On the Safety and Efficiency of Virtual Firewall Elasticity Control

Juan Deng†, **Hongda Li**†, Hongxin Hu†, Kuang-Ching Wang†,
Gail-Joon Ahn‡, Ziming Zhao‡ and Wonkyu Han‡

† CLEMSON UNIVERSITY

‡ ASU ARIZONA STATE UNIVERSITY

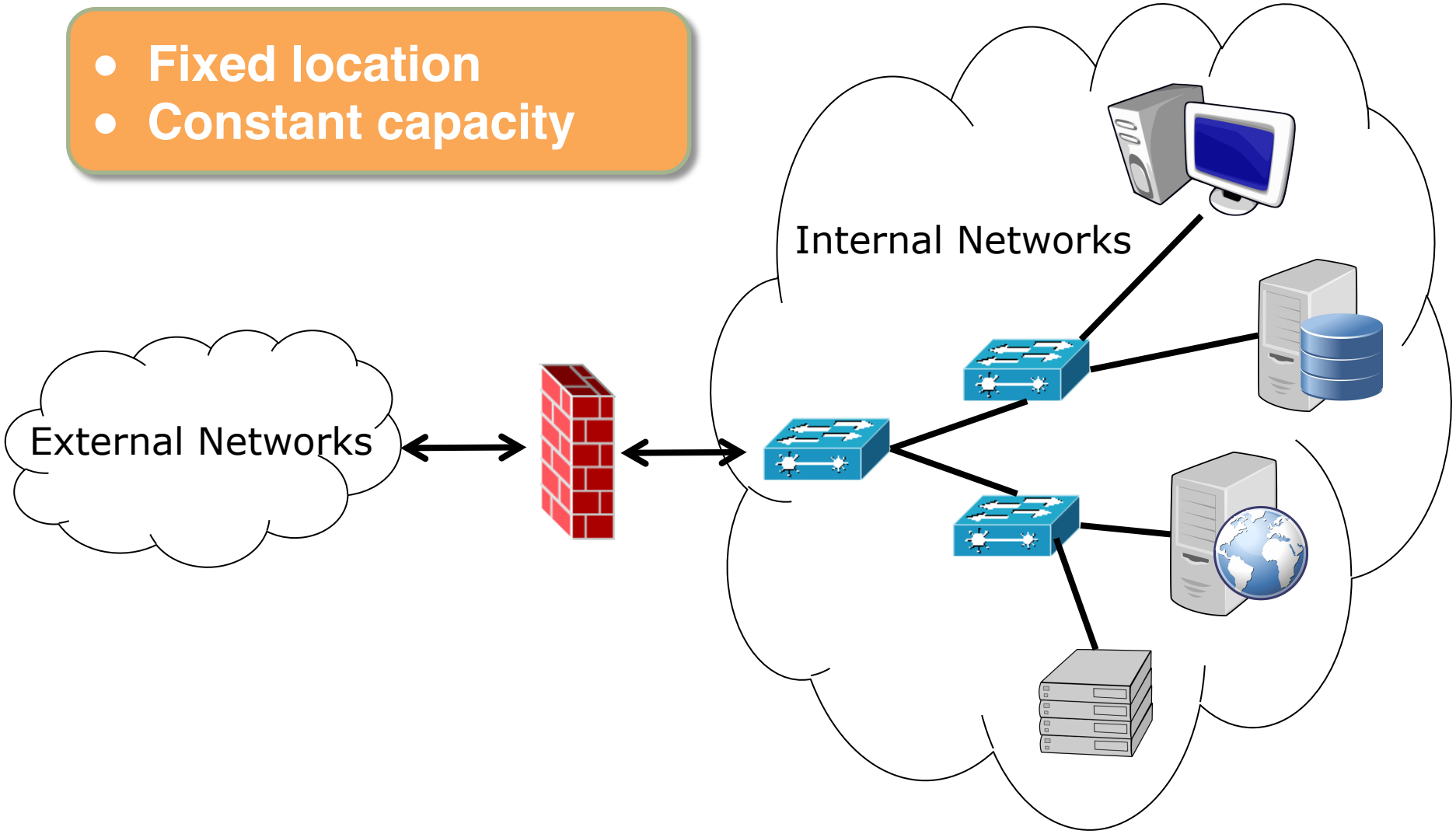
NDSS 2017

Outline

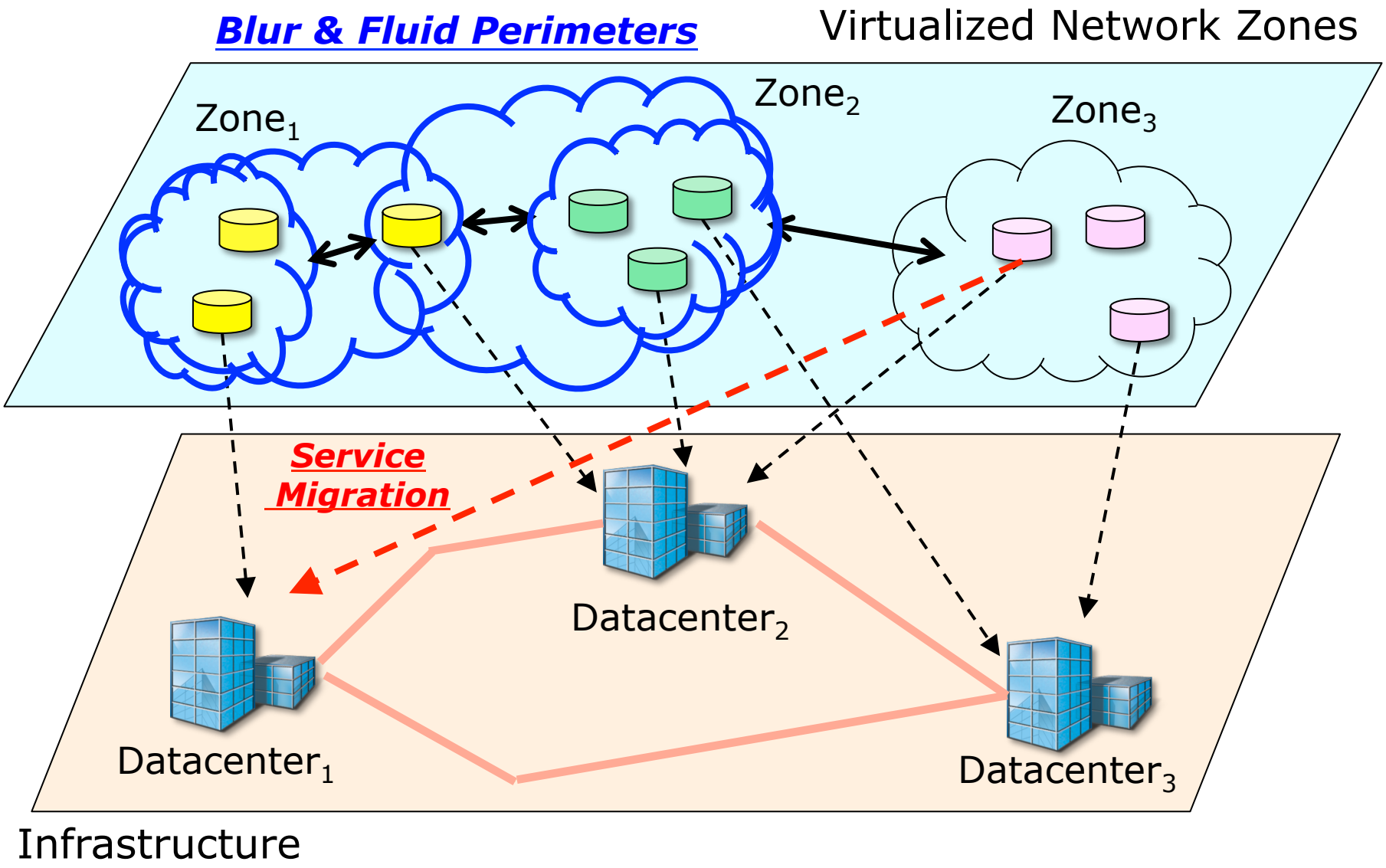
- Introduction
- Overview of VFW Controller
- Our Approach
  - Dependency Analysis and Semantic Consistency
  - Flow Update Analysis
  - Buffer Cost Analysis
  - Optimal Scaling
- Implementation and Evaluation

Traditional Hardware-based Firewall

- Fixed location
- Constant capacity

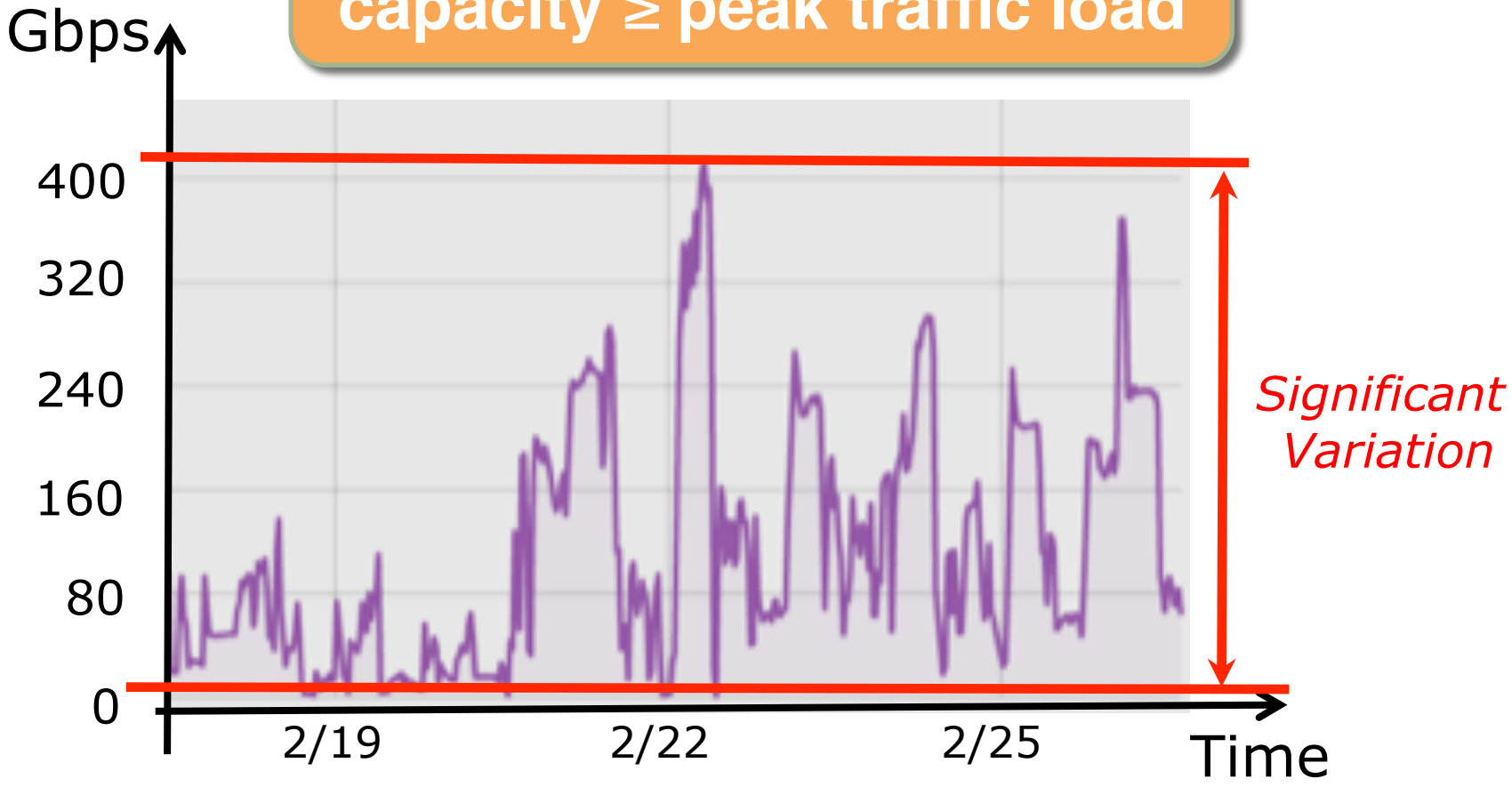


Virtualized Environments



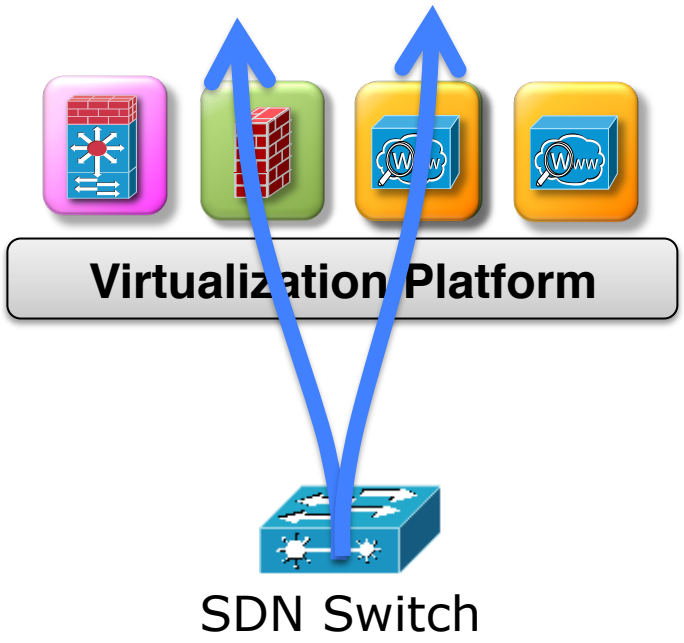
Traffic Volume Variation

Expensive option:
capacity ≥ peak traffic load



Source: https://blog.cloudflare.com/a-winter-of-400gbps-weekend-ddos-attacks/

New Trends



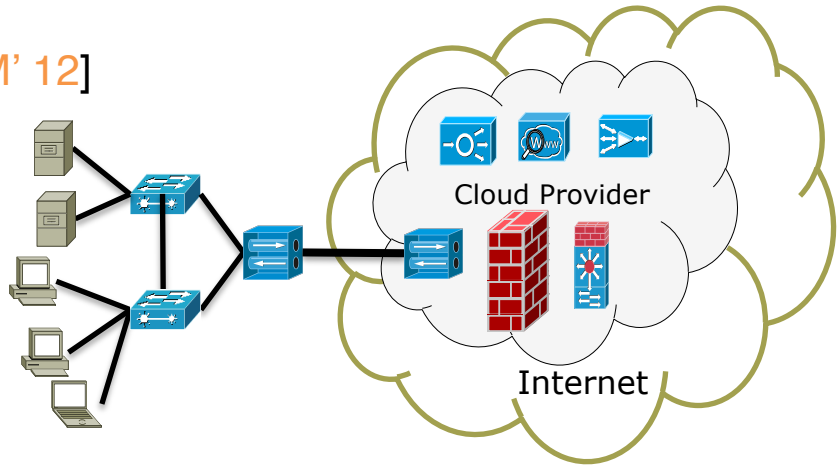
- **N**etwork **F**unction **V**irtualization (NFV)
  - Create and destroy software instances dynamically
- **S**oftware-**D**efine **N**etworking (SDN)
  - Dynamic traffic steering

NFV + SDN → **Virtual Firewall**

Firewall as a Service

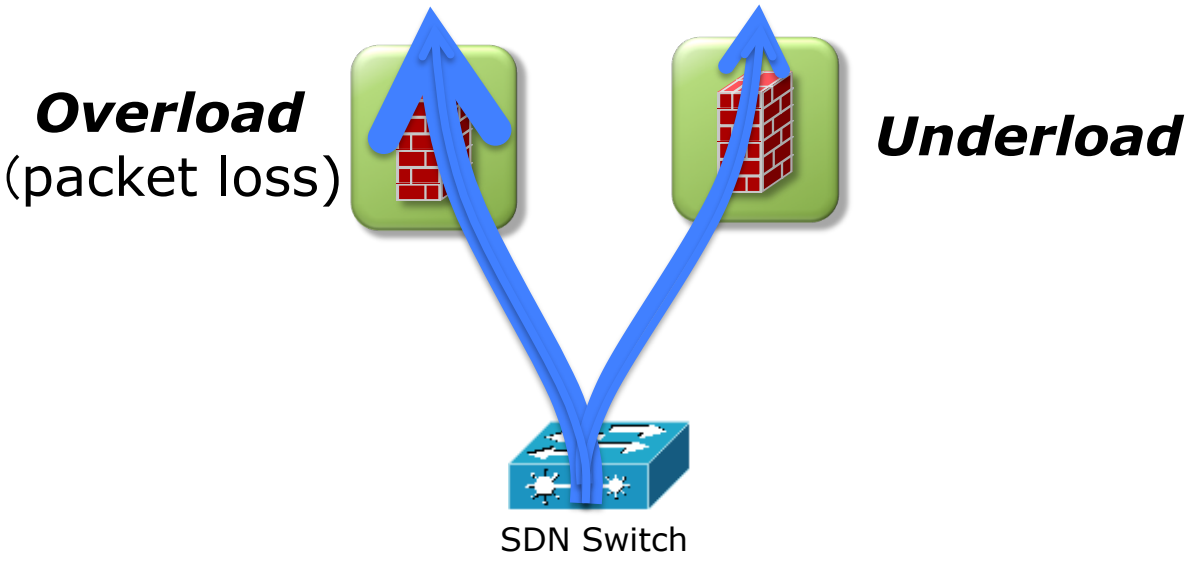
- Virtual firewall in commercial virtualized environments
  - Amazon AWS
  - VMware vCloud
  - VCE Vblock
  - Microsoft Azure
  - Google Cloud Platform

- Virtual firewall used to protect traditional enterprise networks
  - Middlebox Outsourcing [SIGCOMM' 12]



Elastic Virtual Firewall Scaling

- Overload → elastic scaling out
- Underload → elastic scaling in



Safe, Efficient and Optimal

Policy Migration in VFW Scaling

Copy

Seq	Src_ip	Dst_ip	Action
v1	A	B	Deny
v2	C	D	Allow
…	…	…	…

VFW_1

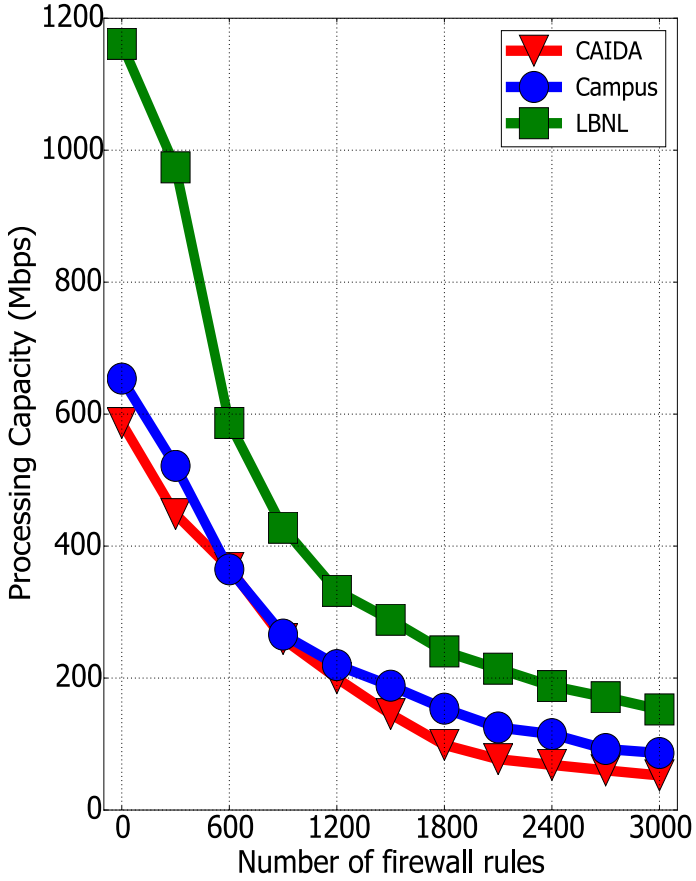
VFW_2

Split

Seq	Src_ip	Dst_ip	Action
v1	**A**	**B**	**Deny**
v2	C	D	Allow
…	…	…	…

VFW_1

VFW_2

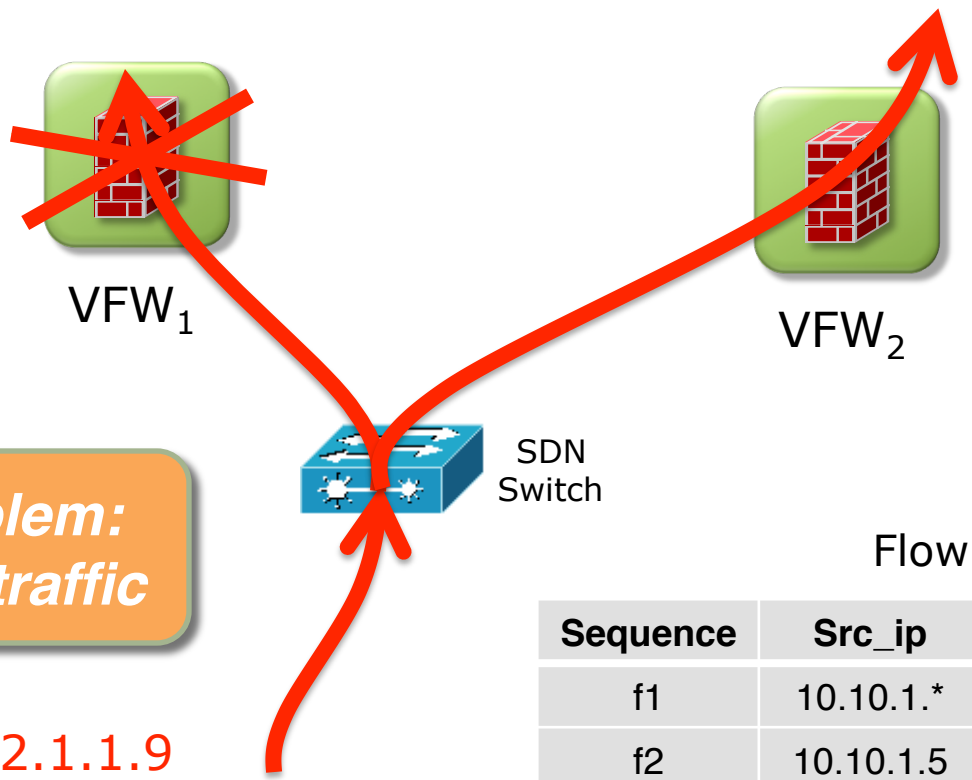


Virtual Firewall
Performance VS. Rule Size

Challenges - Semantic Consistency

Sequence	Src_ip	Dst_ip	Action
v1	10.10.1.5	192.1.1.*	Deny
v2	10.10.1.*	192.1.1.9	Allow
…	…	…	…

Dependent



Safety Problem: Allow illegal traffic

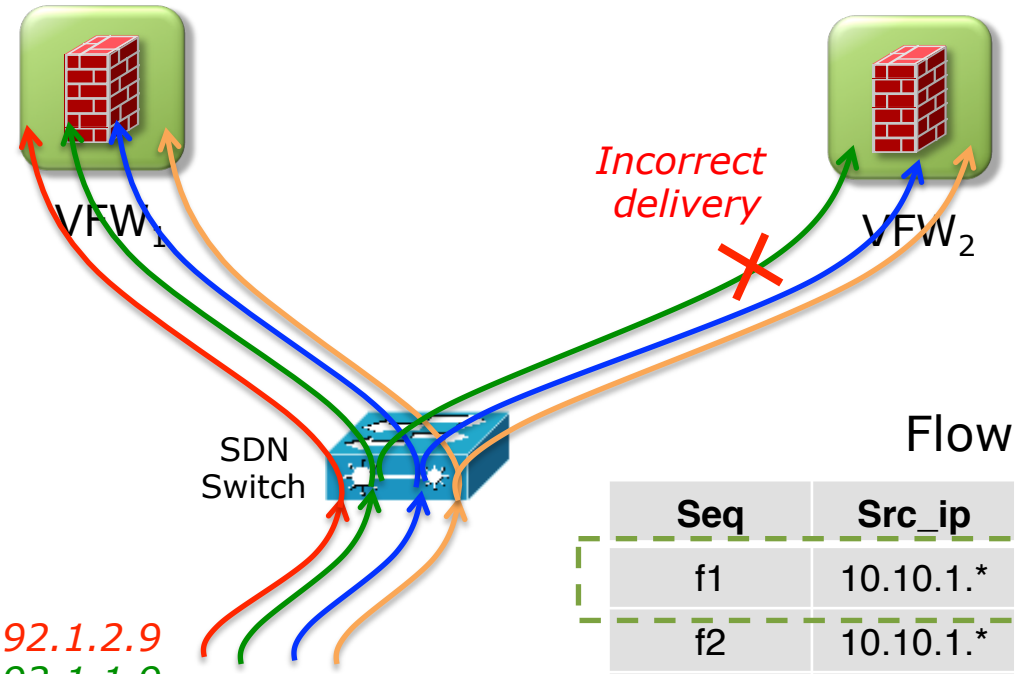
10.10.1.5 → 192.1.1.9

Flow Table

Sequence	Src_ip	Dst_ip	Action
f1	10.10.1.*	192.1.1.9	**To VFW_2**
f2	10.10.1.5	192.1.1.*	To VFW_1
…	…	…	…

Challenges - Correct Flow Update

Sequence	Src_ip	Dst_ip	Action
v1	10.10.*.5	192.1.2.*	Allow
v2	10.10.*.6	192.1.1.*	Deny
v3	10.10.*.7	192.1.1.*	Allow
v4	10.10.*.8	192.1.1.*	Deny
...	...	...	...

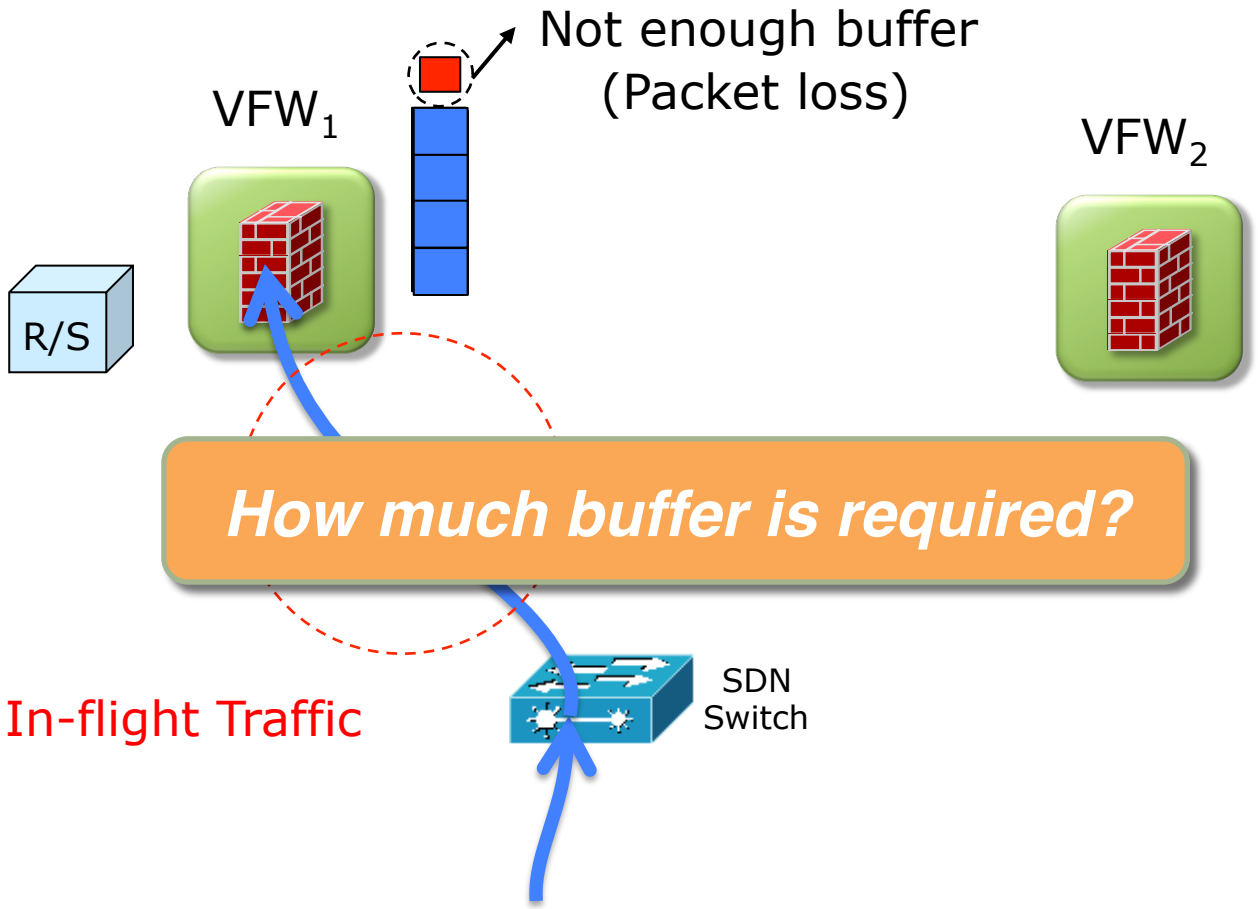


Not exactly matched

Flow Table

Seq	Src_ip	Dst_ip	Action
f1	10.10.1.*	192.1.1.*	To VFW_2
f2	10.10.1.*	192.1.2.*	To VFW_1
...	...	...	...

Challenges - Buffer Overflow Avoidance

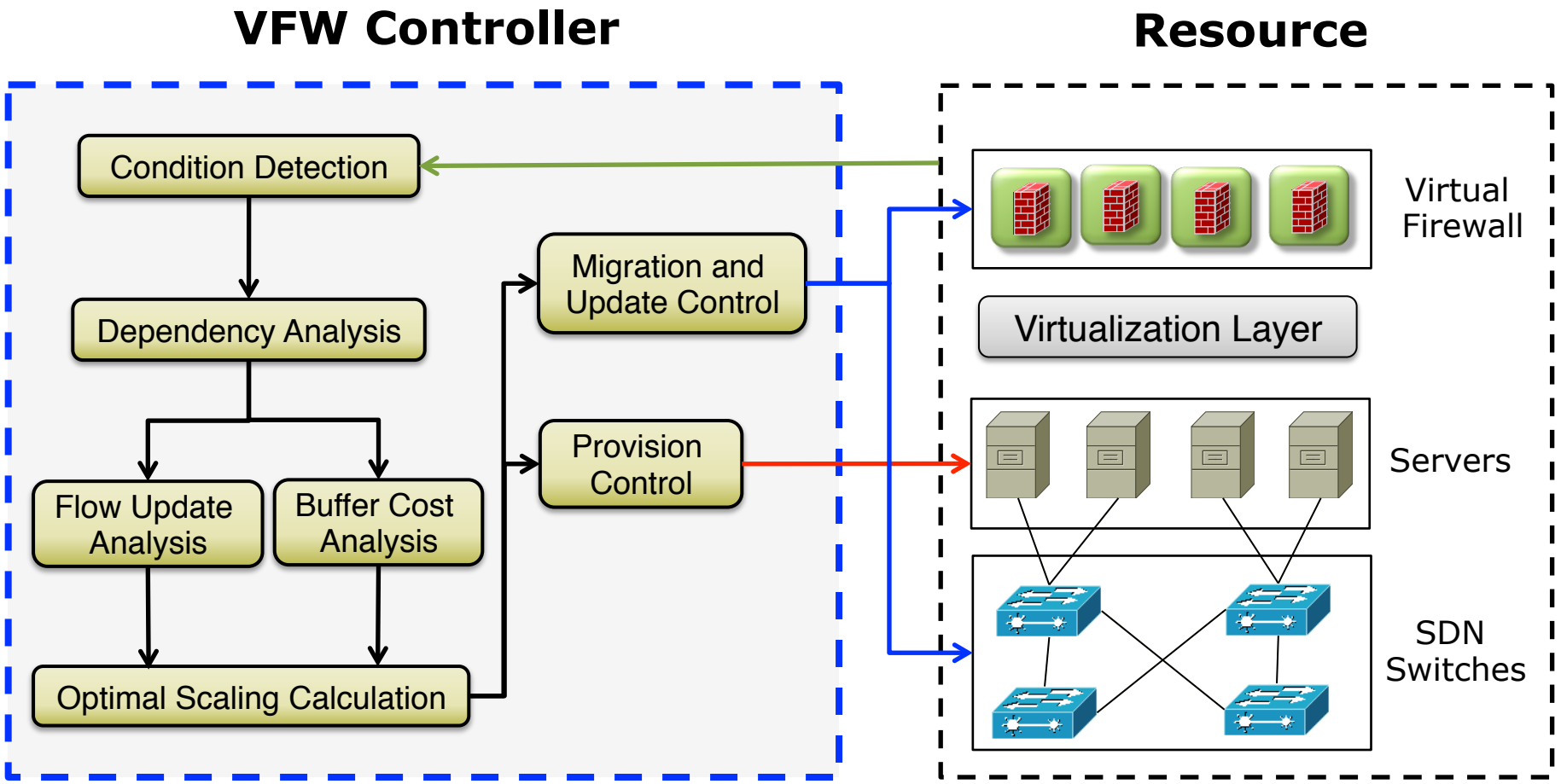


Challenges - Optimal Scaling

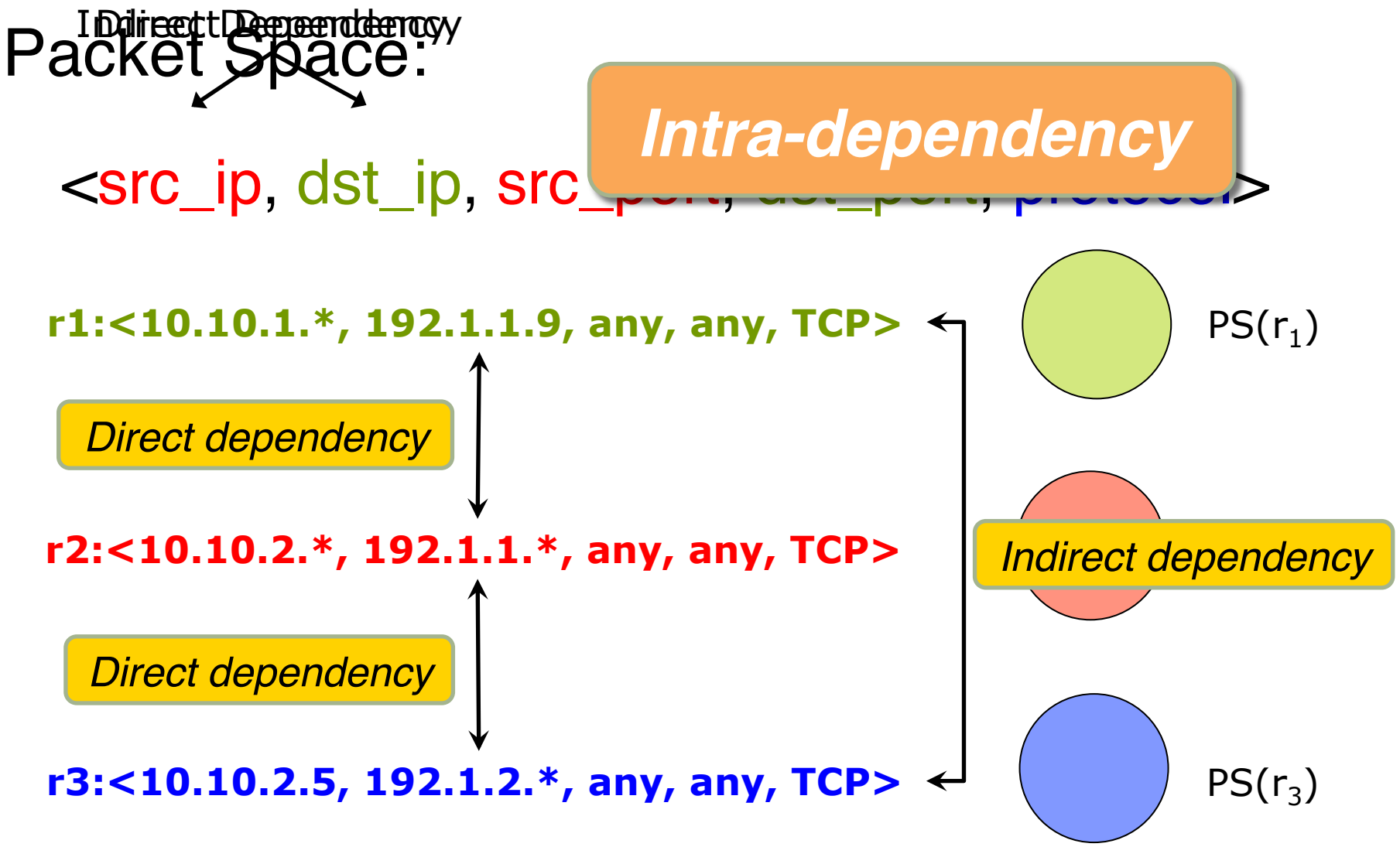
- Goal: minimum resource consumption
  - Scaling-out: least new instances
  - Scaling-in: most killed instances
- Constraints

Satisfy SLAs | *Minimize Update* | *Avoid Buffer Overflow*

Overview of VFW Controller



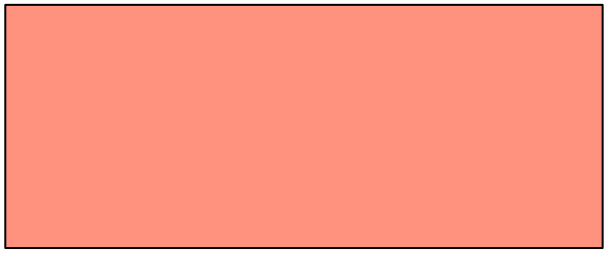
Dependency Analysis



Dependency Analysis

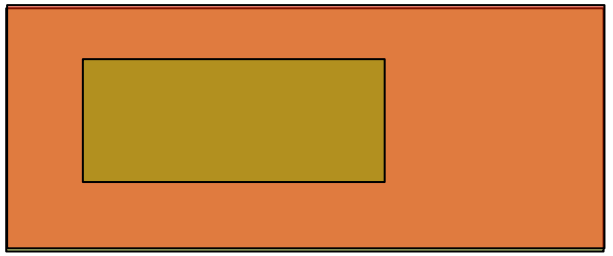
Relation be **Inter-dependency** rules

Firewall Rule Group (V)



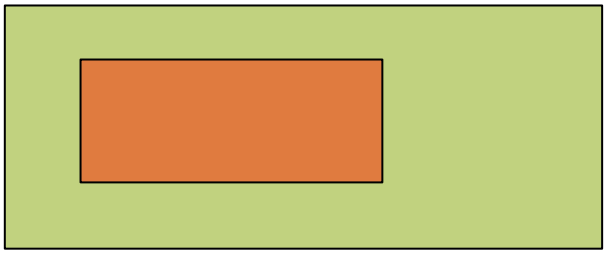
$$PS(V) = PS(F)$$

Flow Rule Space (F)



$$PS(V) \supset PS(F)$$

Subspace



$$PS(V) \subset PS(F)$$

Intersection

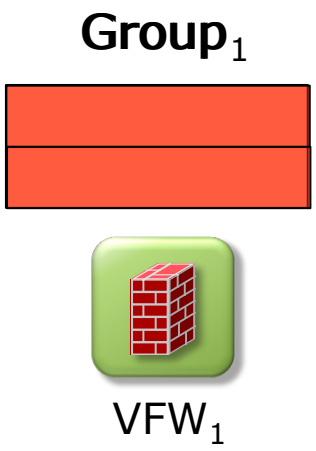
$$PS(V) \cap PS(F) \subset PS(V)$$

$$PS(V) \cap PS(F) \subset PS(F)$$

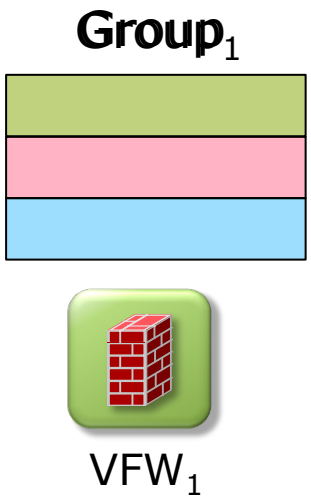
Semantic Consistency

Causes

Group-based Migration



Group is broken



Order is not preserved

Flow Update Analysis

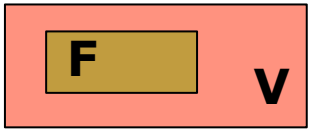
***V**: firewall rule group to be migrated*
F**: flow rule group inter-dependent with **V

Congruence

$PS(V) = PS(F)$

or

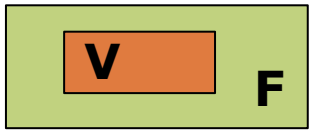
Superspace



$PS(V) \supset PS(F)$

"CHANGE" all $f_i \in F$

Subspace



$PS(V) \subset PS(F)$

or

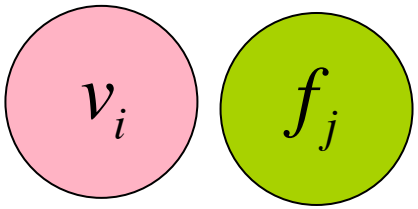
Intersection

$PS(V) \cap PS(F) \subset PS(V)$
$PS(V) \cap PS(F) \subset PS(F)$

"CHANGE" or "INSERT"

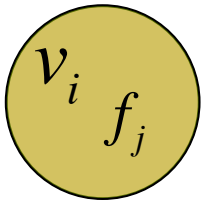
Flow Update Analysis

For each $v_i \in V, f_j \in F$



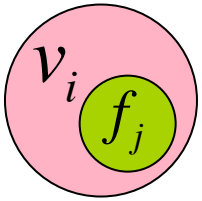
$PS(v_i) \cap PS(f_j) = \phi$

No Update



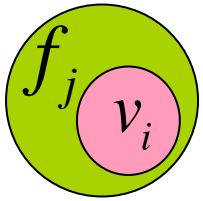
$PS(v_i) = PS(f_j)$

or



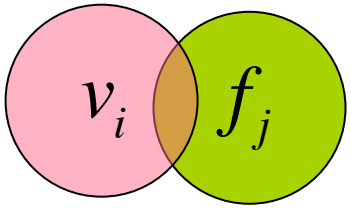
$PS(v_i) \supseteq PS(f_j)$

"CHANGE" f_j



$PS(v_i) \subset PS(f_j)$

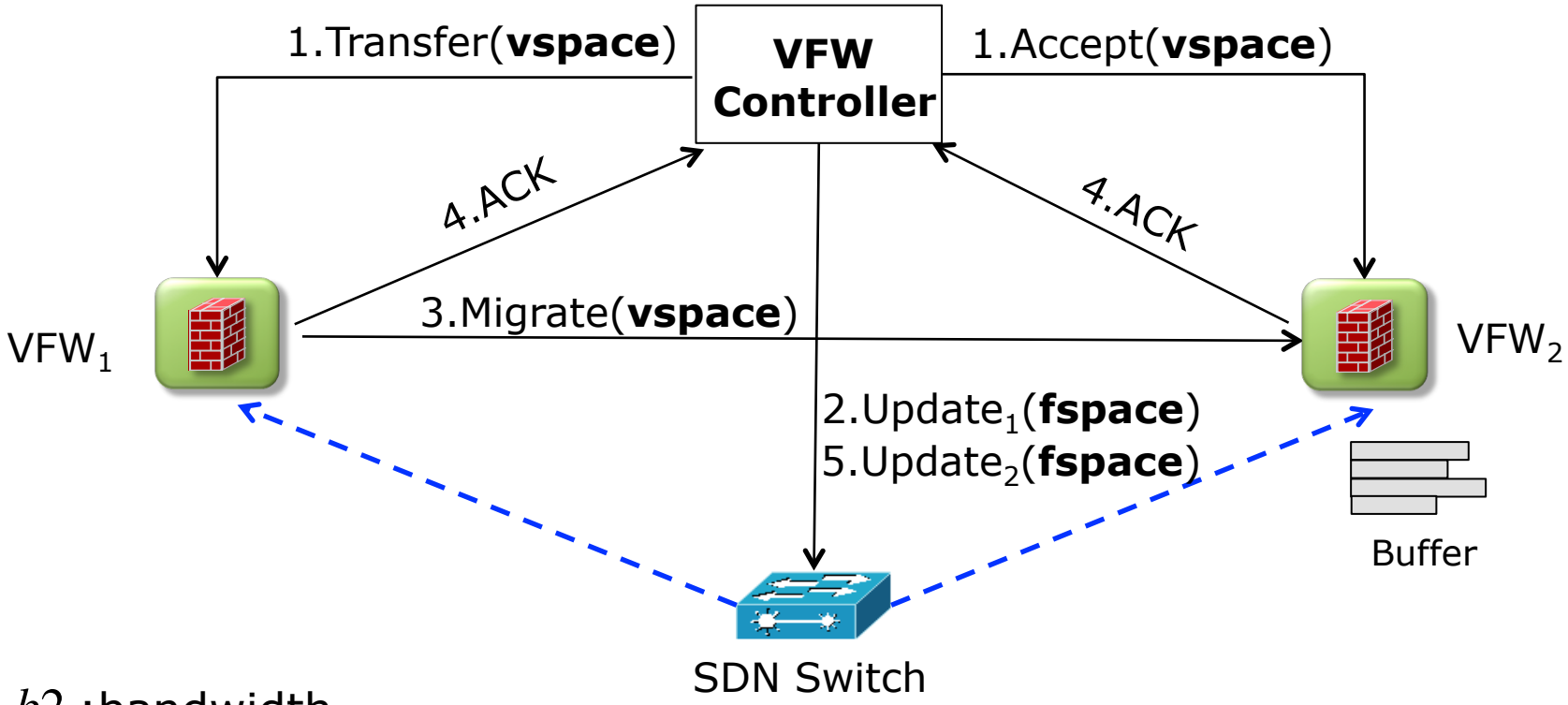
or



$PS(v_i) \cap PS(f_j) \subset PS(v_i)$
$PS(v_i) \cap PS(f_j) \subset PS(f_j)$

"INSERT" f_j' where $PS(f_j') = PS(v_i) \cap PS(f_j)$

Buffer Cost Analysis



$b1, b2$:bandwidth

$d1, d2, d3$:transmission delay

λ : sending rate of the affected flows

$$\beta = (\sum \lambda) \times \{d1 + d3 - d2 + b1 + b2\}$$

Optimal Scaling Calculation

$X = \{x_{11}, \ldots, x_{mn}\}$ $x_{ij} \in \{0,1\}$ *are indicators*

- Goals

Scaling-out

firewall rule group V_i *is moved to instance* j → $x_{ij} = 1$

$$\min \sum_{i=1}^{m} \sum_{j=1}^{n} x_{ij} \gamma_i$$

Minimize extra instances

Sca

inst

Solved by Integer Linear Programming

$$\max \sum_{j=1} \sum_{i=1} x_{ij}$$

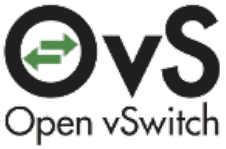
Maximize merged instances

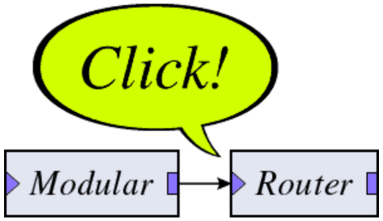
- Constraints

Satisfy SLAs | *Minimize Update* | *Avoid Buffer Overflow*

Implementation

- Implementation
  - Xen-4.4.1, ClickOS [NSDI'14]
  - Floodlight, Open vSwitch
  - Simple stateful firewall: 7 new Click elements, ~3000 lines of C++.
  - VFW Controller: python interface, based on Hassel Library [NSDI'12]





- Testbed
  - CloudLab (https://www.cloudlab.us/)
  - Experiment profile is available:

    https://www.cloudlab.us/p/SeNFV/Firewall-VLANs

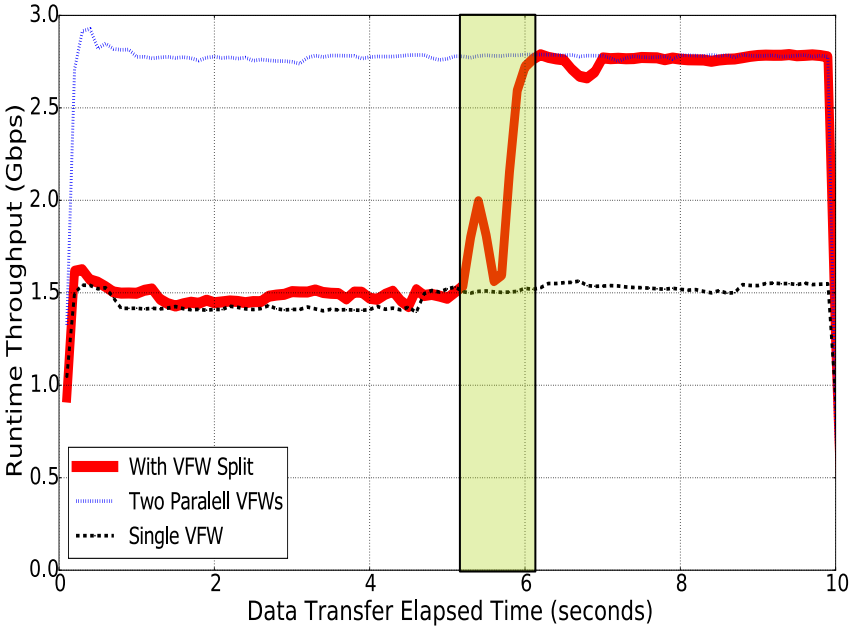
Evaluation

- Intra-dependency in real-world firewall policies

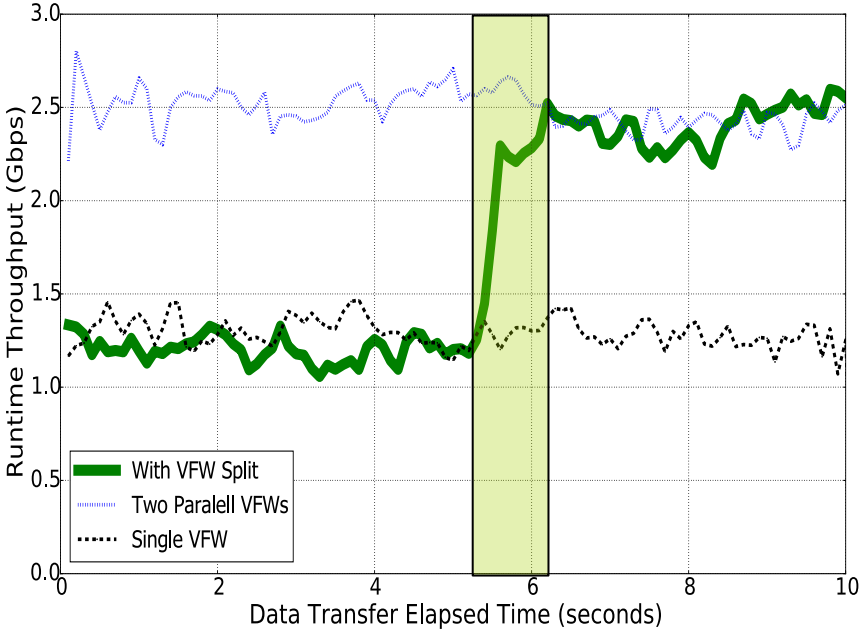
Policy	Rule(#)	Group(#)	Largest Group Member (#)
A	12	2	3
B	18	3	5
C	25	3	6
D	52	7	7
E	83	9	7
F	132	10	9
G	354	10	12
H	926	13	18

Evaluation

- Capability to quickly scale



Split with UDP flow overload



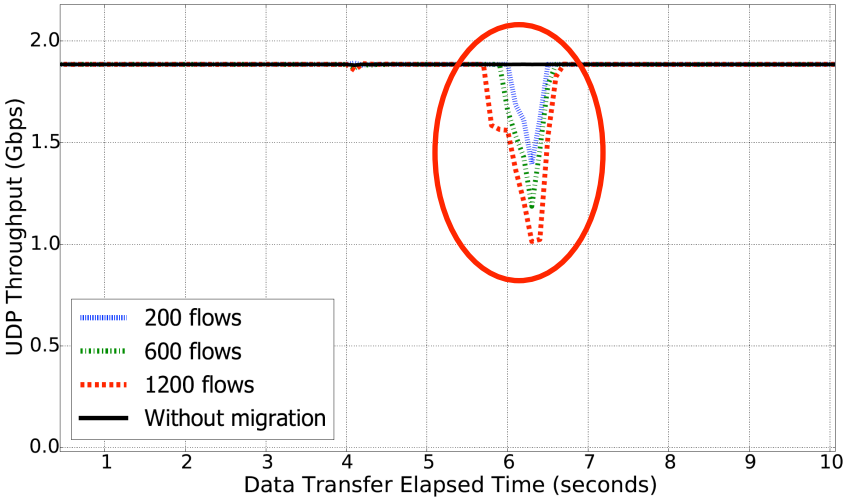
Split with TCP flow overload

< 1 second

Evaluation

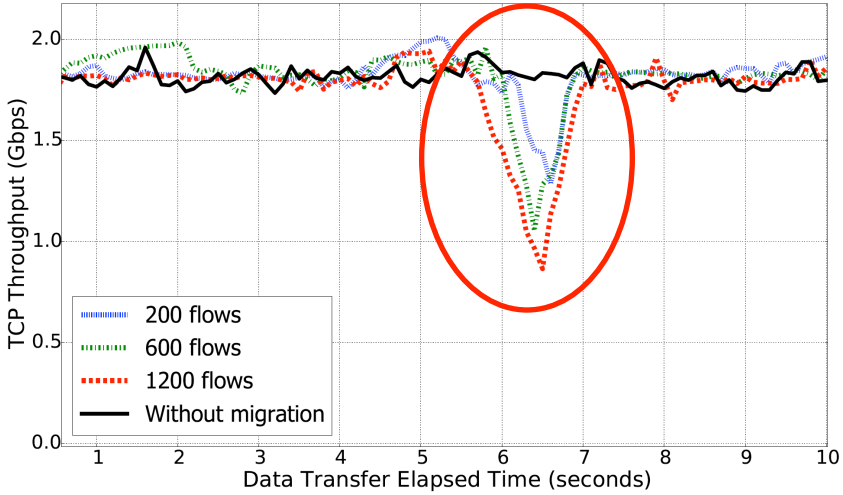
- Migration impact on throughput

Throughput Degradation



Impact on UDP throughput

Throughput Degradation

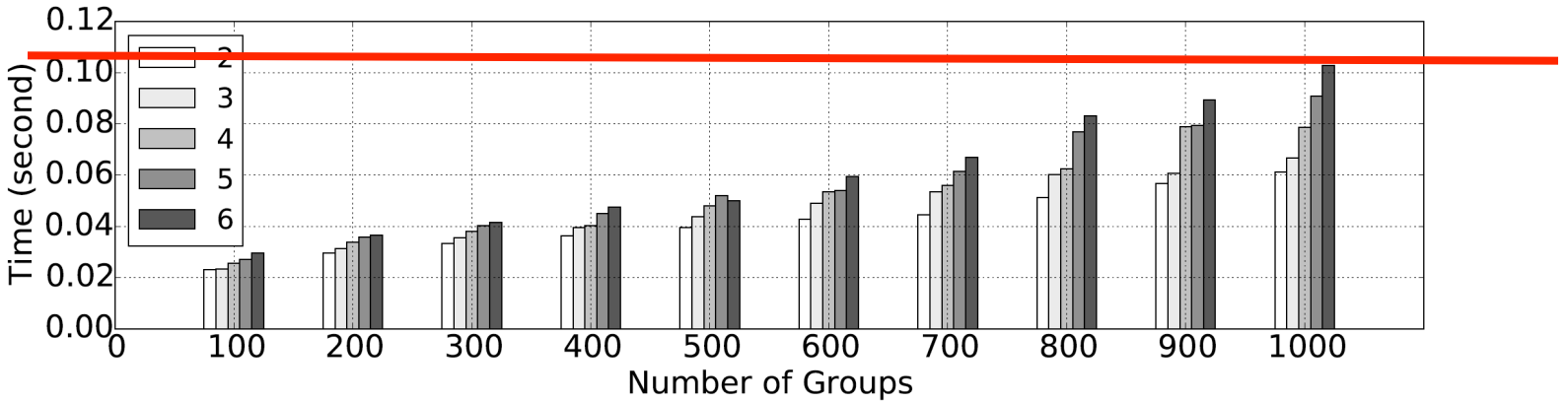


Impact on TCP throughput

Evaluation

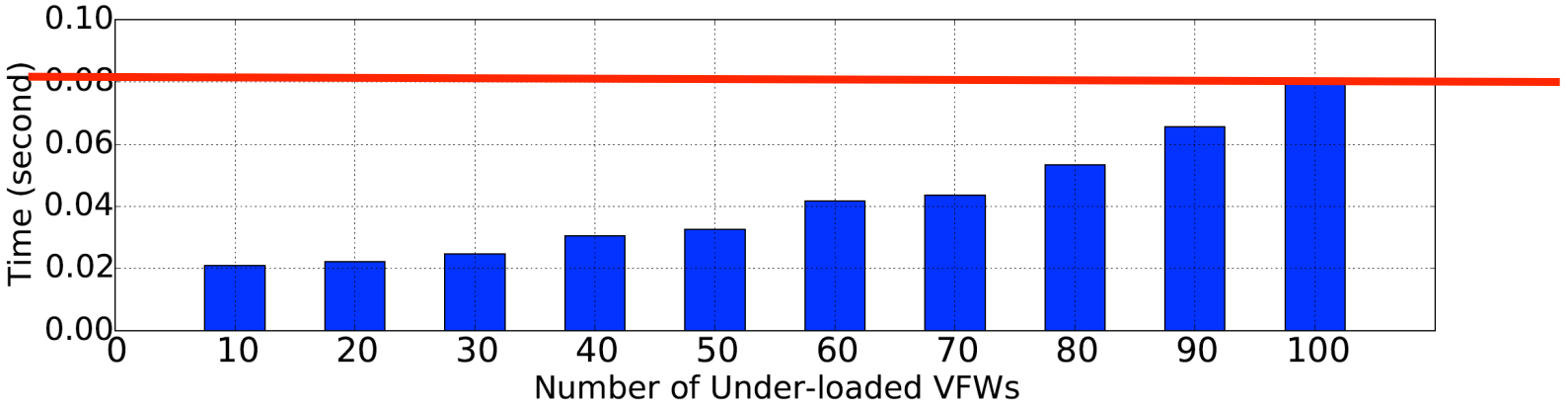
- Performance of optimal scaling calculation

6 addition virtual firewall instances,
1000 firewall rule groups to split



Scaling-out calculation

100 underloaded virtual firewall instances



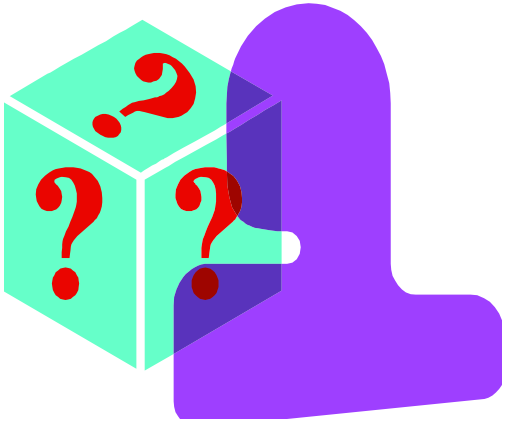
Scaling-in calculation

Conclusion

- NFV+SDN push forward a new breed of firewalls, ***virtual firewalls***

- **VFW Controller** enables ***safe***, ***efficient*** and ***optimal*** virtual firewall scaling
- Implementing and evaluating VFW Controller

Q & A



This work was partially supported by grants from National Science Foundation (NSF-ACI-1642143 and NSF-ACI-1642031)

State Of The Art

- Safe Migration
  - Split/Merge [NSDI'13]
  - OpenNF [SIGCOMM'14]
- NFV and SDN for security
  - Bohatei [USENIX Security'15]
- SDN Firewall
  - FlowGuard [HotSDN'14]
- Firewall policy deployment [S&P'07]
- Distributed firewall [CCS'00]

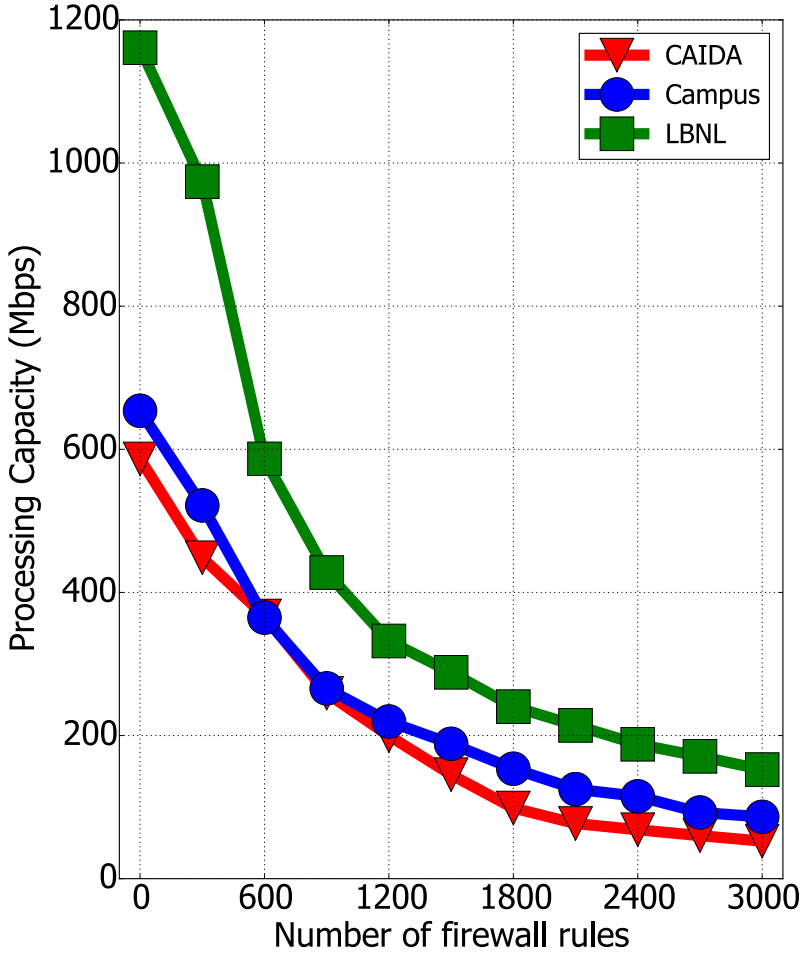
Study of Real-world Firewall Policies

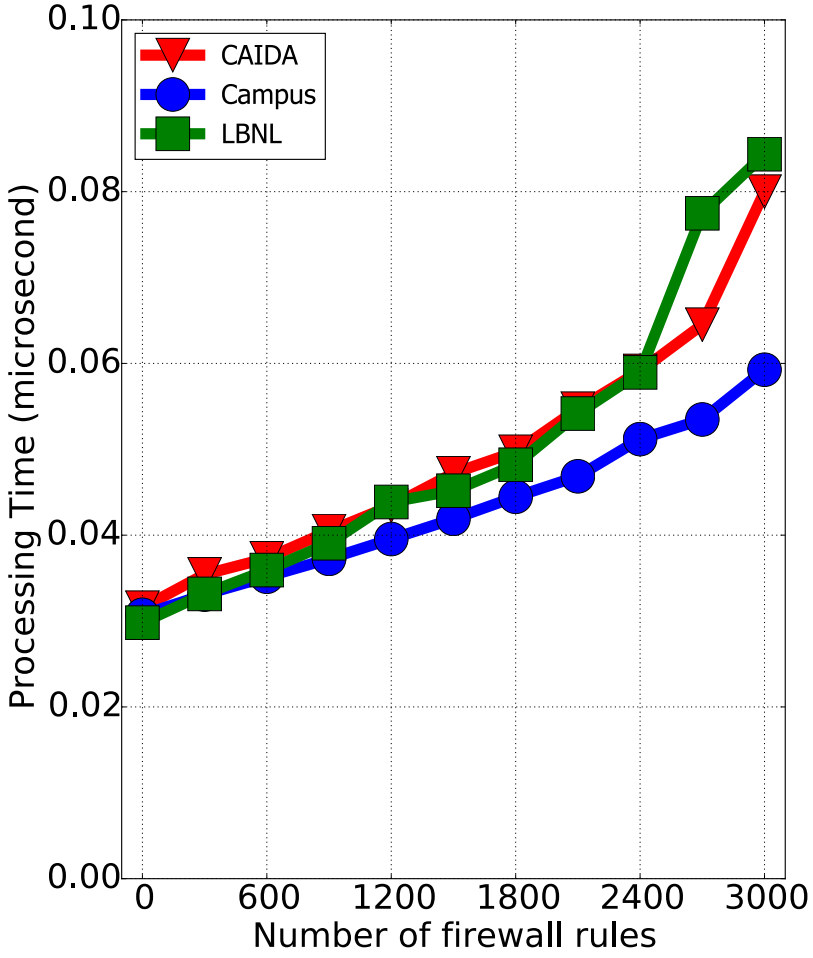
Policy	Rule(#)	Group(#)
A	12	2
B	18	3
C	25	3
D	52	7
E	83	9
F	132	10
G	354	10
H	926	13

Rule Dependencies in Real-world Firewall Polices

Evaluation

- Rule size impact on performance

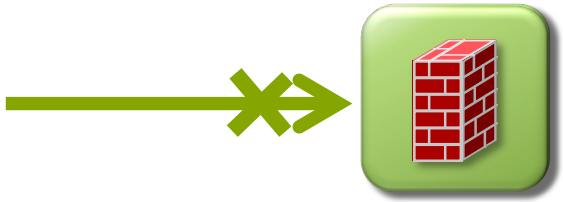




Challenges (Semantic Consistency)

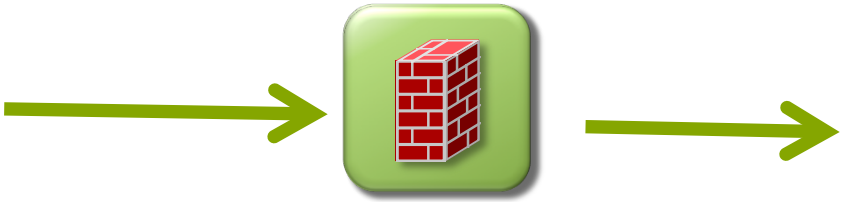
Sequence	Src_ip	Dst_ip	Action
v1	**10.10.1.5**	**192.1.1.***	**Deny**
v2	10.10.1.*	192.1.1.9	Deny
v3	10.10.1.*	192.1.1.*	Allow
...	...	...	...

Sequence	Src_ip	Dst_ip	Action
v2	10.10.1.*	192.1.1.9	Deny
v3	**10.10.1.***	**192.1.1.***	**Allow**
...	...	...	...



Original VFW

10.10.1.5 → 192.1.1.1



Merged VFW

10.10.1.5 → 192.1.1.1

~~Semantic Consistency~~