#SDN2012

Welcome!

SDN Security Seminars 2012

#SDN2012 Agenda

February 28th, 2012

5:30pm – 6:00pm	**Networking**
6:00pm – 6:30pm	**Phil Porras, SRI International** Insecurity of OpenFlow/SDNs & Mitigation Techniques
6:30pm – 7:00pm	**Matt Davy and Chris Small, InCNTRE@Indiana U.** Birds of a Feather discussion on Security and SDN
7:00pm – 7:30pm	**Networking**

Event Promoters:

big switch networks

vello SYSTEMS

wiretap

InCNTRE

SRI International

sdn central

#SDN2012

www.sdncentral.com

SDN Security Seminars 2012

Empowering Dynamic Network Defenses Across OpenFlow Networks

Phillip Porras (porras@csl.sri.com)
http://www.csl.sri.com/~porras/
Computer Science Laboratory, SRI International

wiretap InCNTRE SRI International sdn central

What's Interesting Here

Our Vision:

- Help OpenFlow Security Practitioners focus on building composable security algorithms : Providing an API to abstract details til the dust settles
- An OpenFlow security kernel extension that enforces policy and facilitate greater security compliance
- An application scripting framework that will enable us to push out many cool antimalware / INFOSEC services that leverage OpenFlow

Our Approach:

- **FORT-NOX**: A security kernel for enforcing flow constraints produced by OF Security applications
- **FRESCO**: an application framework for rapid security service implementation

wiretap InCNTRE SRI International sdn central

Why is OF Cool for Security Research?

Decoupling network flow decision from the routers allows enables control apps to consider many dimensions

OpenFlow Application

Elastic Computing

Virtual Network Slicing

Network Hypervisors

Dynamic Net Orchestration

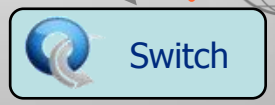
Host B

Host A

wiretap

InCNTRE

SRI International



sdn central

Why is OF Cool for Security Research?

- ***Exactly where NETSEC Lives***
- ***Dynamic Policies are Exciting***
- ***Inline Flow Decisions = Prevention / Response***

The potential to Detect, Alarm, And Execute a Coherent Response

OpenFlow Application

Host B

Host A

wiretap

InCNTRE

SRI International

sdn central

Apps I'd Like to Build

Tarpits: A Tarpit is an advanced anti-attack countermeasure designed to hold (reverse-DoS) inbound TCP connections from attackers

Reflector Nets (*): A FRESCO script may reprogram the OF network to forward an external entity into a remote honeynet

Phantom Nets: A technique in which a scanner is mislead into producing a false topology map for the network being scanned

Emergency Broadcast: When a switch-wide exceptional state is detected, a FRESCO script may auto-insert a high-priority forward rule for all connections originating from network operator owned addresses, while inserting drop filters to reject detected flooding sources/ports

White holes: A strategy for defeating sophisticated density-aware IP scanning techniques , which is are used by scan-and-infect malware to increase the rate at which viable infection targets are discovered

BotHunter: A method for diagnosing infections in internal network assets using dialog correlation to discover flow sequences that match coordination centric malware infections

wiretap InCNTRE SRI International sdn central

Many More: TRW (*), BotMiner (*), P2P Plotter (*)

…Thinking about SDN Security

Classic Network Perimeter Defense

- Provide a well-defined security policy instantiated for a target topology
- Vet both policy and network for compliance
- Deploy policy enforcement consistently across the network
- Test and monitor the network for violations

wiretap InCNTRE SRI International sdn central

…Thinking about SDN Security

Security Cant Wait for Dust To Settle

- Lets build BotHunter once, agnostic to OF protocol versions, Switch implementations, the Controller make/model
- Learn now … innovate now … influence now

Security Policy Enforcement

- Policy is a function of what connection requests are received …
- OF apps can compete, contradict, override one another, incorporate vulnerabilities
- Worst case: an adversary can use the deterministic OF app to control the state of all OF switches in the network

wiretap InCNTRE SRI International sdn central

…Thinking about Security

Least Privilege

- Don't lay trust where its NOT needed
- Enable flow rule priorities: Admin, NetSec App, OF Apps
- Role Separation / Controller Process Protection

Distributed Synchronization of Policy

- Distributed policy insertion must be atomically synchronized
- Distributed policy removal must be atomically committed: harder

wiretap InCNTRE SRI International sdn central

…Issues

We'd like the robustness of our network security posture to not rely on the absence of

- Vulnerabilities in OF applications
- Malicious code in 3rd party OF apps
- Complex interaction that arise of OF app interactions
- State inconsistencies due to switch garbage collection or policy coordination across distributed switches
- Sophisticated OF applications that employ packet modification actions
- Adversaries who might directly target our security services to harm the network

wiretap InCNTRE SRI International sdn central

FortNOX and FRESCO

wiretap

InCNTRE

SRI International

sdn central

What is FortNOX

Objectives:

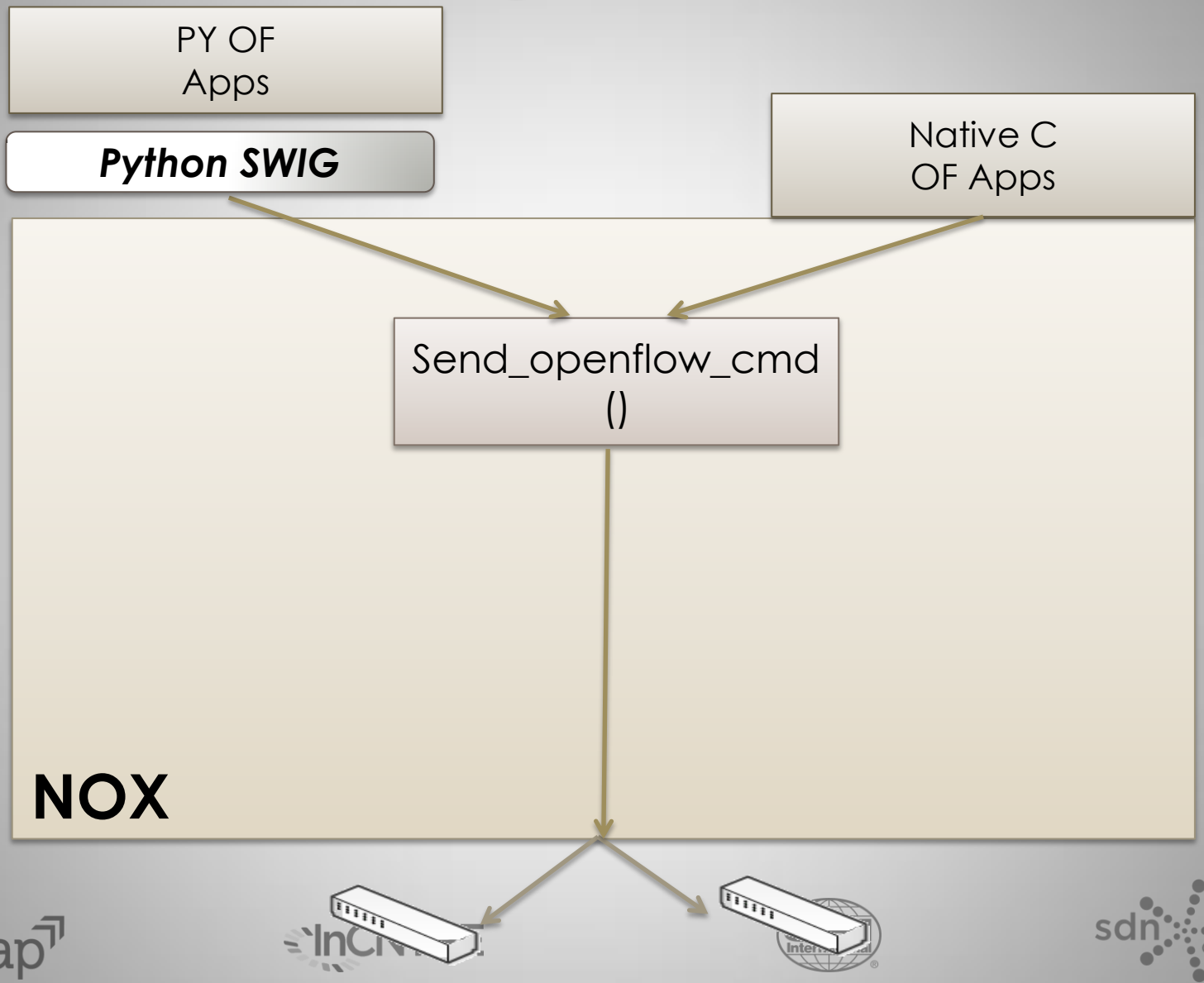
Enable automated security services to produce dynamic flow policy constraints with guaranteed enforcement

FortNOX: *a security kernel for NOX*

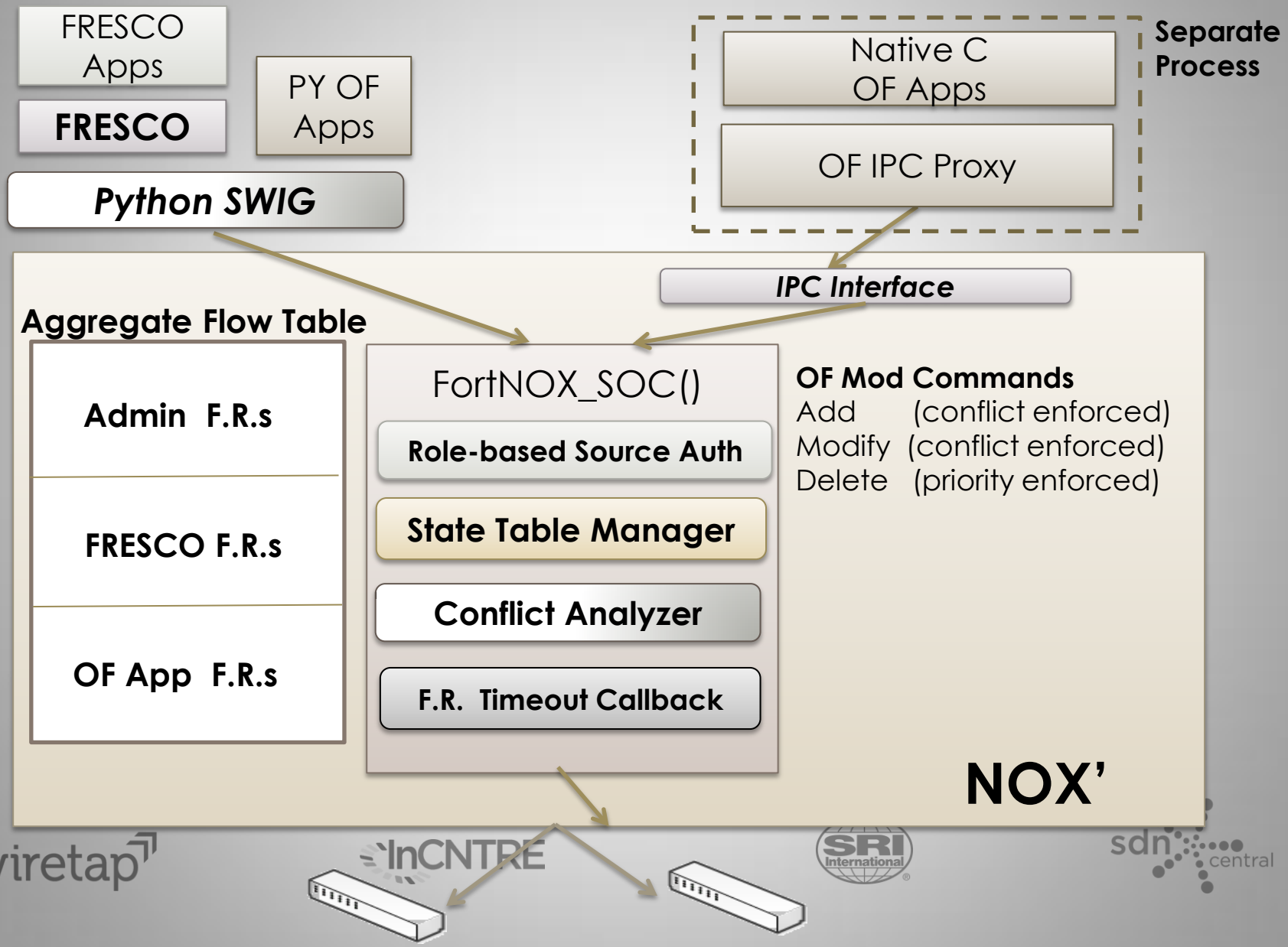
- A non-bypassable mediation service that performs inline vetting of new OF application flow rules against security constraints
- Provide a supportive framework to FRESCO that enables FRESCO policy actions

wiretap InCNTRE SRI International sdn central

Architecture Integration



Architecture Integration



Flow Rule Conflict Resolution

A Candidate Rules

Match: a → b

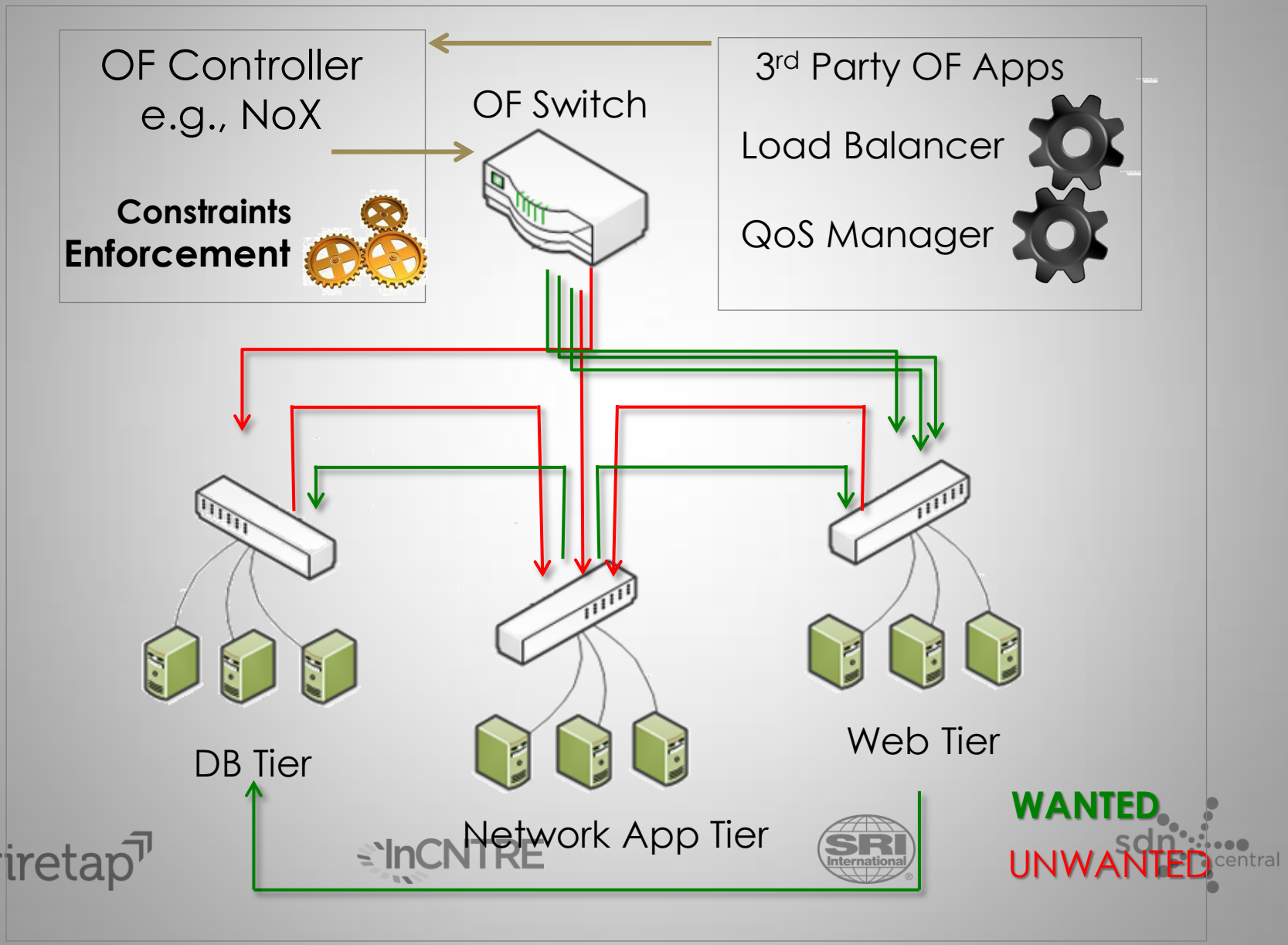
Actions:
a ← a'
b ← c
forw

Conflict Resolution

- Derive ARRs per candidate rule
- Compare each ARR against FortNox's Aggregate Flow Table
- **IF** ARR intersects with registered rule **Then** flag candidate rule if ARR conflicts
  - Possible Resolution
    - Based on role-based priority
      - EQ - *policy*
      - GR - DEL, ADD
      - LT - REJECT

wiretap InCNTRE SRI International sdn central

Putting This in Context



A Demonstration

http://goo.gl/En7f2

wiretap

sdn central

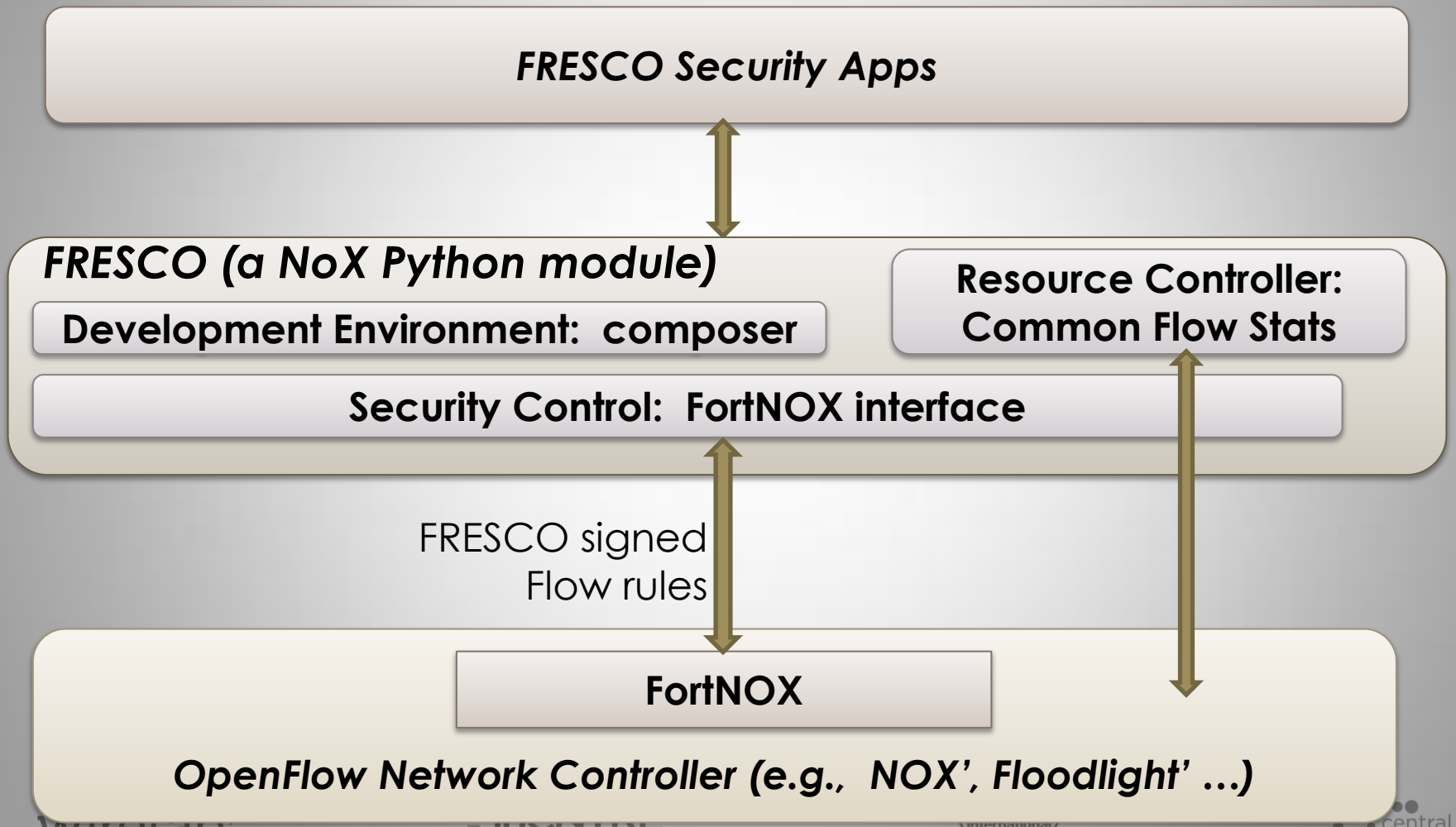
What is FRESCO

An application framework for rapidly deploying security applications in OpenFlow Networks

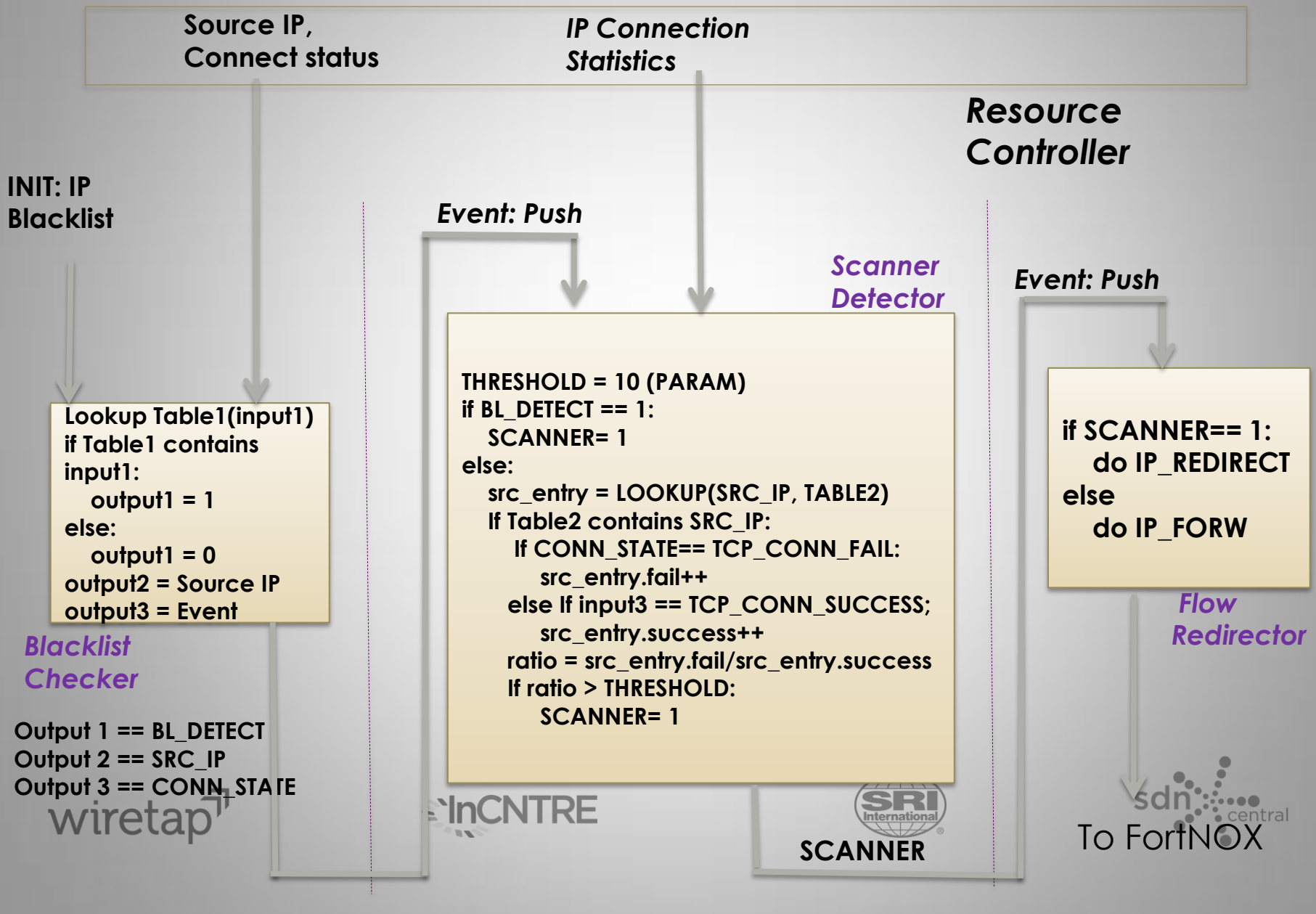
- FRESCO takes inspiration from Click in its goals for building a scripting framework for rapid security prototyping
- FRESCO scripts are translated into OF controller modules that
  - OBSERVE FLOWS/SWITCH STATE
  - DECIDE NETWORK POLICY
  - INSERT NON-BYPASSABLE FLOW CONSTRAINTS INTO SWITCHES and CONTROLLERS
- FRESCO modules *compose* into full security services

wiretap InCNTRE SRI International sdn central

What FRESCO Provides



Example : ReflectorNet



Example: A ReflectorNet

MODULE_START:Scan1
EVENT:TCP_CONNECTION_FAIL, TCP_CONNECTION_SUCCESS
INPUT: SRC_IP
OUTPUT: Result, Input1, Event
PARAMETER: -
MODULE_END: -

Blacklist Checker

MODULE_START:Scan2
EVENT:PUSH
INPUT:Scan1-0, Scan1-1, Scan1-2
OUTPUT: Result
PARAMETER:10
MODULE_END: -

Scanner Detector

MODULE_START:Scan3
EVENT:PUSH
INPUT:Scan2-0
OUTPUT:-
PARAMETER:-
MODULE_END:

Flow Redirector

wiretap InCNTRE SRI International sdn central

Status and Directions

Coming Soon: www.openflowsec.org

- Technical Reports
- Videos: FortNoX, FRESCO, Sample Apps (Reflector nets, Antiscanner phantom topology generator, BotMiner, P2P Plotter, BotHunter, …)
- FortNOX beta, single switch (multi-switch will follow)
- FRESCO beta
- Several FRESCO Apps
- Demo Mininets, VMs for test, code templates

- **DARPA MRC**: SRI and Cambridge/UK (*advisor BigSwitch*): High Assurance SDNs with no central control logic

wiretap InCNTRE SRI International sdn central

wiretap

InCNTRE

SRI International

sdn central

Related Work

Extensible Networking: software for extending control planes in networks

- Software Routing: CLICK, XORP
- Using CLICK for Security Control Apps: BotProbe, GQ, iSink

Firewall and Interdomain Routing Policy Management: Testing and validating security policies in single and distributed networks

- Firewall Design Diagrams [Liu08]
- Testcase gen: [Senn05, El-atawy07]
- Verifying FW policies [Seen05, Lie08, Al-shaer09, Xie05, Al-shaer10]
- Wide Area Reachability Analysis [Al-shaer09, Xie05]

Enterprise Network Protection Architectures: clean slate

- SANE [Casado06] : clean slate. Centralized servers, domain controllers, authenticate host to switch.
- ETHANE [Casado07] : can coexist in traditional nets, proposes a higher-level net policy scripting language for enterprise management
- vs FRESCO – complementary: a framework for rapid prototyping of composable security libraries to create full antimalware services.

FlowVisor [Sherwood07] : Network Slicing separates logical net planes to enable *non-interference* among OF apps.

wiretap InCNTRE SRI International sdn central