On the Safety and Efficiency of Virtual Firewall Elasticity Control

Hongda Li¹, Juan Deng¹, Hongxin Hu¹, Kuang-Ching Wang¹
Gail-Joon Ahn², Ziming Zhao² and Wonkyu Han²
¹Clemson University and ²Arizona State University

Motivation

- Traditional Hardware-based Firewall
  - Fixed location & constant capacity
- New Requirements
  - Virtualized environments
  - Services need migration often
  - Significant traffic volume variation
- New Trends
  - NFV: create and destroy software instances dynamically
  - SDN: dynamic traffic steering

NFV + SDN ➔ Virtual Firewall

Virtual Firewall Elastic Scaling
- Overload ➔ elastic scaling out
- Underload ➔ elastic scaling in

Challenges to achieve safe, efficient and virtual firewall scaling
- Split or copy firewall policies?
- Semantic consistency & correct flow update
- Buffer overflow avoidance
  - Prior work assumes unlimited buffer size
- Optimal scaling

Our Approach

Core Components of VFW Controller
- Dependency Analysis
- Flow Update Analysis
- Buffer Cost Analysis
- Optimal Scaling Calculation

- Group-based firewall rule migration to ensure semantic consistency

Flow Update Analysis
- Update operation
  - CHANGE existing flow rules' actions
  - INSERT a new flow rule in front of an existing flow rule
  - V: firewall rule group to be migrated
  - F: flow rule group inter-dependent with V

Buffer Cost Analysis
- Update cost
  - Number of new flow rules inserted

Optimal Scaling Calculation
- Scaling-out: least new instances
  - three-step heuristic
  - Scaling-in: most merged instances
  - integer linear programming

Implementation

- We implemented VFW Controller in real NFV/SDN platforms
- Xen-4.4.1. ClickOS
- Floodlight, Open vSwitch
- Simple stateful firewall: new Click elements
- VFW Controller: Hassel Library
- Testbed: CloudLab (https://www.cloudlab.us)
- Source code available:
  - https://www.cloudlab.us/p/SafEFV/Firewall-VLANs

Evaluation

- Evaluation of group size based on real-world firewall policies
- Largest firewall group contains 18 rules
- Capability to quickly scale
- Scale in less than 1 sec for 400 firewall rules

- Migration impact on throughput
  - TCP connection preserved

- Performance of optimal scaling calculation
  - 6 new instances, 1000 firewall rule groups in 110ms
  - 100 underloaded virtual firewall instances in 80ms

- Optimal scaling calculation for scaling-out

Publication