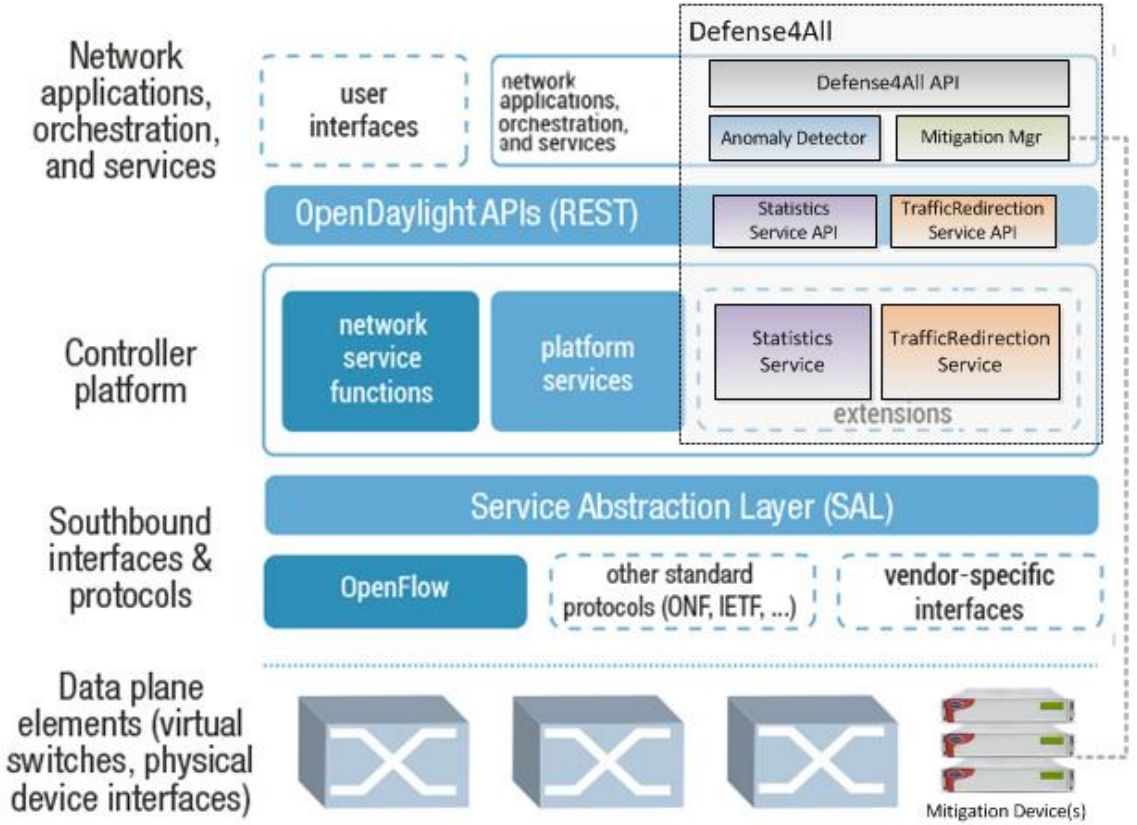

```
PortScanDetector
ID: 8d7e52b11239d08a9d22b214b26a43de
Version 1.0

Launched: 2015-05-13 16:17:09.856287

2015-05-13 16:17:28.573458
New host discovered:00:00:00:00:00:01

2015-05-13 16:17:28.672934
New host discovered:00:00:00:00:00:08

2015-05-13 16:17:28.673282
New host discovered:00:00:00:00:00:09

2015-05-13 16:17:28.673549
New host discovered:00:00:00:00:00:07

2015-05-13 16:17:42.440481
Suspected TCP attack from: 00:00:00:00:00:01
Type of attack suspected: ACK
Action taken: Block TCP replies to host
Action taken: Replace SYNACK replies to host with RSTACK
```

OpenDaylight Example

Defense4All Application provided by RadWare:

- DDoS attack detection and traffic diversion
- Doesn't include attack mitigation

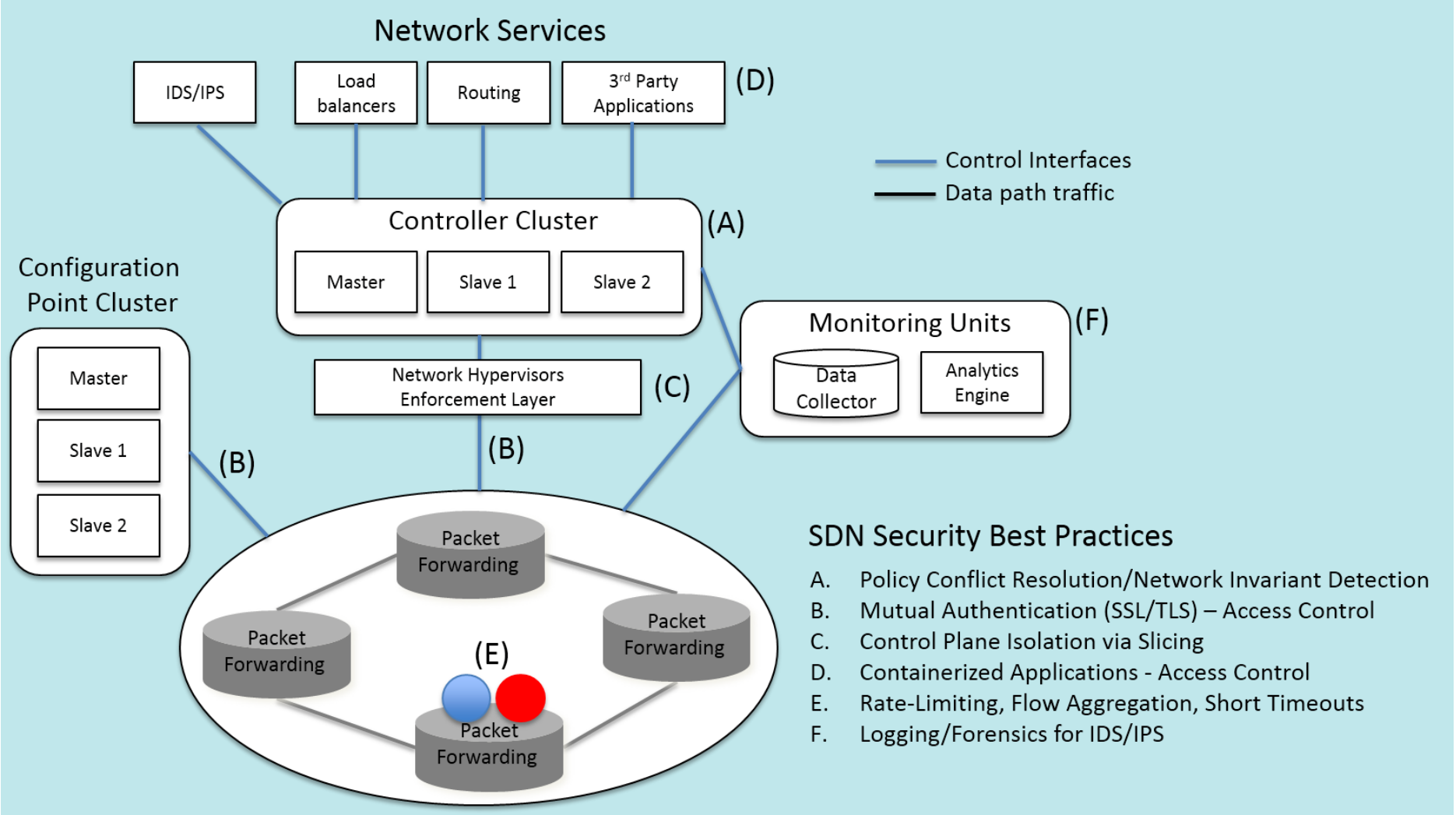
https://wiki.opendaylight.org/view/Project_Proposals:Defense4All



Security Products - SDN

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

Future Research Directions

- Secure Network Map
- Exploiting SDN for Moving Target Defense
- Security Assessment Framework
- Network Security as a Service (NSaaS)
- Removing Middleboxes from the Network


End of Session 7