

FlowGuard: Building Robust Firewalls for Software-Defined Networks

Hongxin Hu[†], Wonkyu Han[‡], Gail-Joon Ahn[‡] and Ziming Zhao[‡]



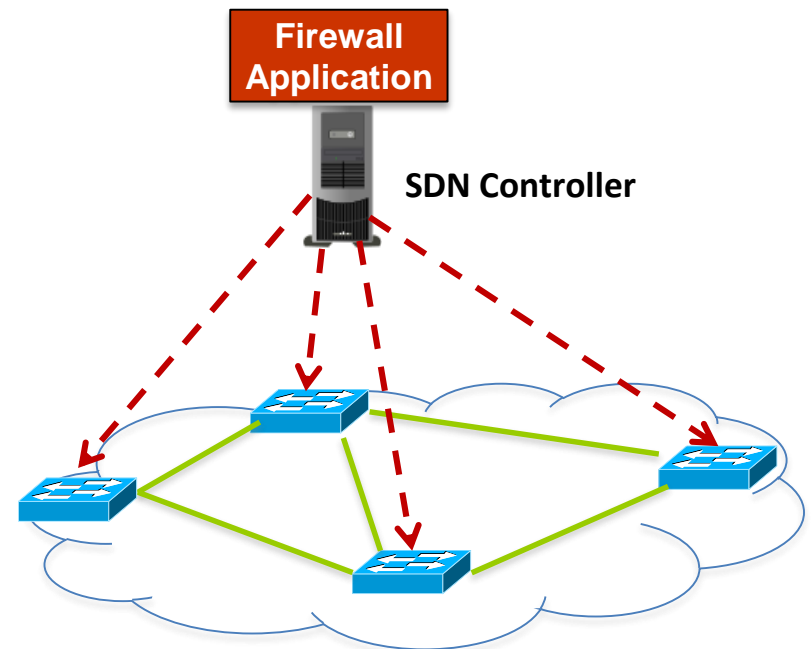
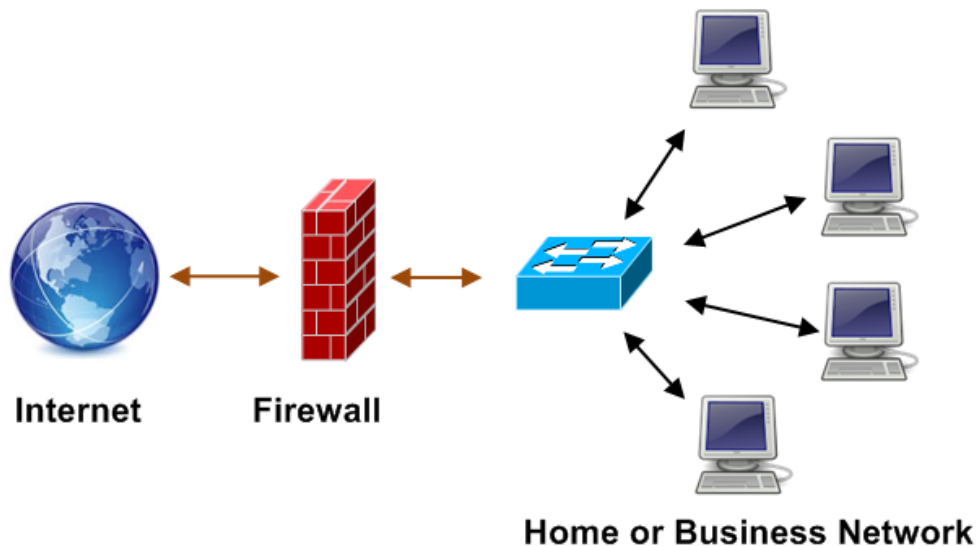
HotSDN 2014

Outline

- Introduction
- Challenges for Building FW in SDN
- FlowGuard framework
 - Violation Detection Mechanism
 - Resolution Mechanism
- Conclusion

Traditional Firewalls Vs. SDN Firewalls

- Traditional FWs: all insiders are **trusted**
 - Internal traffic is not seen and cannot be filtered by the traditional firewall
- **SDN FWs: monitoring all insiders**



Challenges

■ Examining **Dynamic** Network Policy Updates

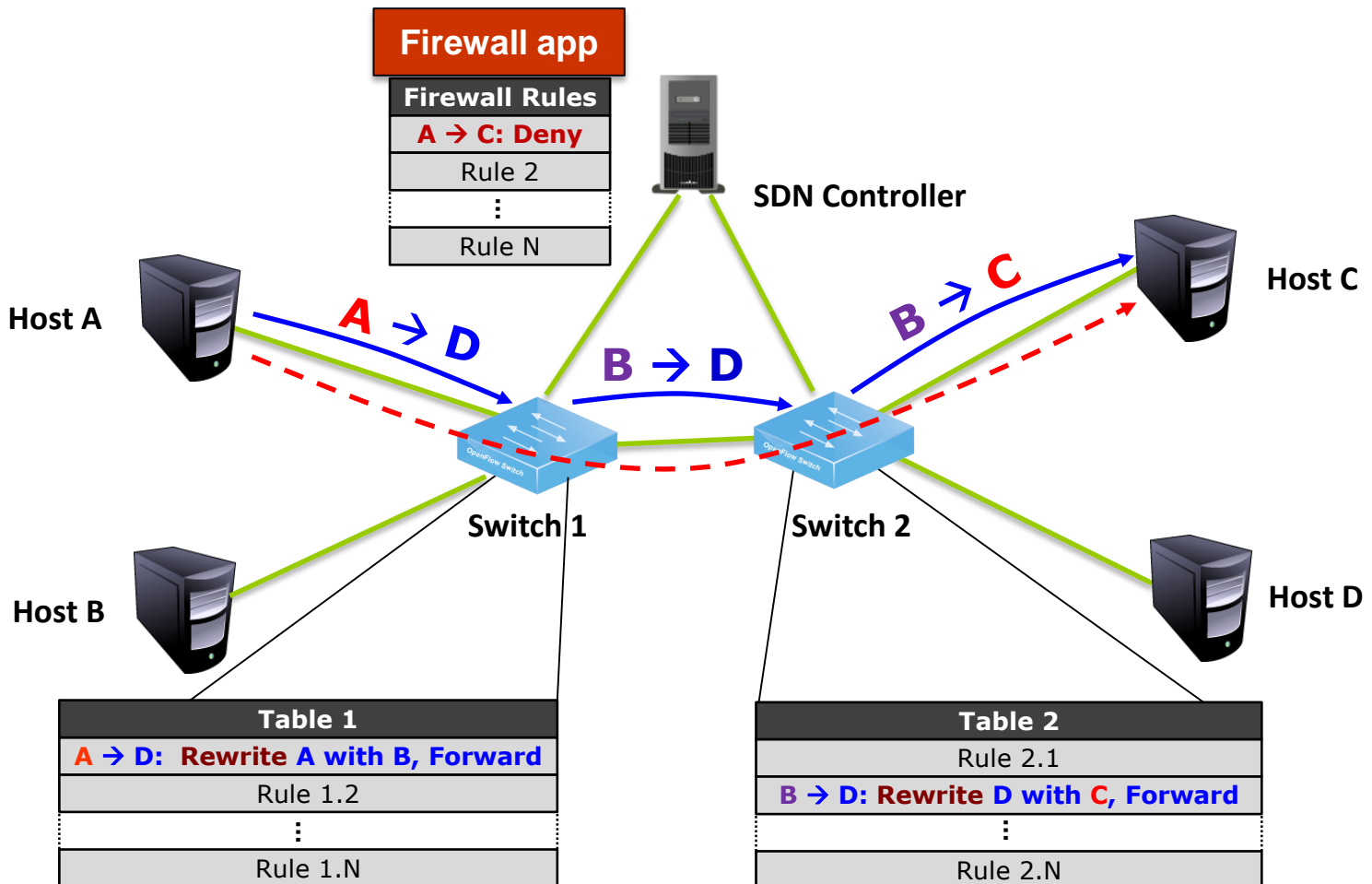
- A firewall in SDN is both
 - ▶ Packet Filter + **Policy Checker**
 - The **first packet** goes through the controller and is filtered by firewall
 - The **subsequent** packets of the flow directly match the flow policy

■ Checking Indirect Security Violations

- **Indirect violation** caused by
 - ▶ **Dynamic packet modification**
 - OpenFlow allows an action, **Set-Field**, which can rewrite packet header
 - ▶ **Rule dependency**
 - Dependency relation depends on their priority
 - Rules may overlap **partially / entirely** each other (inter / intra table)

Challenges (cont'd)

■ Indirect violation scenario



Challenges (cont'd)

■ Architecture Options

● Centralized SDN firewall

- ▶ Firewall policy is **centrally** defined and enforced at the controller
- ▶ Limitation: cannot deal with **partial** policy violations

● Distributed SDN firewall

- ▶ Firewall policy is defined centrally, but propagated and enforced at each **individual** flow entry (ingress switch)
- ▶ Limitation: needs a complicated **revocation** and **repropagation** mechanism to handle **dynamic** policy updates

State Of The Art

■ SDN Firewall App

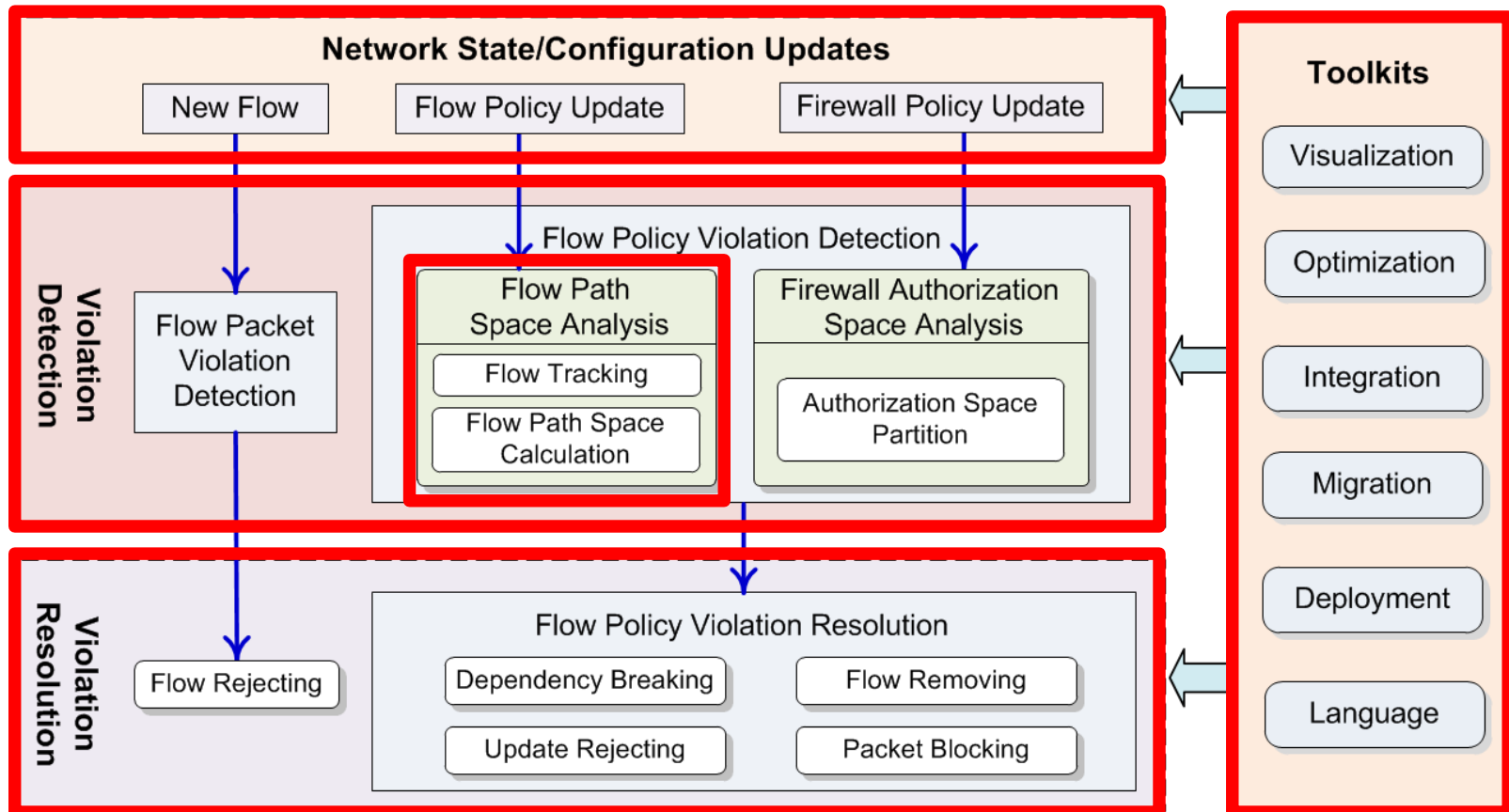
- Built-in firewall application in Floodlight
 - ▶ Limited to check *flow packet* violations and unable to examine *flow policy* violations

■ Policy Conflict Detection and Resolution

- VeriFlow [Khurshid'13] and NetPlumber [Kazemian'13]
 - ▶ Lack of automatic, effective and *real-time* violation resolution
- Pyretic [Monsanto'13]
 - ▶ Cannot discover and resolve *indirect* security violations
- FortNOX [Porras'12]
 - ▶ Only conducts *pairwise* conflict analysis without considering *rule dependencies* in flow tables and firewall policies

Our Approach

- **FlowGuard**: a comprehensive framework for building robust SDN firewalls

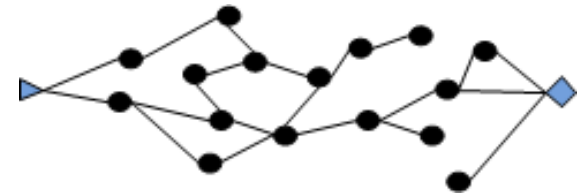


Space Analysis

■ Flow Path Space Analysis

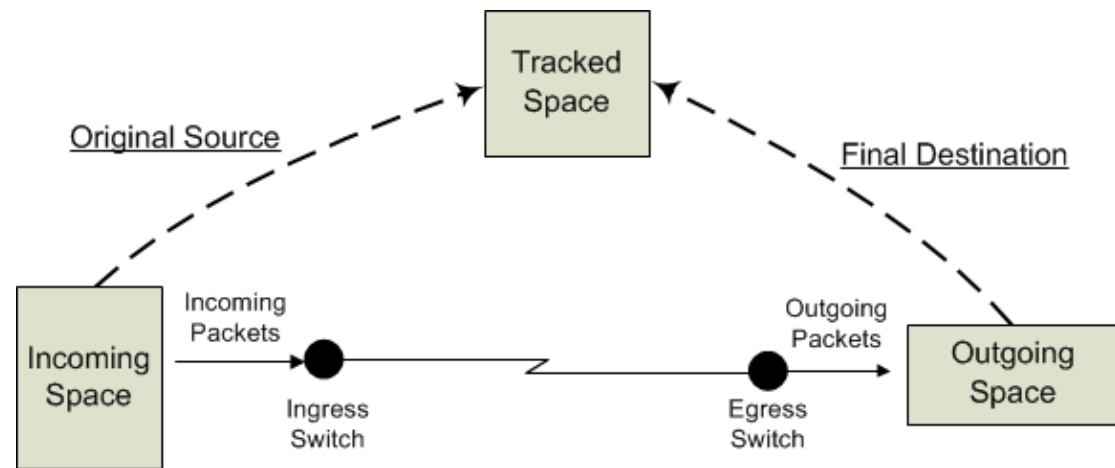
- Flow tracking graph(NetPlumber [Kazemian'13])

- ▶ Dynamic packet modification
- ▶ Rule dependency



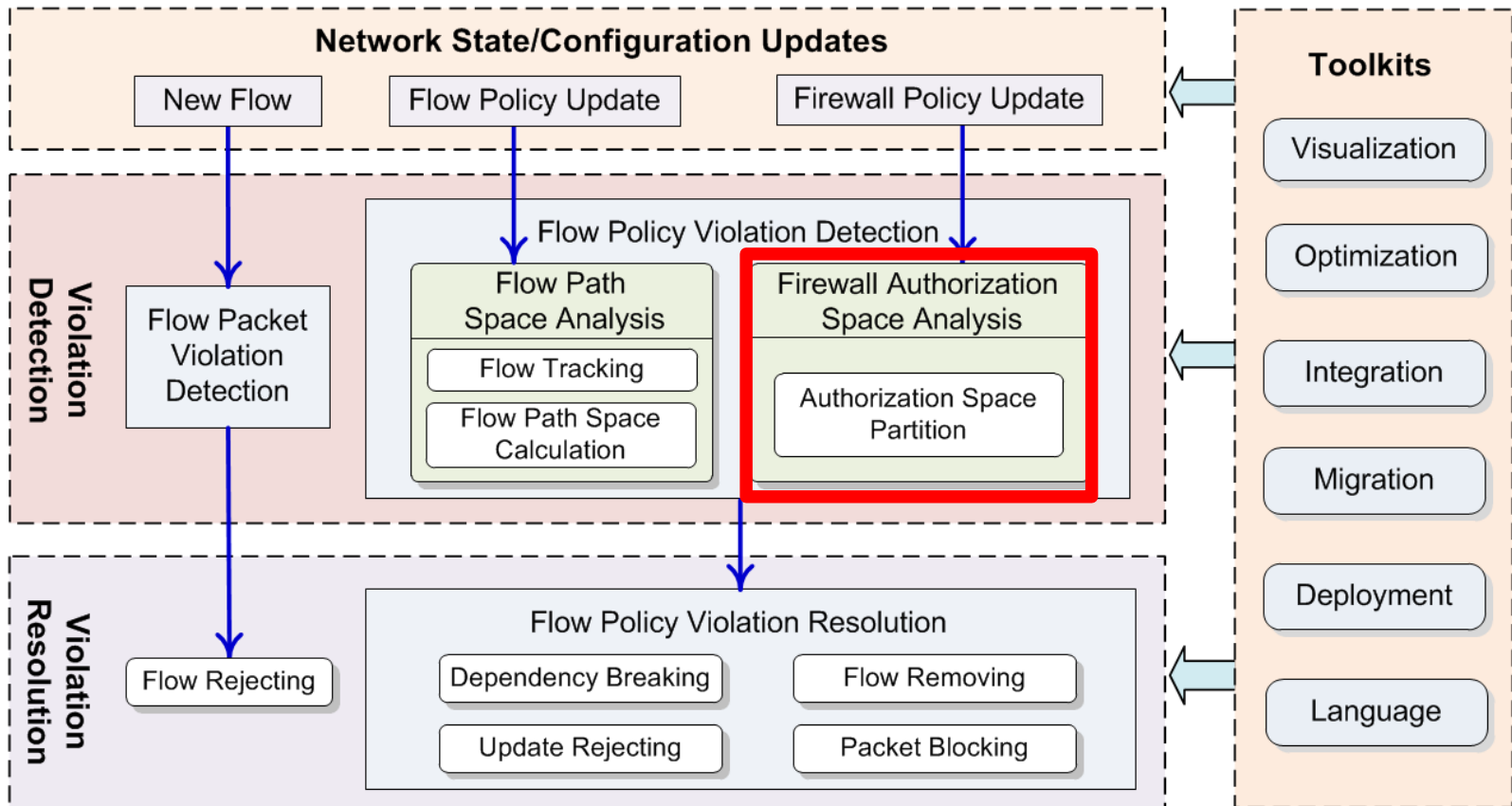
- Flow path space calculation

- ▶ Incoming space
- ▶ Outgoing space
- ▶ Tracked space



Our Approach

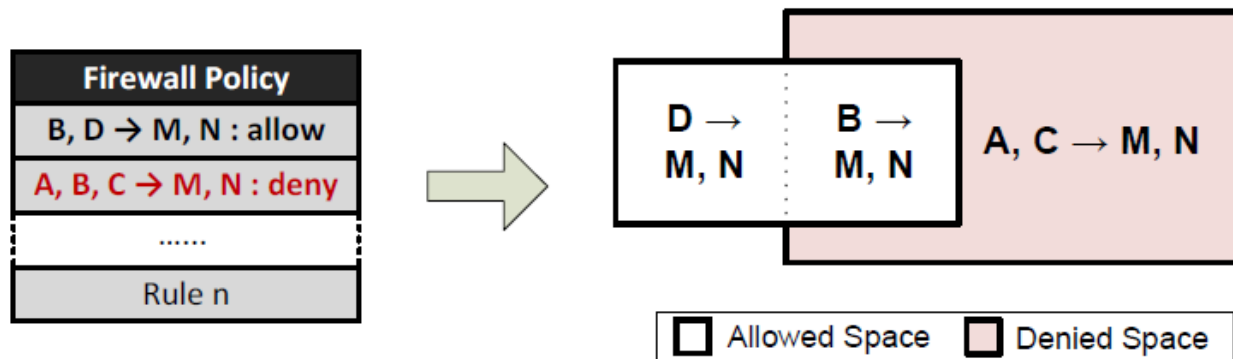
- **FlowGuard**: a comprehensive framework for building robust SDN firewalls



Space Analysis (cont'd)

■ Firewall Authorization Space

- Decouple dependency relations between “allow” rules and “deny” rules in the firewall policy
 - ▶ Denied authorization space
 - ▶ Allowed authorization space

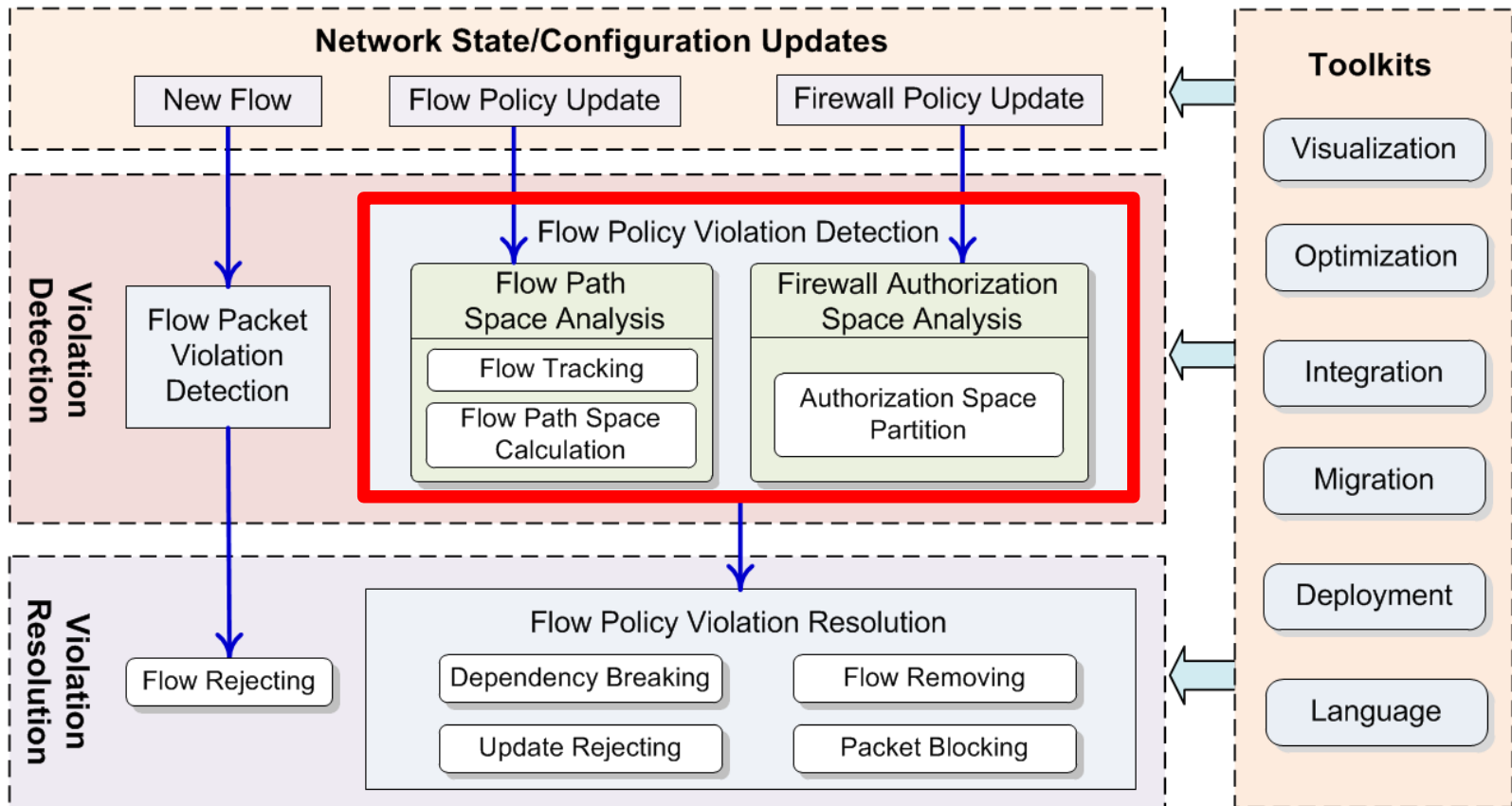


(a) Example firewall policy

(b) Authorization space partition

Our Approach

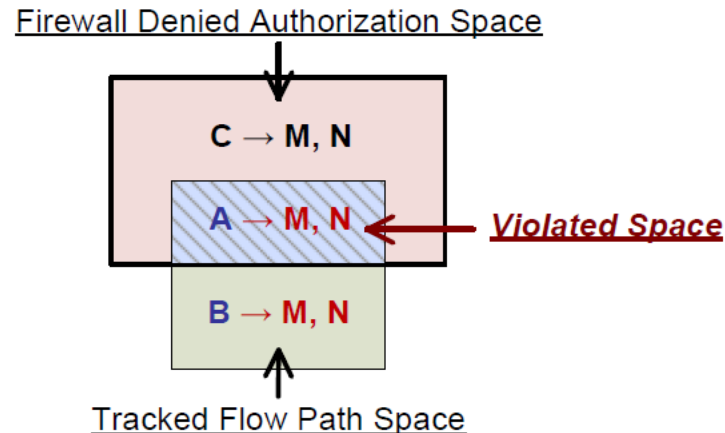
- **FlowGuard**: a comprehensive framework for building robust SDN firewalls



Violation Detection

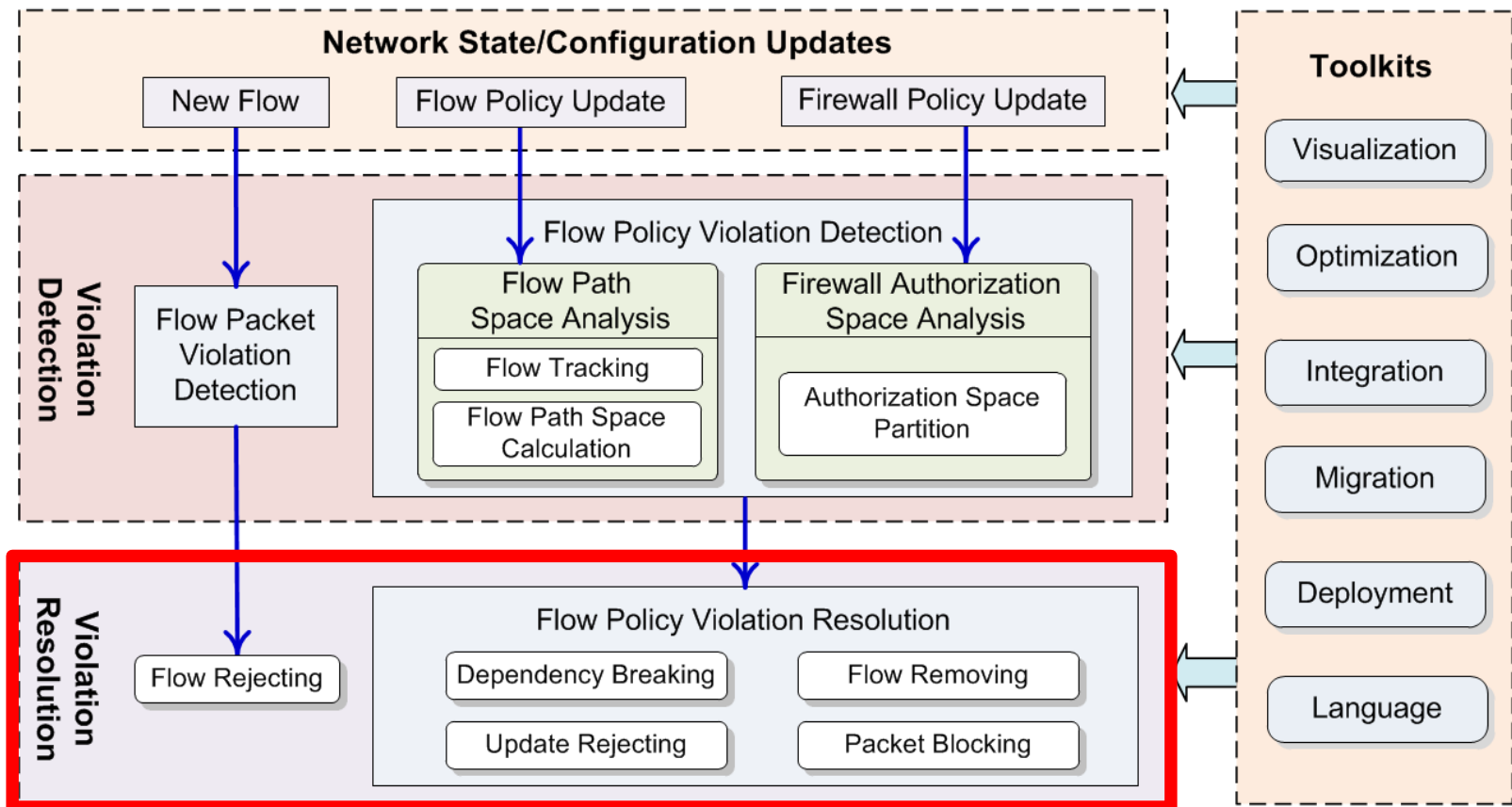
■ Space Comparison

- Compare Tracked Flow Space against Firewall Denied Authorization Space
 - ▶ Entire Violation
 - Denied authorization space includes whole tracked space
 - ▶ Partial Violation
 - Denied authorization space partially includes tracked space



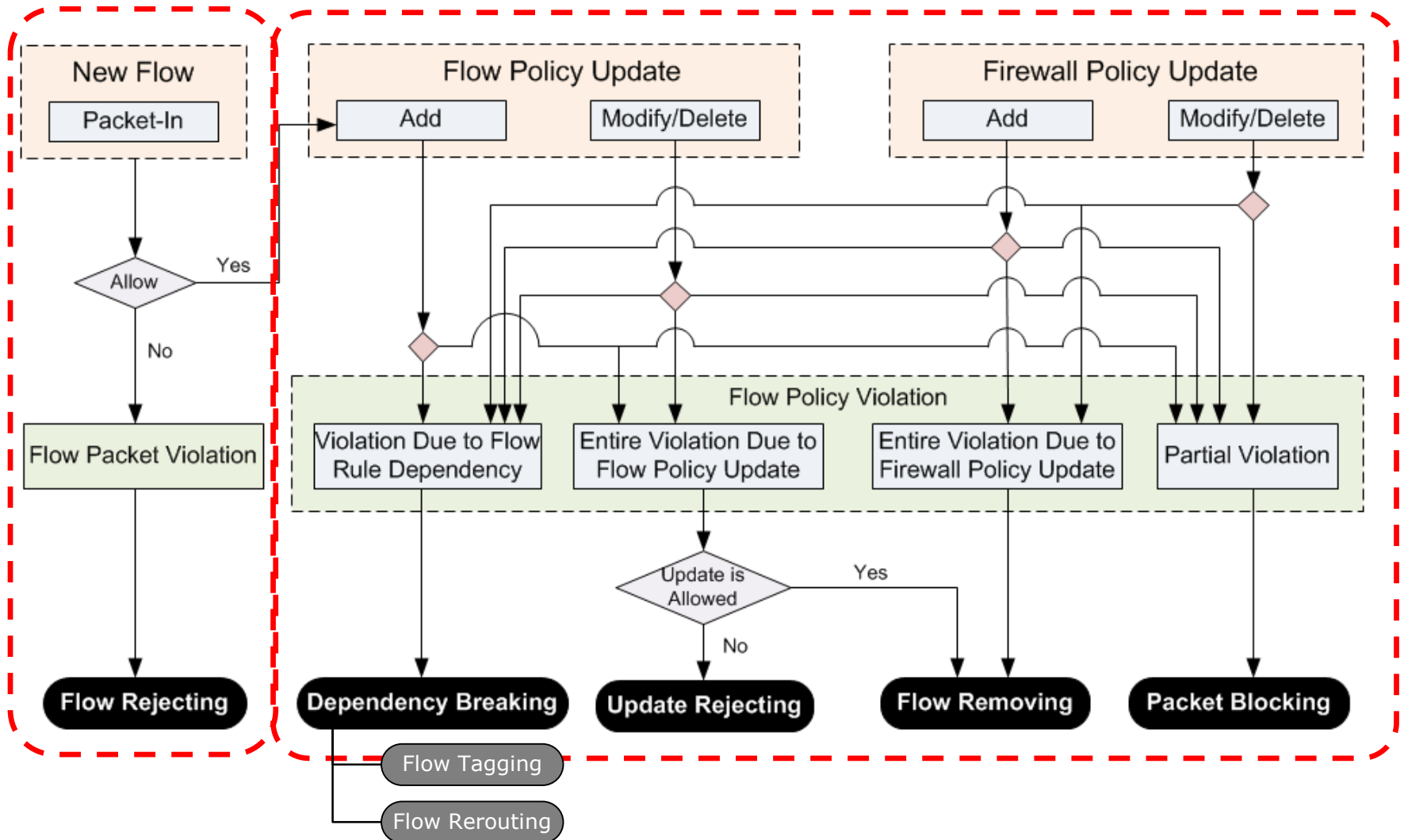
Our Approach

- **FlowGuard**: a comprehensive framework for building robust SDN firewalls



Violation Resolution

■ Automatic Violation Resolution Mechanism



Implementation & Evaluation

■ Prototype of FlowGuard

- Floodlight V 0.90

■ Evaluation Environment

- Real-world network topology
 - Stanford backbone network [kazemian'13]
- Mininet 2.0

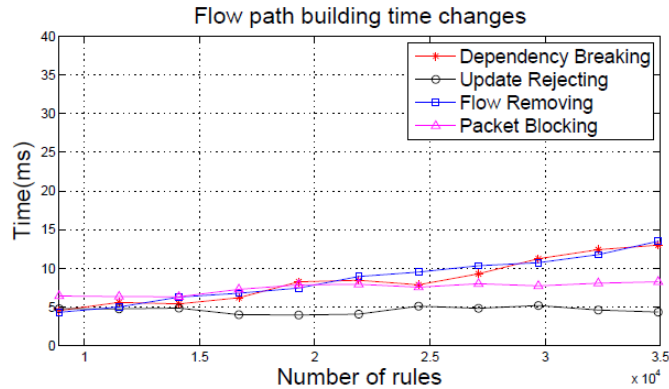
■ Flow Tracking, Violation Detection and Resolution

	Flow Rejecting	Dependency Breaking		Update Rejecting	Flow Removing	Packet Blocking
		Tagging	Rerouting			
Tracking	-	4.54		4.78	4.32	6.42
Detection	0.03	0.04		0.05	0.07	0.06
Resolution	0.03	4.34	1.88	3.73	3.71	2.53

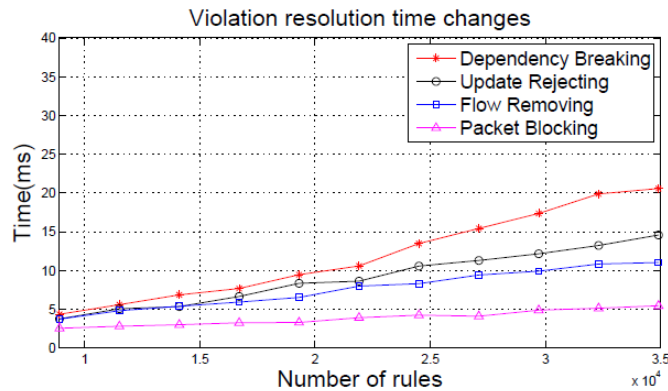
Table 1: Tracking, Detection and resolution time (ms) for different resolution strategies

Evaluation (cont'd)

■ Scalability and Performance Analysis

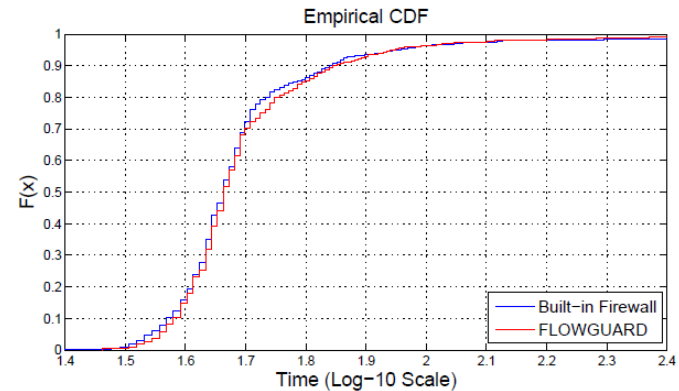


(a) Flow path building time changes.

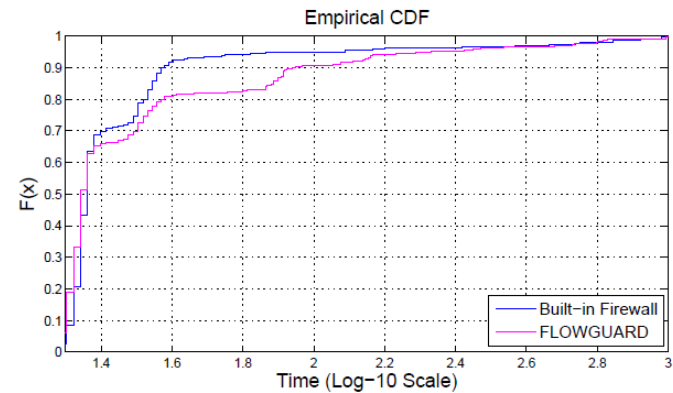


(b) Violation resolution time changes.

Figure 3: Scalability analysis.



(a) Firewall rule update time in microsecond.



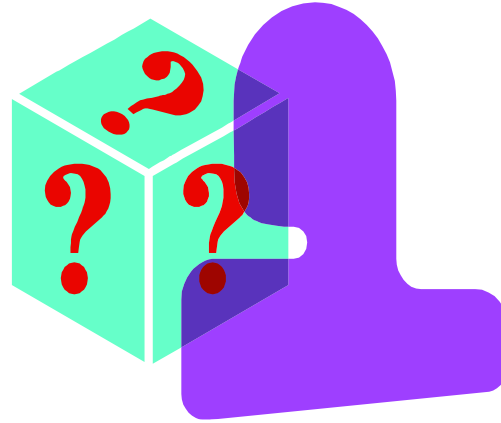
(b) Per packet inspection time in microsecond.

Figure 4: Performance comparison.

Concluding Remarks

- Identifying essential challenges for building robust firewall in SDN
- Proposing a comprehensive framework, ***FlowGuard***, to address identified challenges
- Future Work
 - Developing ***Stateful*** SDN Firewall
 - Firewall ***virtualization*** using Network Function Virtualization (NFV)
 - Robust ***security enforcement kernels*** for SDN controllers

Q & A



**This work was partially supported by the grant
from Department of Energy (DE-SC0004308)**