Practical and Incremental Convergence between SDN and Middleboxes

Zafar Qazi
Cheng-Chun Tu
Luis Chiang
Vyas Sekar

Rui Miao
Minlan Yu


Stony Brook University

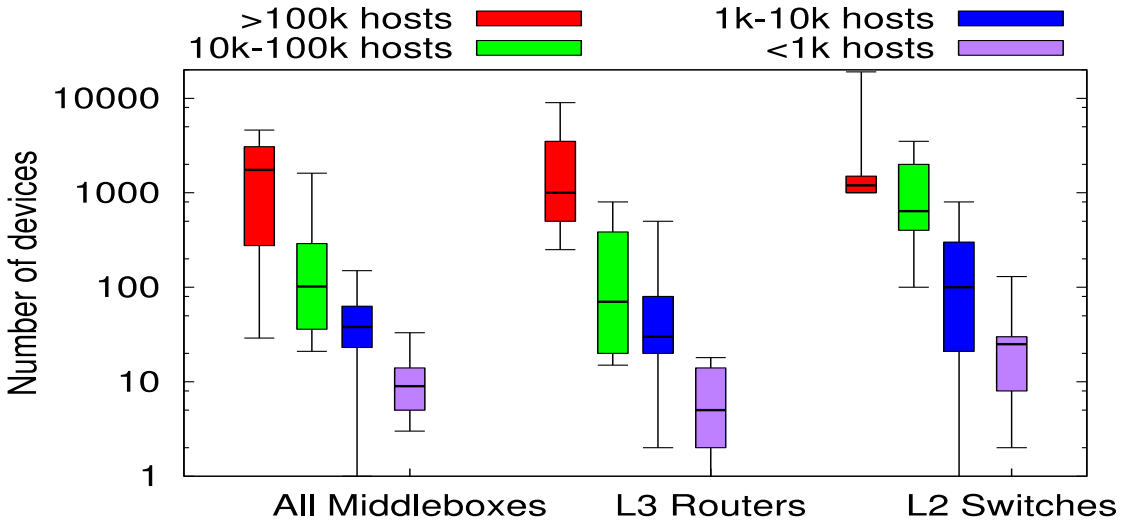

USC University of Southern California

Why middleboxes?

Data from a large enterprise

Type of appliance	*Number*
Firewalls	166
Intrusion detection	127
Media gateways	110
Load balancers	67
Proxies	66
VPN gateways	45
WAN Optimizers	44
Voice gateways	11
Total Middleboxes	***636***
Total routers	***~900***

Survey across 57 network operators



Critical for security, performance, compliance
But painful to manage

Why should SDN community care?

Aug. 2012 ONF report

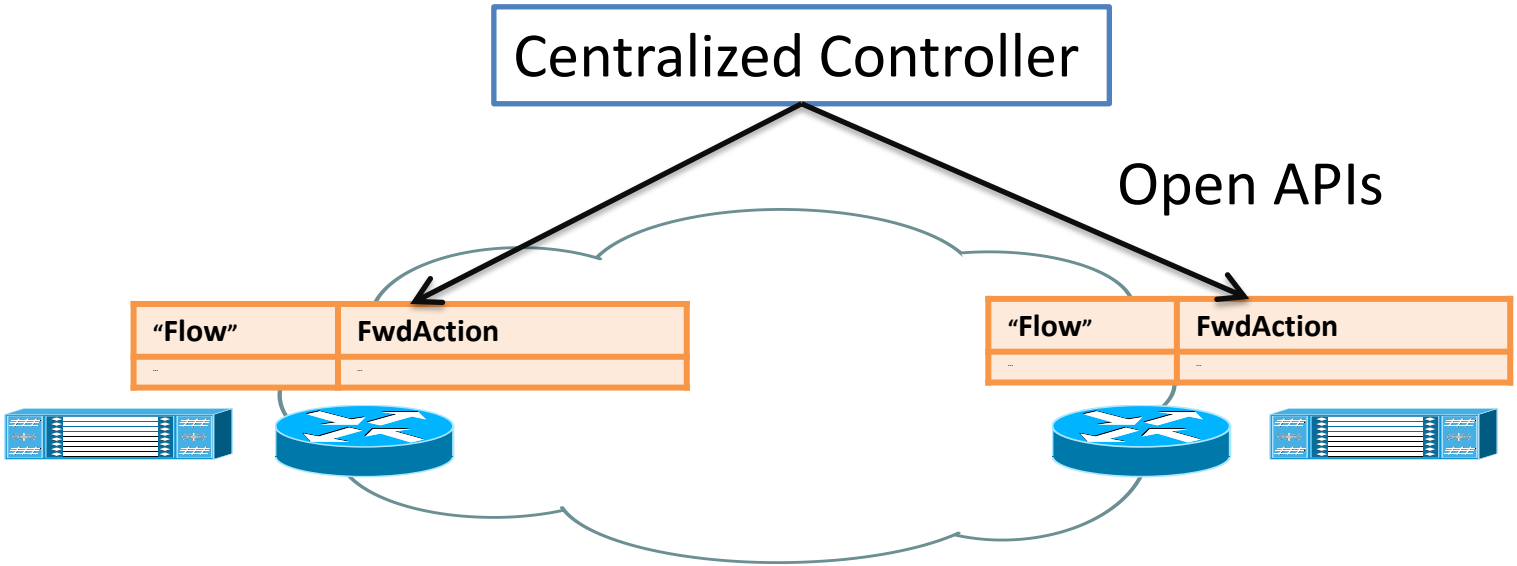
- "integrate into production networks"
- "APIs for functions market views as important"

Survey on SDN adoption [Metzler 2012]

- "use cases that justify deployment"
- "add a focus on Layer 4 through Layer 7 functionality … change in the perceived value of SDN."

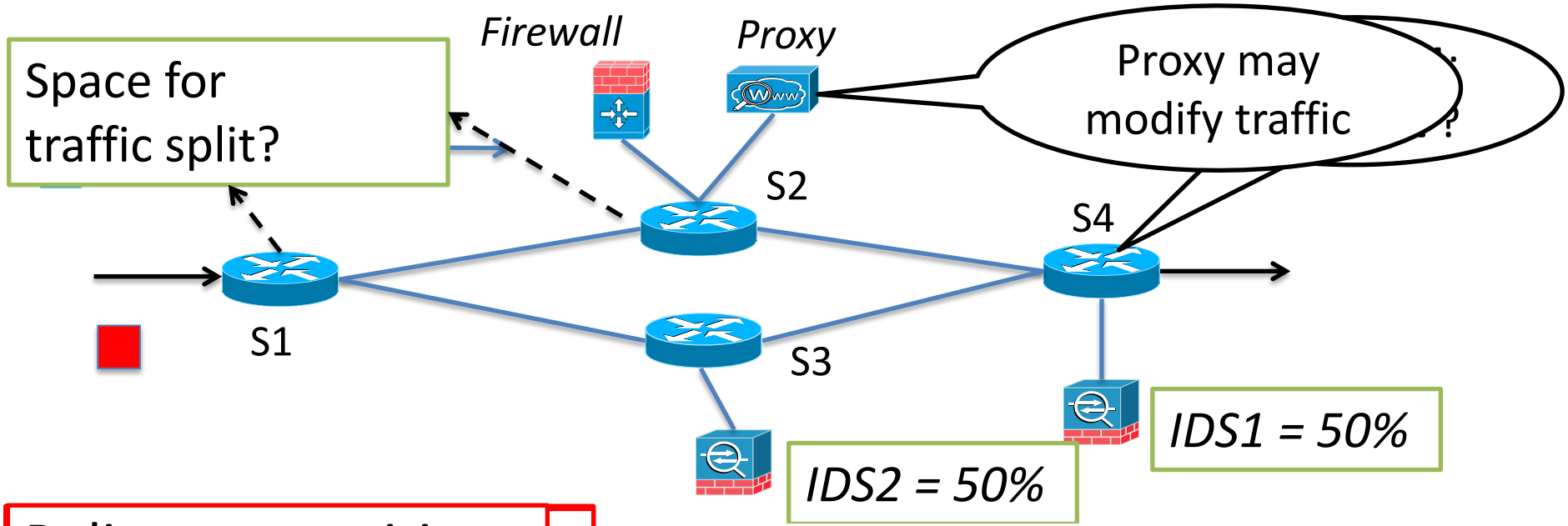
Middleboxes: *Necessity* and *Opportunity* for SDN

Goal: SDN + Middlebox integration



Can we achieve SDN-Middlebox integration:
with *existing* SDN APIs?
with *unmodified* middleboxes?

Challenges in SDN-MB integration



Policy composition

Simple flow rules may not suffice!

Are forwarding rules correct?

Recap: Three main challenges

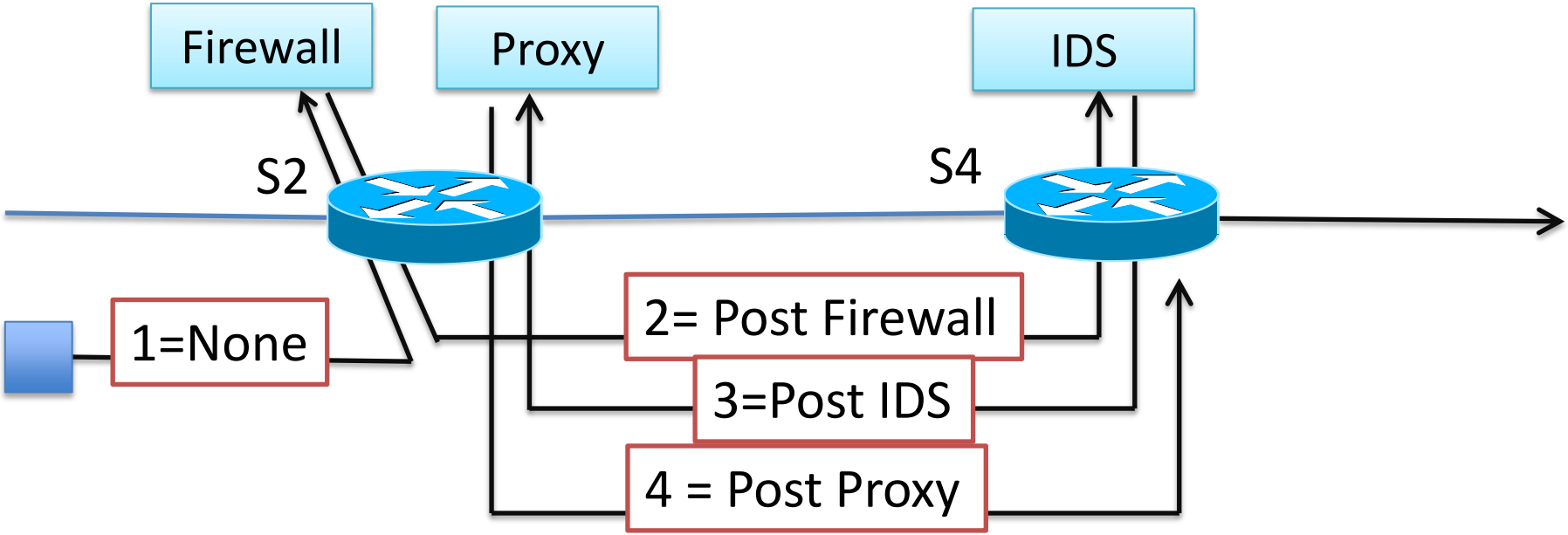
Policy composition → *Flow rules may not suffice*

Resource constraints → *Is there enough rule space?*

Traffic modifications → *Correctness?*

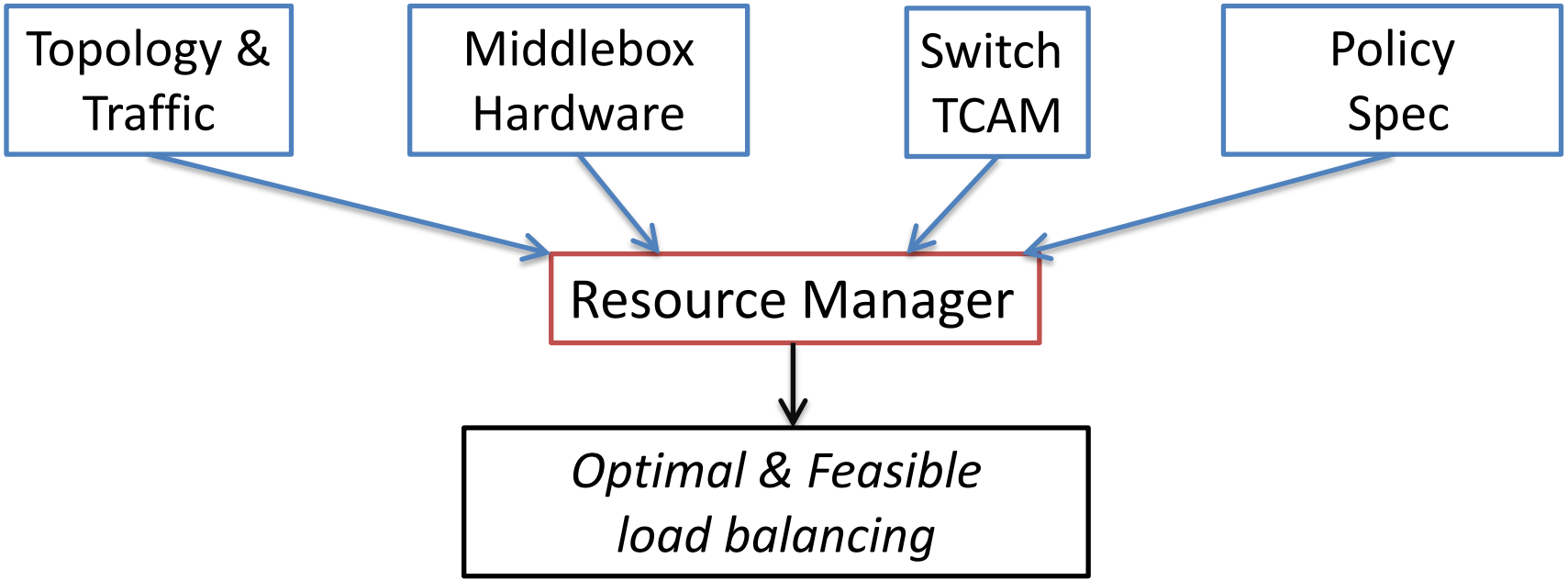
New dimensions beyond Layer 2-3 tasks

Composition → Tag Processing State



Use “state” tags in addition to header, interface info

Resource constraints→ Joint Optimization



Theoretically hard, but have practical near-optimal heuristics

NIMBLE System Overview

Web → FW → IDS → Proxy

Resource Manager
(Scalable joint optimization)

Modifications Handler
(Infer flow correlations)

Rule Generator
(Processing state tags, Switch tunnels)

POX extensions

OpenFlow 1.0

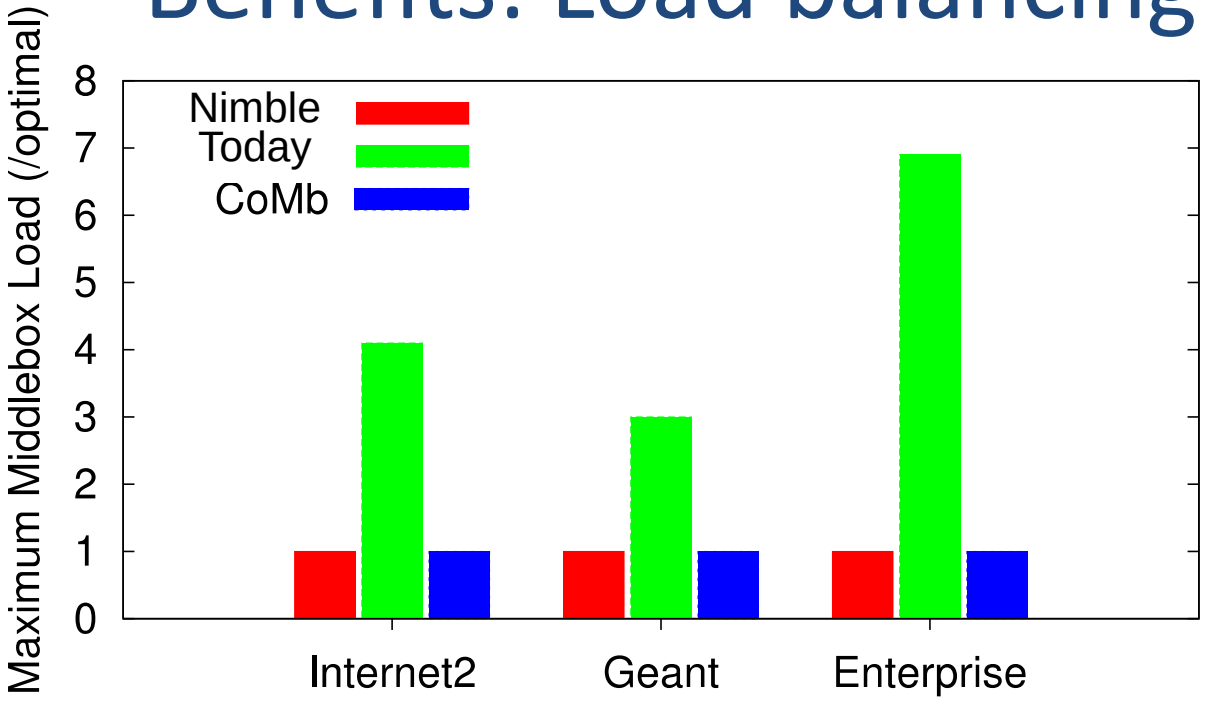
Flow	Tag/Tunnel	Action
..		..

Flow	Tag/Tunnel	Action
..		..

Legacy Middleboxes

OpenvSwitch 1.7.1

Benefits: Load balancing



4-7X better load balancing without modifying middleboxes

Low overhead: 0.1s to reconfigure after failure/overload

SDN + Middlebox Convergence

Middlebox pain points

High OpEx

Inflexible

High CapEx

NIMBLE
Practical Integration
[today's talk]

APLOMB
Cloud Outsourcing
[SIGCOMM'12]

COMB
Consolidation
[NSDI '12]
ONS Poster