FlowGuard: Building Robust Firewalls for Software-Defined Networks

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

![Diagram of network with Host A, Host B, Host C, Host D, Switch 1, Switch 2, SDN Controller, and Firewall app.]

Table 1

<table>
<thead>
<tr>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>A → D: Rewrite A with B, Forward</td>
</tr>
<tr>
<td>Rule 1.2</td>
</tr>
<tr>
<td>Rule 1.N</td>
</tr>
</tbody>
</table>

Table 2

<table>
<thead>
<tr>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>B → D: Rewrite D with C, Forward</td>
</tr>
<tr>
<td>Rule 2.1</td>
</tr>
<tr>
<td>Rule 2.N</td>
</tr>
</tbody>
</table>
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**
  - 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

![Diagram showing FlowGuard components]

Network State/Configuration Updates:
- New Flow
- Flow Policy Update
- Firewall Policy Update

Flow Policy Violation Detection
- Flow Packet Space Analysis
  - Flow Tracking
  - Flow Path Space Calculation
- Firewall Authorization Space Analysis
  - Authorization Space Partition

Flow Policy Violation Resolution
- Flow Rejecting
- Flow Policy Violation Resolution
  - Dependency Breaking
  - Update Rejecting
  - Flow Removing
  - Packet Blocking

Toolkits:
- Visualization
- Optimization
- Integration
- Migration
- Deployment
- Language
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

![Diagram showing the workflow of FlowGuard]
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

![Diagram]

- Firewall Denied Authorization Space
- Tracked Flow Path Space
- Violated Space
Our Approach

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

![Diagram](image)

**FlowGuard** components:
- **Flow Packet Violation Detection**
  - New Flow
  - Flow Policy Update
  - Firewall Policy Update

**Toolkits**:
- Visualization
- Optimization
- Integration
- Migration
- Deployment
- Language
Violation Resolution

Automatic Violation Resolution Mechanism

- New Flow
  - Packet-In
    - Allow
      - Yes
        - Flow Packet Violation
          - Flow Rejecting
        - No
          - Flow Packet Violation
            - Flow Rejecting
  - No

- Flow Policy Update
  - Add
    - Modify/Delete
      - Flow Policy Violation
        - Violation Due to Flow Rule Dependency
          - Dependency Breaking
            - Update Rejecting
              - Flow Tagging
              - Flow Rerouting
          - Entire Violation Due to Flow Policy Update
            - Update Rejecting
              - Flow Removing
                - Packet Blocking
          - Entire Violation Due to Firewall Policy Update
            - No
              - Update is Allowed
                - Yes

- Firewall Policy Update
  - Add
    - Modify/Delete
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

<table>
<thead>
<tr>
<th></th>
<th>Flow Rejecting</th>
<th>Dependency Breaking</th>
<th>Update Rejecting</th>
<th>Flow Removing</th>
<th>Packet Blocking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking</td>
<td>-</td>
<td>4.54</td>
<td>4.78</td>
<td>4.32</td>
<td>6.42</td>
</tr>
<tr>
<td>Detection</td>
<td>0.03</td>
<td>0.04</td>
<td>0.05</td>
<td>0.07</td>
<td>0.06</td>
</tr>
<tr>
<td>Resolution</td>
<td>0.03</td>
<td>4.34</td>
<td>1.88</td>
<td>3.71</td>
<td>2.53</td>
</tr>
</tbody>
</table>

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