Securing the Software-Defined Network Control Layer

Phillip Porras, Steven Cheung, Martin Fong,
Keith Skinner, and Vinod Yegneswaran

Computer Science Laboratory, SRI International
333 Ravenswood Avenue, Menlo Park, CA 94025

NDSS 2015

SDN for Security: Sophisticated Flow Orchestration

	SOLUTION!	but would we rather…..
Malicious Packet Stream	Drop	Auto-Redirect Malicious Source to Honeynet
Policy Violations	Drop	Redirect User to a Notification Server
Network Wide Anomaly	Drop	Selective Filtering or reprovision assets
Infected Host	Drop	Quarantine
Floods and Service Denials	Drop	Block, Migrate Mission Critical services, Redirect
Malicious Logic injection	Drop	Redirect into Sandnet
Remote Shell or C&C	Drop	Redirect In and outbound flows to separate data sinks
Server Behavioral Deviations	Drop	Dynamic quota adjustment, fishbowl and reprovision new server
Network Reconnaissance	Drop	Proactively redirect probes to whitehole or honeynet
Threat Reputation	Drop	Selectively limit network privileges or apply added antifraud challenges
Stepping Stone Tunneling	Drop	Selective interruption to validate that tunnel exists

Security challenges: What happens when software defines your network flow policy?

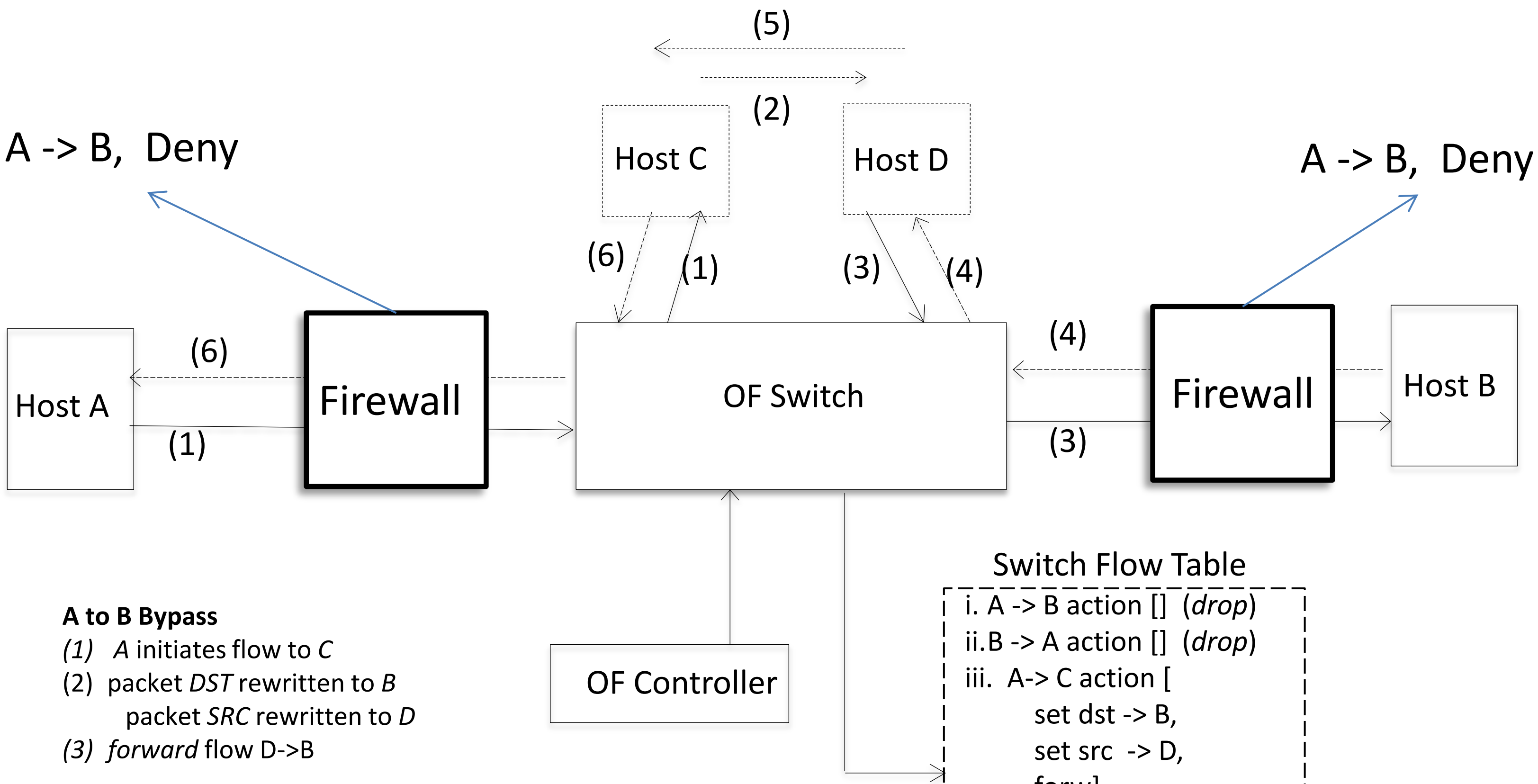
- **We grew up with (fairly) "static policies":** With SDNs … *Traffic Engineering* (TE) Apps constantly orchestrate the network flows to adapt to network conditions
- **Security must not depend on the absences of complex SDN App interactions**
- **Ideally, flow policies made in response to threats should take precedence**
- **The SDN Stack is itself a fair TARGET for attack**

Solving these challenges is a prerequisite for adoption by secure computing facilities, … anywhere compliance is needed

Security Challenge Virtual Flow Orchestration

http//www.openflowsec.org/OpenFlow_Security/Demo_Vids.html

May 2012, **A Demonstration of Inline Constraints Policy Enforcement**, 6 minutes



A to B Bypass

(1)   *A* initiates flow to *C*

(2) packet *DST* rewritten to *B*
packet *SRC* rewritten to *D*

(3) *forward* flow D->B

B to A Bypass

(4)   *B* initiates flow to *D*

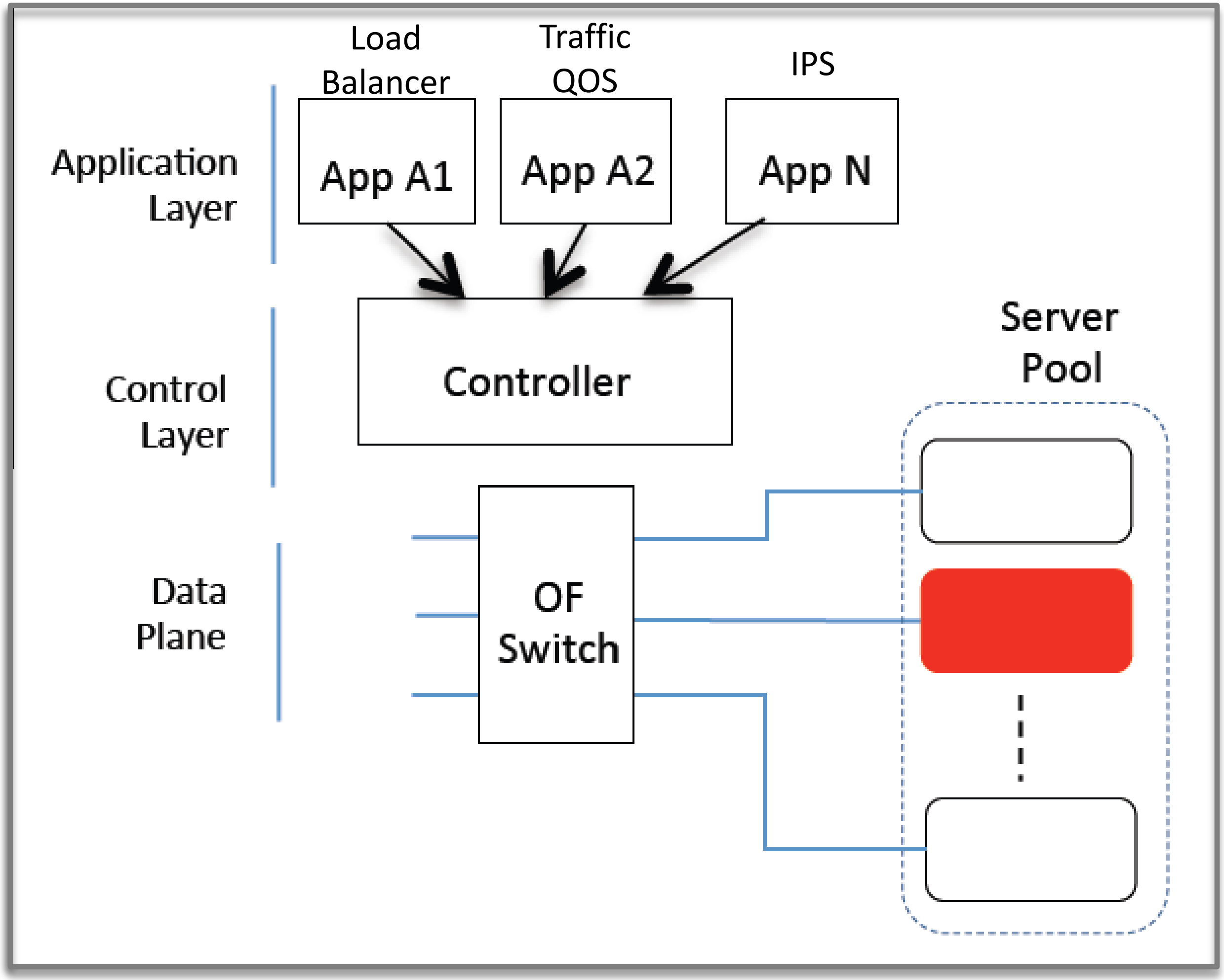
(5)   packet *DST* rewritten to *A*
packet *SRC* rewritten to C

(6)   *forward* flow C->A

Switch Flow Table

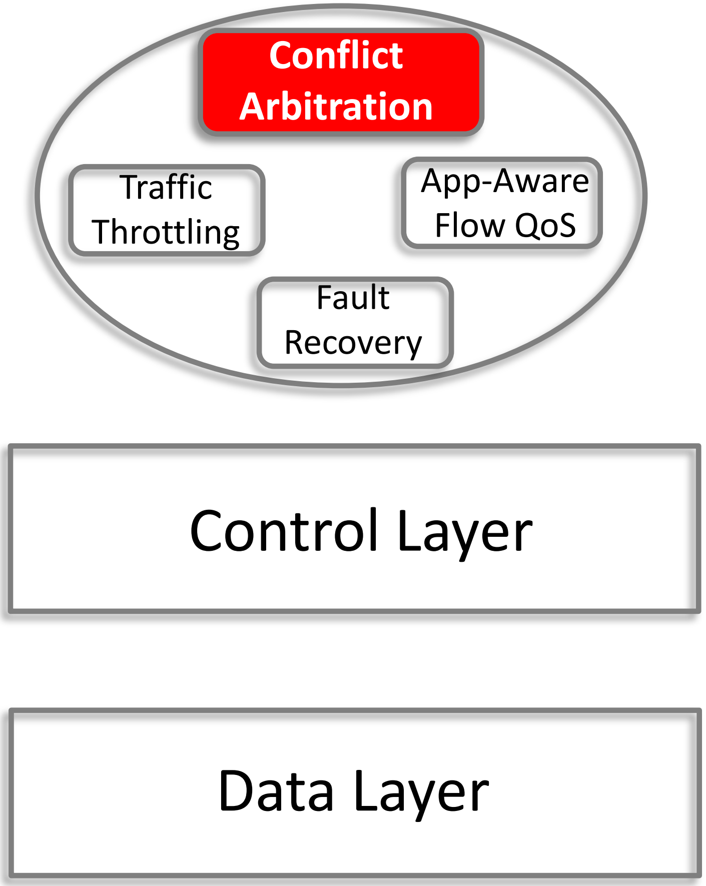
i. A -> B action [] (*drop*)
ii.B -> A action [] (*drop*)
iii. A-> C action [
set dst -> B,
set src -> D,
forw]
iv. B -> D action [
set dst -> A,
set src -> C,
forw]

Network Policy Conflict Arbitration



Network Policy Conflict Arbitration

Monolithic App Design



Conflict Arbitration

Traffic Throttling

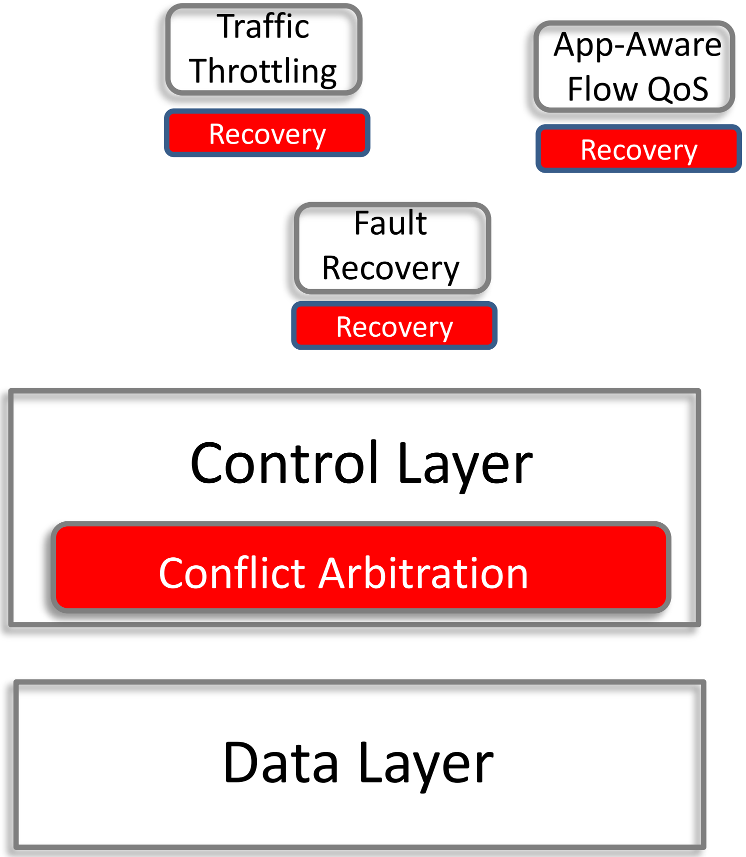
App-Aware Flow QoS

Fault Recovery

Control Layer

Data Layer

Sharable, Composable, Design



Traffic Throttling

Recovery

App-Aware Flow QoS

Recovery

Fault Recovery

Recovery

Control Layer

Conflict Arbitration

Data Layer

We are here

What is SE-Floodlight?

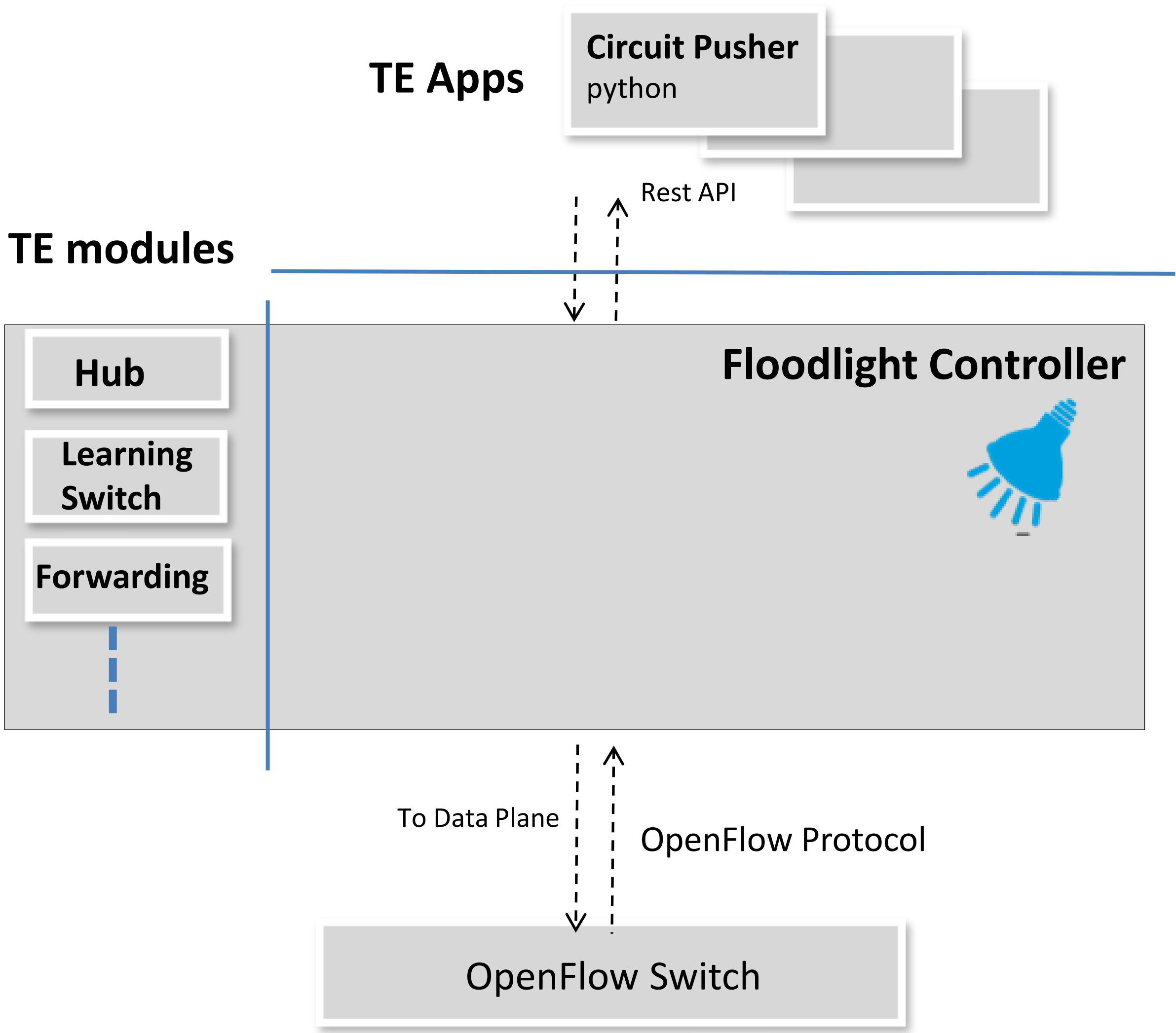
An application-to-data-plane security mediation service embedded in the control layer

- Recognizes and resolve conflicts between a Candidate Flow rules and the current *flow policy*

- Allows the dynamism of OpenFlow applications to produce optimal flow routing decision

- Empowers *OpenFlow* *security applications* and operators to dynamically assert *defensive* flow policy when new threats are perceived

An OpenFlow Controller

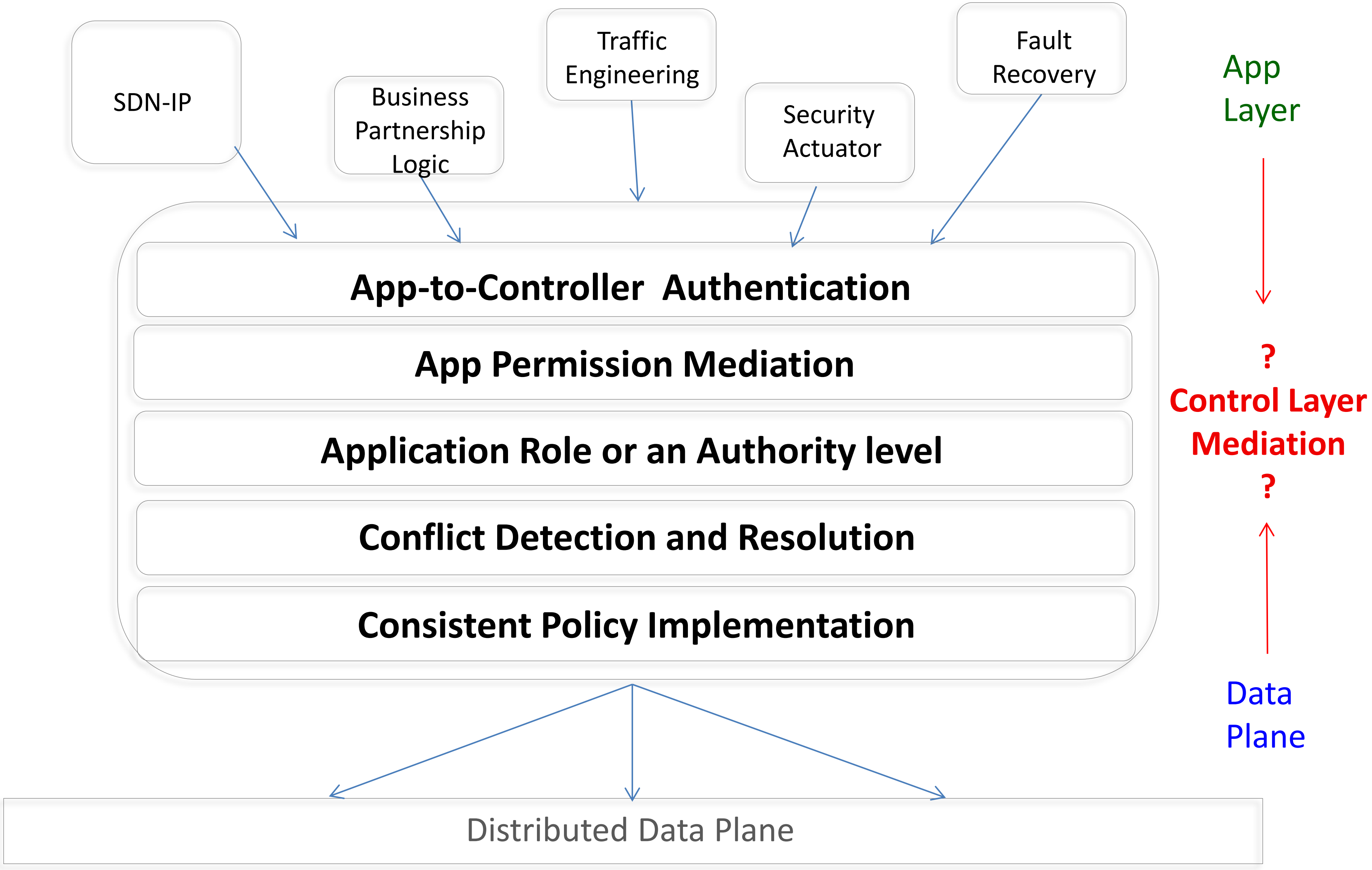


The Floodlight Controller

a coordination point through which traffic engineering apps

- convey flow rules
- submit configuration requests to the switch
- probe the data plane for state information
- Probe the controller state
- configure the controller

Control Layer Mediation?



SDN-IP

Business Partnership Logic

Traffic Engineering

Security Actuator

Fault Recovery

App-to-Controller Authentication

App Permission Mediation

Application Role or an Authority level

Conflict Detection and Resolution

Consistent Policy Implementation

Distributed Data Plane

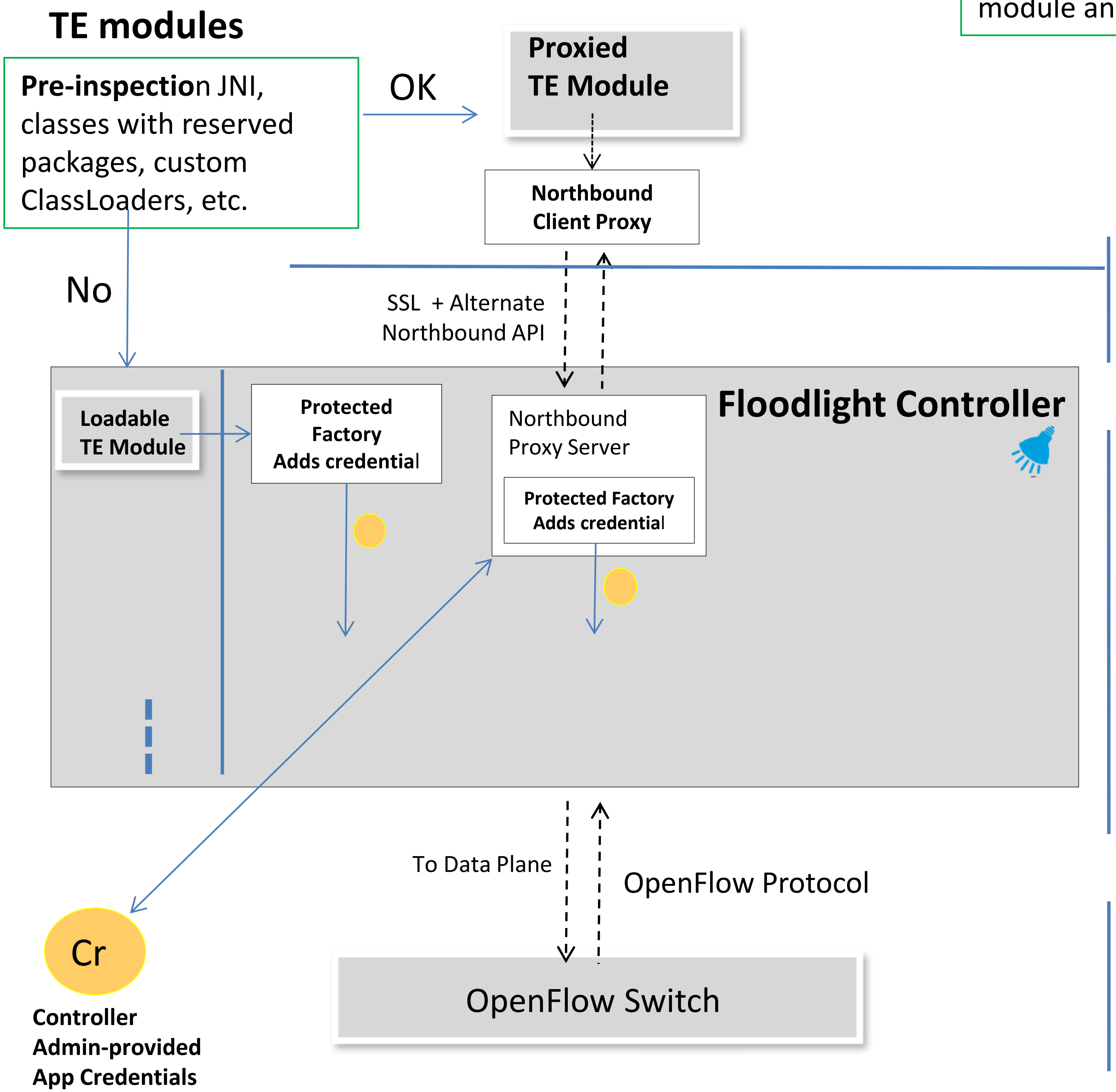
App Layer

? Control Layer Mediation ?

Data Plane

Identifying Authentication

Runtime Credential admin generates runtime credential signed manifest, module and classes, SE-Fl credentials



TE modules

Pre-inspection JNI, classes with reserved packages, custom ClassLoaders, etc.

OK

Proxied TE Module

Northbound Client Proxy

No

SSL + Alternate Northbound API

Floodlight Controller

Loadable TE Module

Protected Factory Adds credential

Northbound Proxy Server

Protected Factory Adds credential

To Data Plane

OpenFlow Protocol

OpenFlow Switch

Cr

Controller Admin-provided App Credentials

Class Validation Function Validates integrity of module and manifest

Essentially, We add the credential as an opaque object provided to every client request

5. Legacy modules objects without the protected opaque credential inherit app credential

App Credentials: Hierarchical Authorization Roles

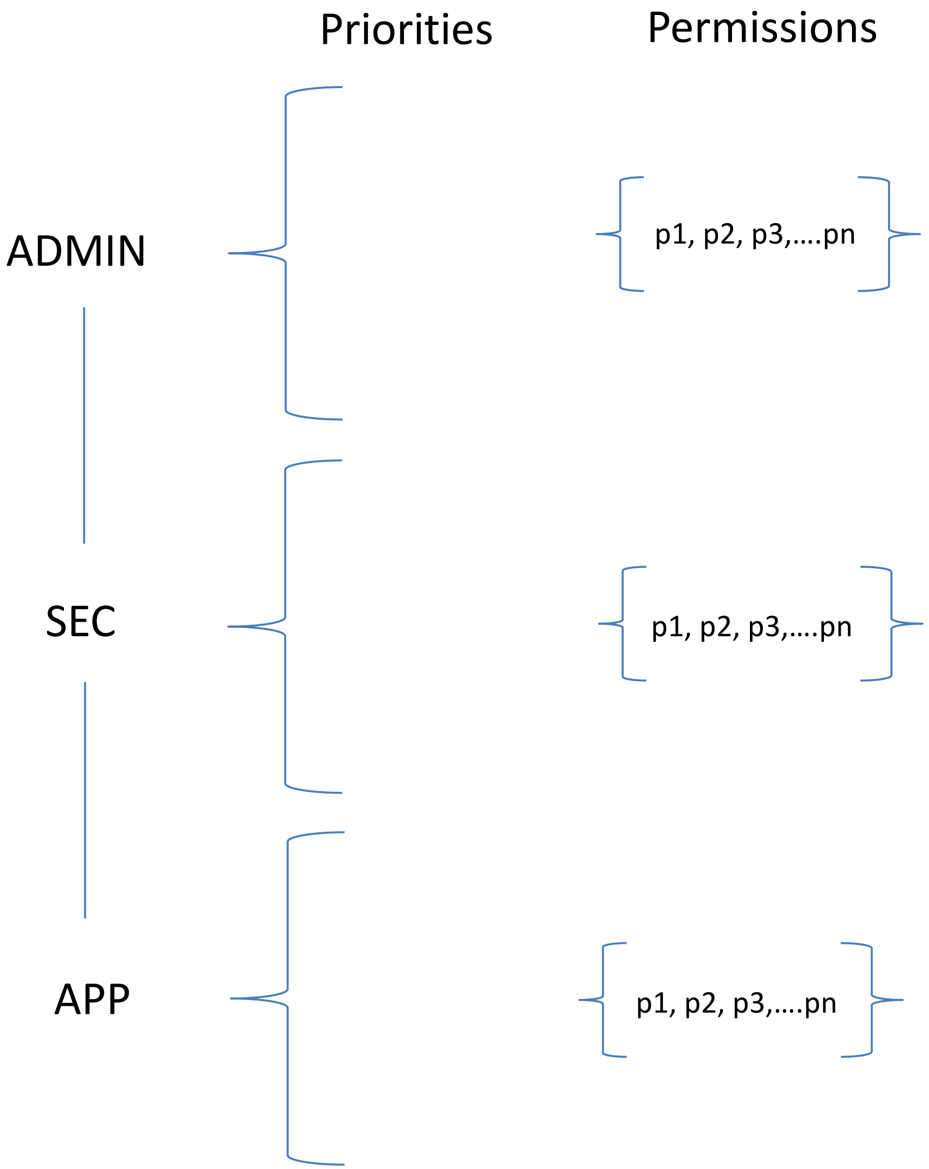
`flowmod`

Conflict resolution

Administrator Applications – scripts and console apps

Security Applications – dynamic filtering and redirection in response to perceived threats or vulnerabilities

Applications - Traffic Engineering applications



Priorities

Permissions

ADMIN

p1, p2, p3,….pn

SEC

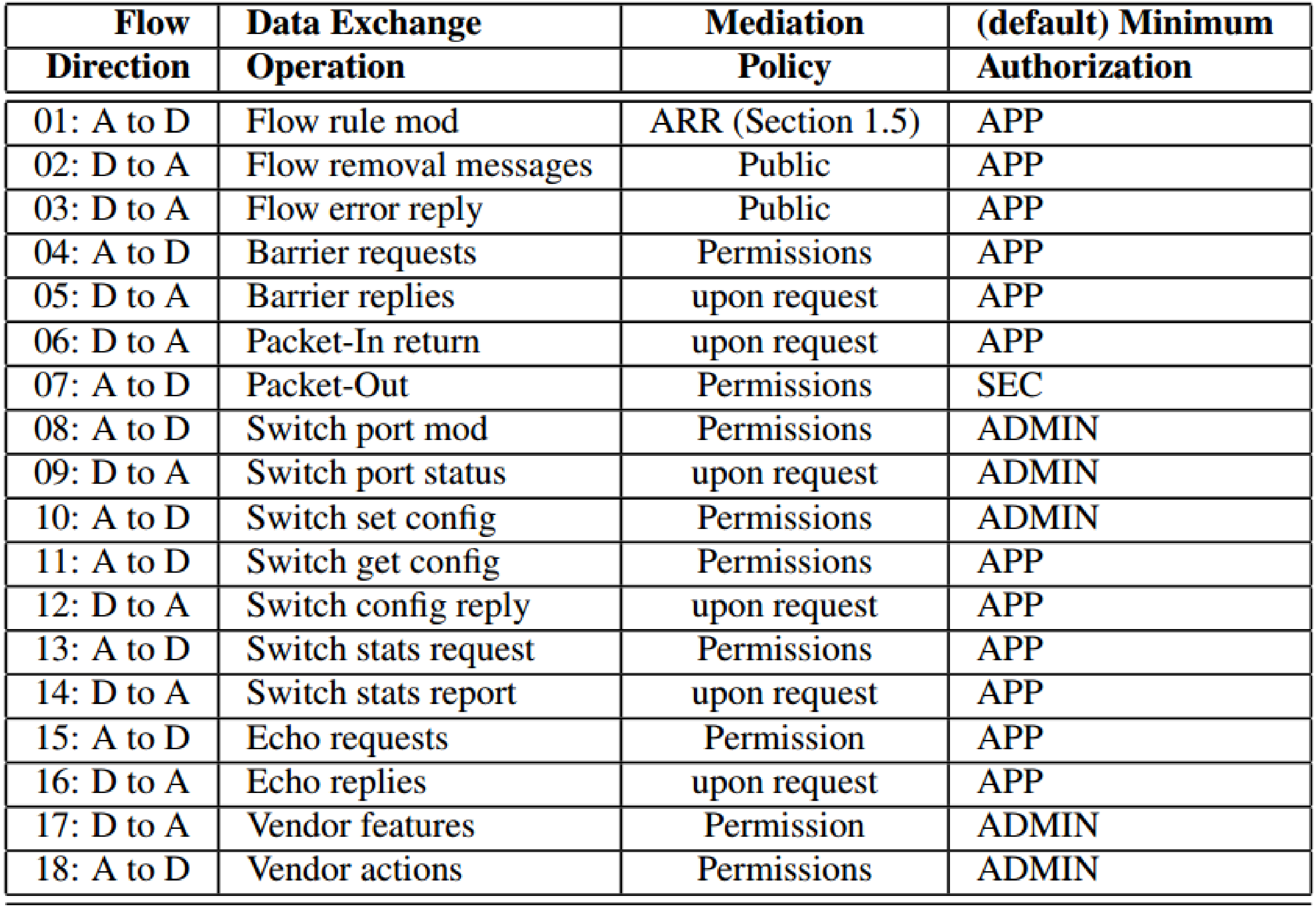
p1, p2, p3,….pn

APP

p1, p2, p3,….pn

App Credentials: Permissions for OpenFlow Apps

We Introduce an app permission model for OpenFlow



Flow Direction	Data Exchange Operation	Mediation Policy	(default) Minimum Authorization
01: A to D	Flow rule mod	ARR (Section 1.5)	APP
02: D to A	Flow removal messages	Public	APP
03: D to A	Flow error reply	Public	APP
04: A to D	Barrier requests	Permissions	APP
05: D to A	Barrier replies	upon request	APP
06: D to A	Packet-In return	upon request	APP
07: A to D	Packet-Out	Permissions	SEC
08: A to D	Switch port mod	Permissions	ADMIN
09: D to A	Switch port status	upon request	ADMIN
10: A to D	Switch set config	Permissions	ADMIN
11: A to D	Switch get config	Permissions	APP
12: D to A	Switch config reply	upon request	APP
13: A to D	Switch stats request	Permissions	APP
14: D to A	Switch stats report	upon request	APP
15: A to D	Echo requests	Permission	APP
16: D to A	Echo replies	upon request	APP
17: D to A	Vendor features	Permission	ADMIN
18: A to D	Vendor actions	Permissions	ADMIN

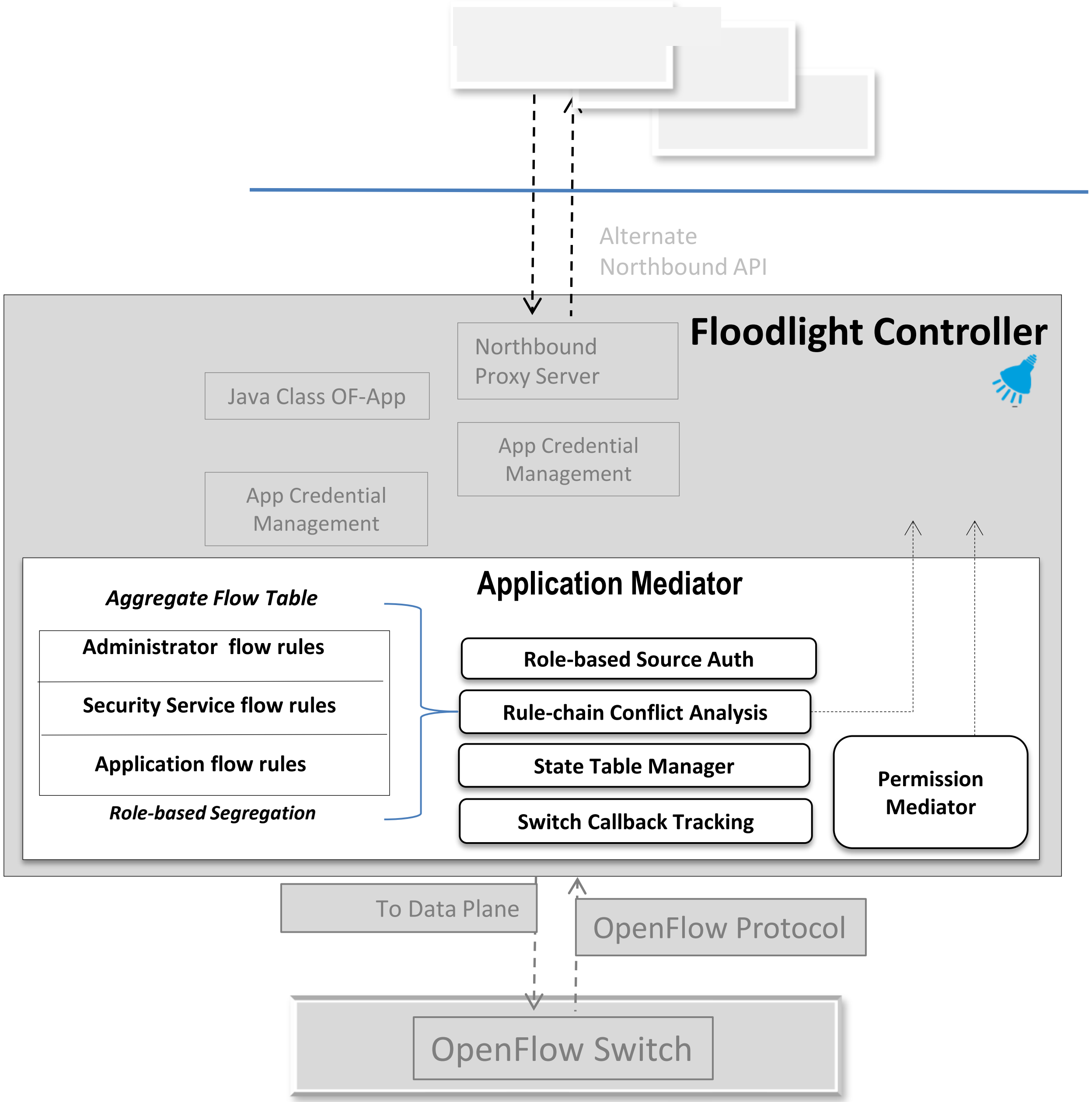
Apps: Insert Flow Policies

Sec: Adds the ability to use **PacketOut**

Admin: manipulate switch configuration

…or select your own model

Application Mediation Service



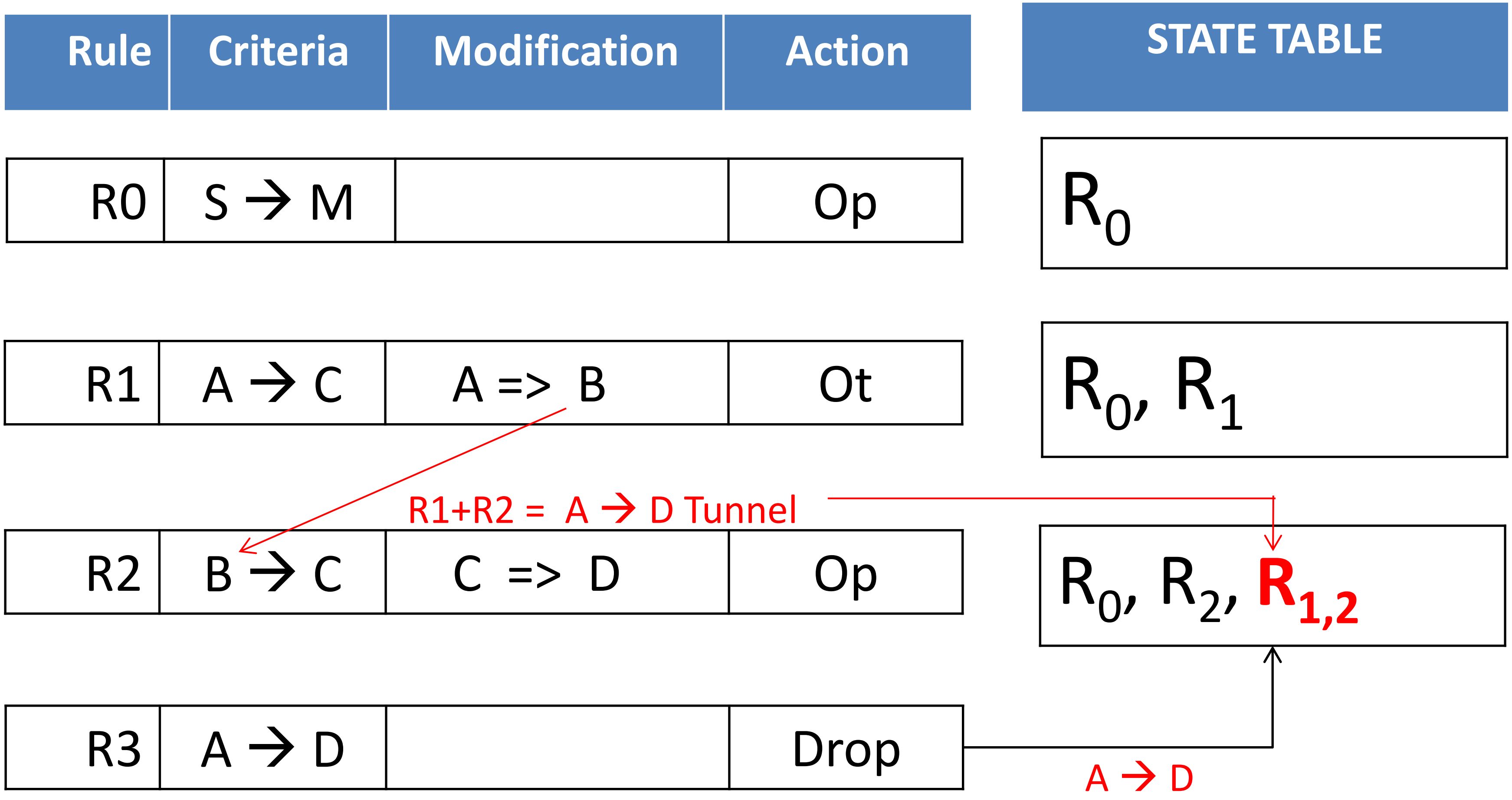
4 main functions

- **State Manager** Maintains aggregate flow logic representation
- **RCA** Performs inline conflict detection between candidate rule and existing rules
- **Resolution** enables authorization rules of rule produces to resolve conflicts
- **Permission Mediator** enforces Module credential permissions

State Table Generation

Flowmods are expanded to rule candidates

The State Table represents the Flow logic of the tables



Rule	Criteria	Modification	Action
R0	S → M		Op
R1	A → C	A => B	Ot
R2	B → C	C => D	Op
R3	A → D		Drop

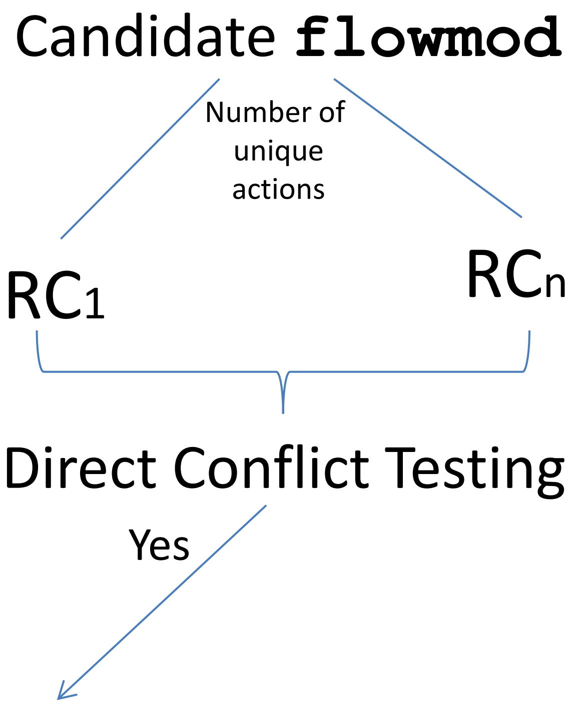
STATE TABLE
R_0
R_0, R_1
$R_0, R_2, \mathbf{R_{1,2}}$

R1+R2 = A → D Tunnel

A → D

There are four output disposition categories (1) output to port, O_P (which may include broadcasts); (2) output to table, O_T; output to controller, O_C; and (4) no output (or Drop).

RCA Rule-Chain Conflict Analysis

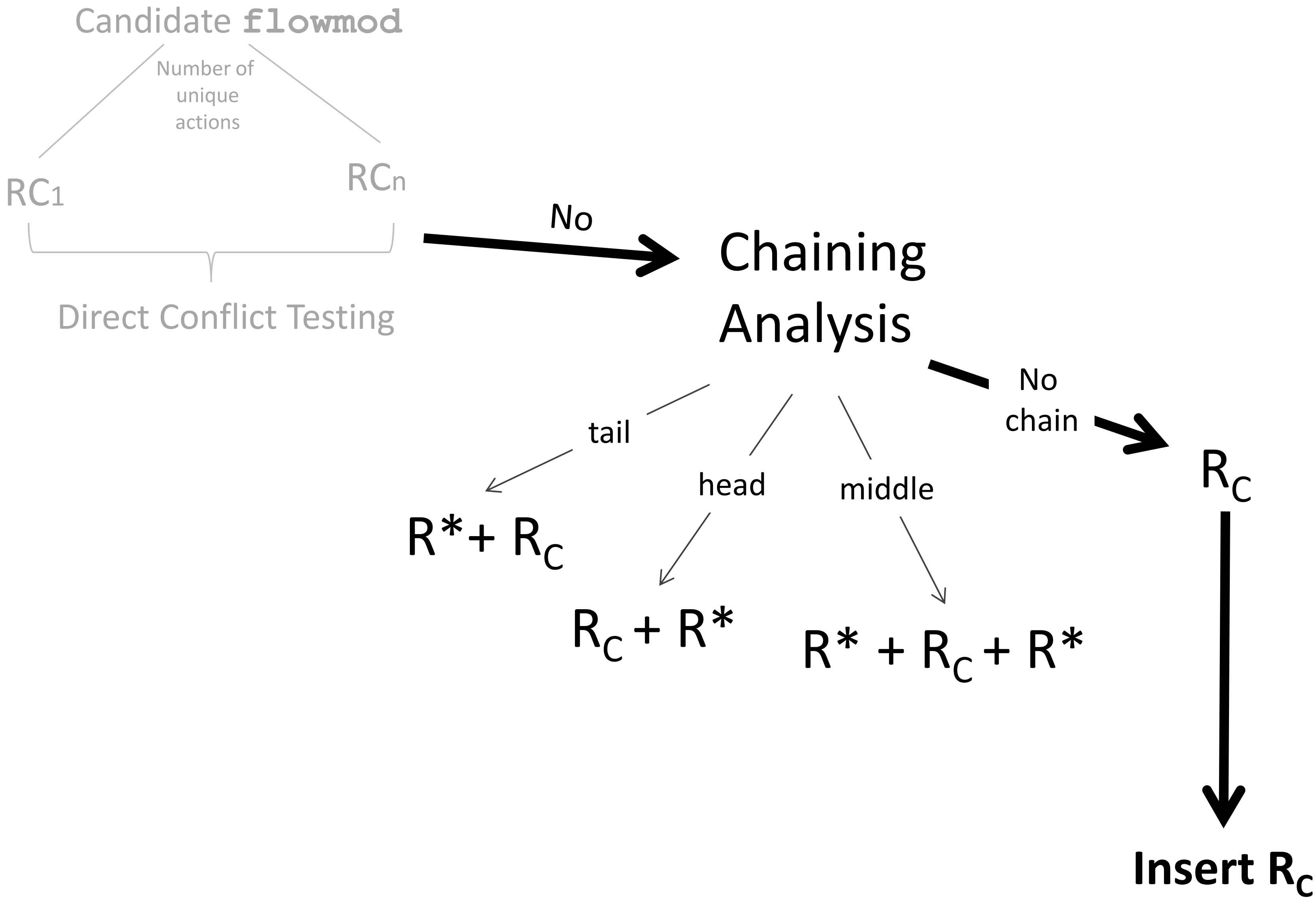


Direct Conflict

arises when RC alters a flow disposition that is currently defined by existing flow rules

Conflict resolution	
RC is lower	Reject RC
RC is higher	Delete conflicting Rs and insert RC
RC is equal	FIFO (reject RC) LIFO (expunge R, accept RC)

RCA



Candidate **`flowmod`**

Number of unique actions

RC_1

RC_n

Direct Conflict Testing

No

Chaining Analysis

tail

head

middle

No chain

$R^* + R_C$

$R_C + R^*$

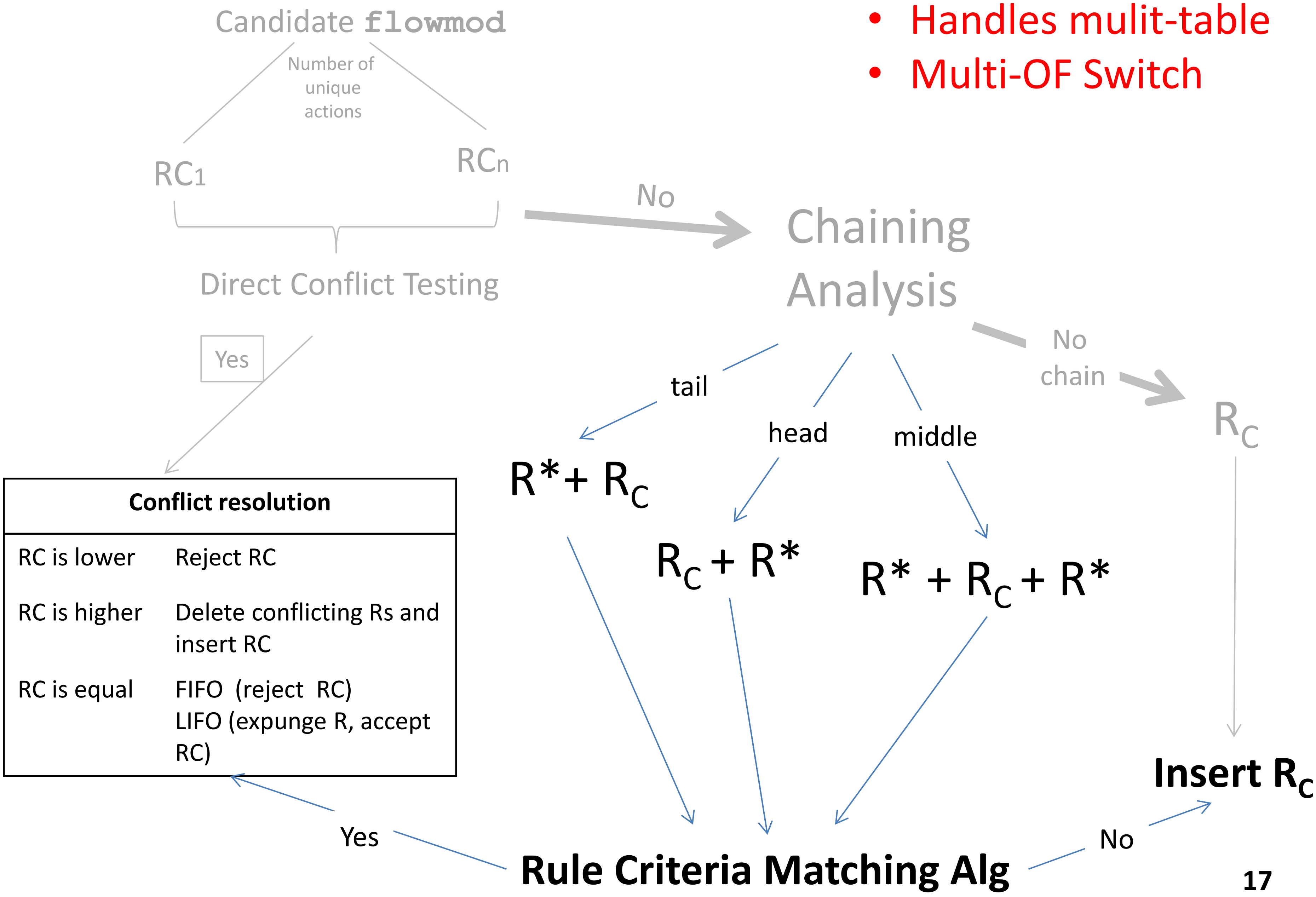
$R^* + R_C + R^*$

R_C

Insert R_C

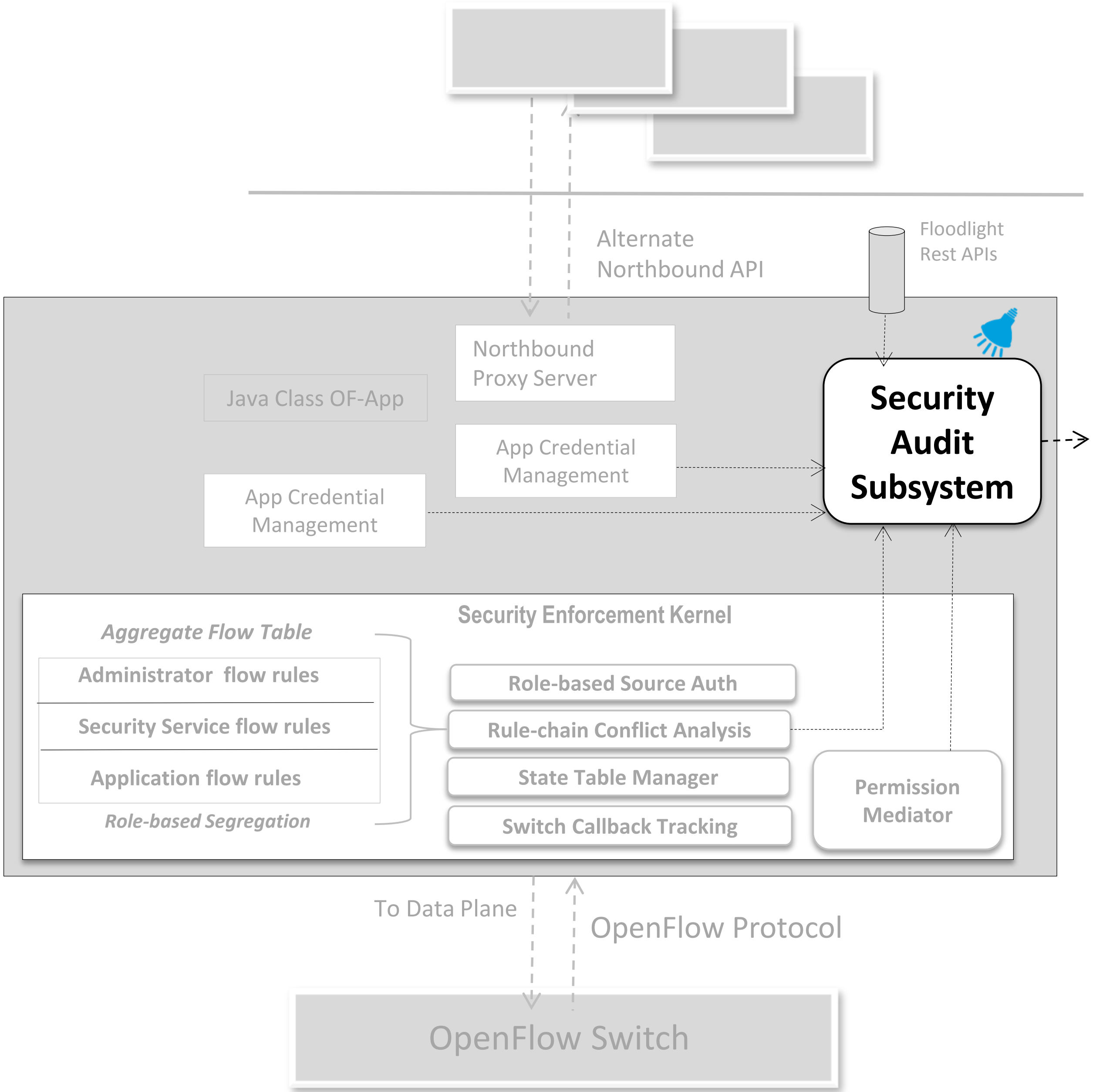
RCA

- Fixes ARR overfitting
- Handles mulit-table
- Multi-OF Switch



Conflict resolution	
RC is lower	Reject RC
RC is higher	Delete conflicting Rs and insert RC
RC is equal	FIFO (reject RC) LIFO (expunge R, accept RC)

Security Audit



SDN Network Auditing

NetSight packet-level flow traversal

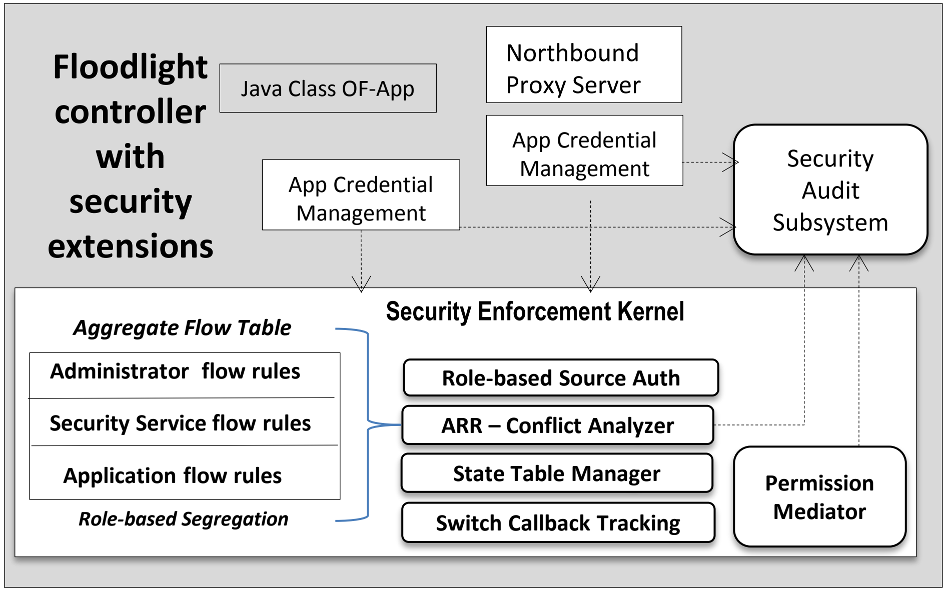
ndb post-card-based route flow route mapping

OFRewind audits and plays back SDN Control Plane traffic

Security audit subsystem

- Flow rule insertions
- Packet_In Events
- All mediation results
- Switch flow table management
- Authentication events
- REST API events

SE-Floodlight



Floodlight controller with security extensions

Java Class OF-App

Northbound Proxy Server

App Credential Management

App Credential Management

Security Audit Subsystem

Security Enforcement Kernel

Aggregate Flow Table

Administrator flow rules

Security Service flow rules

Application flow rules

Role-based Segregation

Role-based Source Auth

ARR – Conflict Analyzer

State Table Manager

Switch Callback Tracking

Permission Mediator

SE-Floodlight

beta1.0 OpenFlow Controller

SE-Floodlight www.openflowsec.org

Inline flow rule conflict detection

Role-based Authorization (conflict resolution)

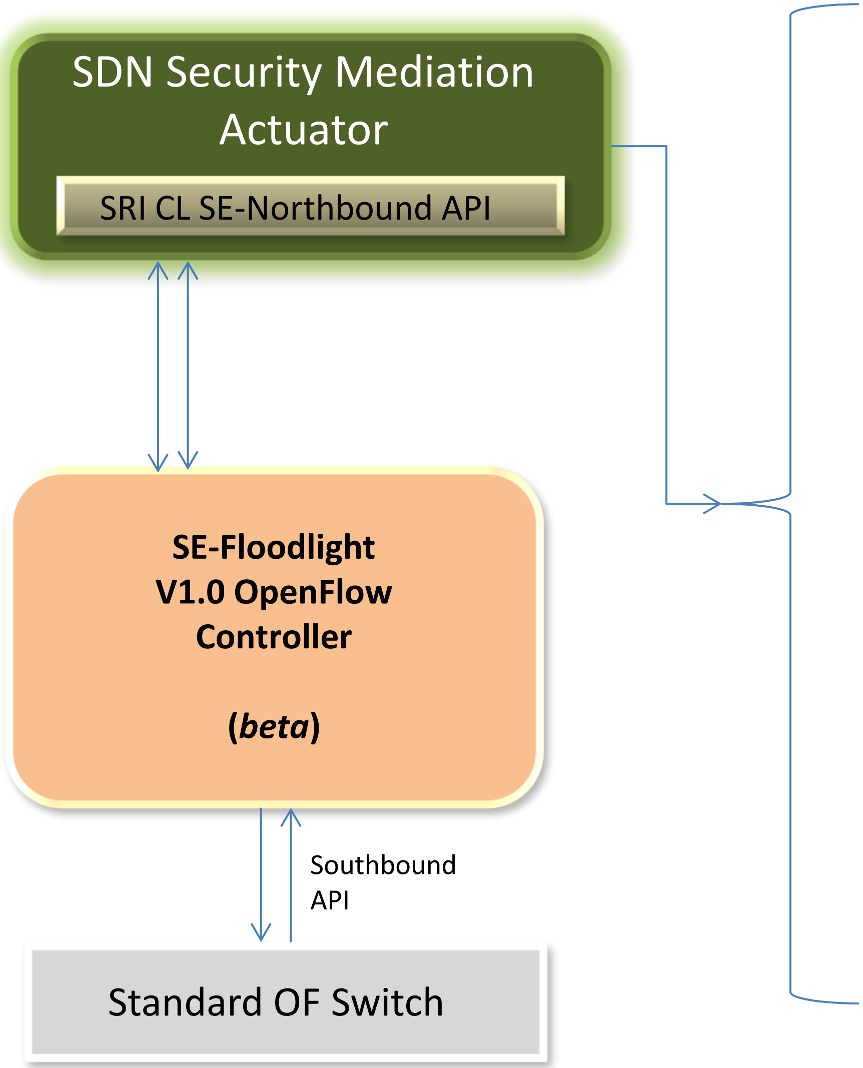
Digital Authentication of FlowRule Source

Privilege Separaton (OF Apps)

Security Audit

Application Permission Model

The Security Actuator Package



SDN Security Mediation Actuator

SRI CL SE-Northbound API

SE-Floodlight V1.0 OpenFlow Controller

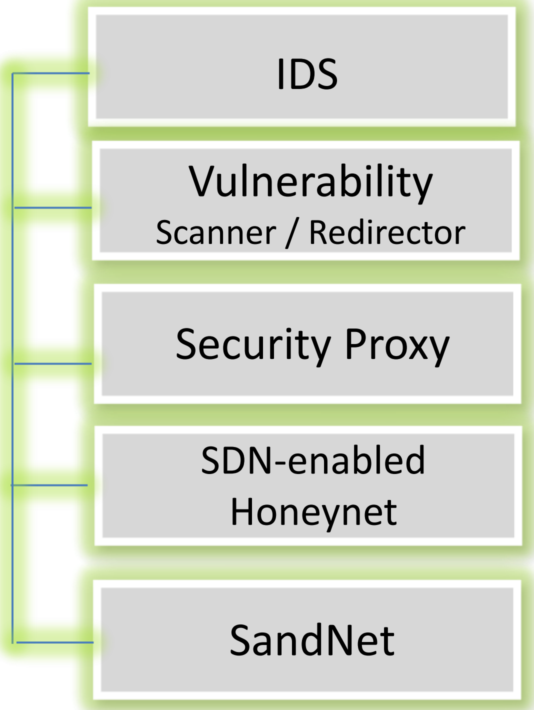
(*beta*)

Southbound API

Standard OF Switch

Security Actuator implements high-level Security directives

- BLOCK
- QUARANTINE
- REDIRECT
- NETMAP
- INFO
- DENY
- UNPLUG
- ALLOW
- UNDO



IDS

Vulnerability Scanner / Redirector

Security Proxy

SDN-enabled Honeynet

SandNet

3rd-parties apps can extend to perform other remediation concepts.

Thank You

More Information

www.openflowsec.org
www.sdnsecurity.org

Acknowledgements

DARPA
MRC

NSF
ACI EAGER Grant