# Application Layer Security using SDN Firewall

**Chao-li Tarng**

Department of Electrical Engineering, San Jose State University, San Jose, California 95192



## Introduction

One essential objective of SDN is to empower a system controller to run different system benefits and deal with the whole system straightforwardly by arranging bundle taking care of instruments in hidden gadgets [1].

firewalls and interruption identification and avoidance frameworks (IDS/IPS) to be relocated to SDN-based systems by re-outlining and executing these frameworks as good security applications or administrations. Firewalls are the most broadly sent security system in many organizations and foundations.

Our study uncovers that SDN presents colossal chances to systems administration, as well as brings awesome difficulties for building SDN firewalls as takes after:

- **Examining Dynamic Network Policy Updates**
- **Checking Indirect Security Violations**
- **Architecture Option**
- **Stateful Monitoring**

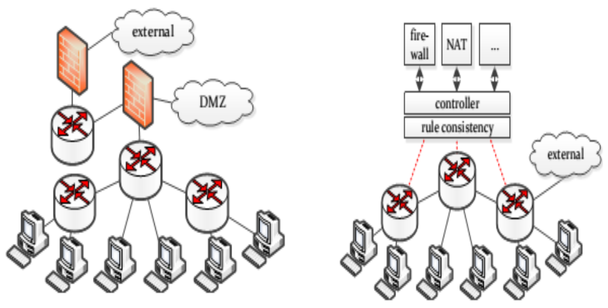


**Fig1. Conventional vs. SDN architecture**

## Research Objective

Policy rules must not be overlaid, decayed, shadowed and conflict.

- Defining a firewall that spanned to application, control and data layers of SDN.
- A policy manager will be defined that splits policy rules and evaluates the rule conflicts in the hierarchy of network layers.
- Network transactions will be evaluated by the firewall in the order of network layer hierarchy. This helps to avoid the conflicts raised between rules. Also helps to minimize the number of rules during network transaction valuation, but number of valuations will increase, which is inevitable.
- Policy manager handles the intra, inter layer dependency.

A simulation model of the SDN will be devised by using SDNsim API. Further a SDN packet generator will be devised that is compatible to SDNsim. The cross layered firewall and policy manager will be implemented and tested on simulation model of the SDN.

## Design Approach

***Key Points***

- *SDN System Architecture.*
- *Architecture of Policy Rule Analyzer*
- *SDN Firewall Log Analysis Layered Approach*
- *Layered Approach.*

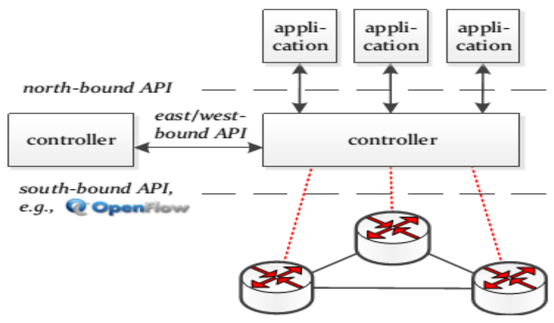


***Fig2. Conceptual Architecture of SDN.***

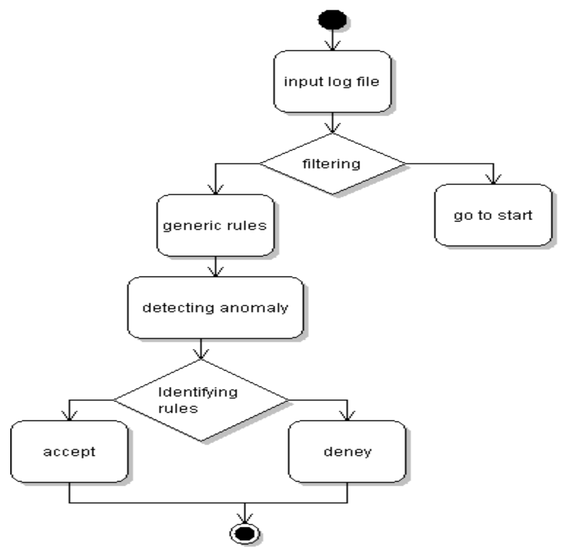


***Fig3. Architecture of Policy Rule Analyzer.***

In Rule Analysis prepare, the technique contains next three modules: log preprocess, log investigation, likewise lead speculation.

## Results


***Fig3. Main screen of the Application***

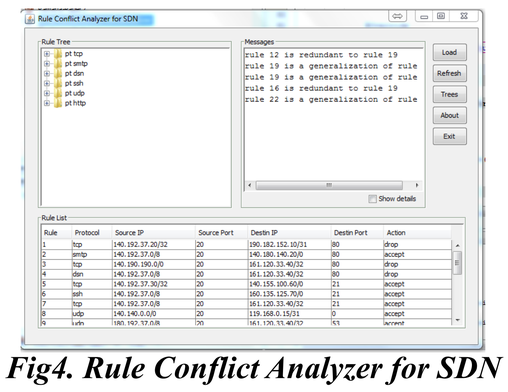


***Fig4. Rule Conflict Analyzer for SDN***

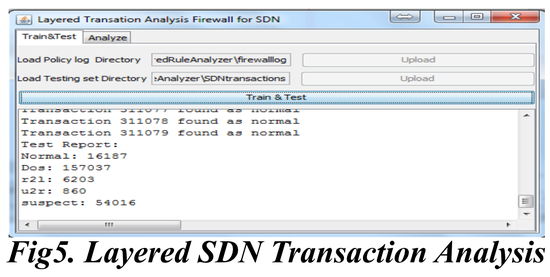


***Fig5. Layered SDN Transaction Analysis***

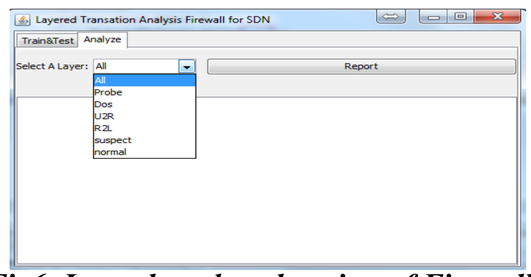


***Fig6. Layer based exploration of Firewall***

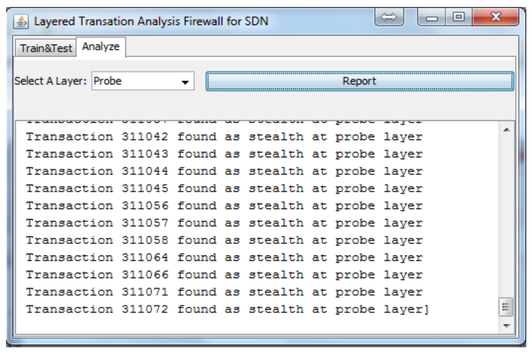


***Fig7. Firewall activity at different layers***

## Conclusions

This thesis is aimed to redefine the activity of SDN firewall to minimize the transaction evaluation complexity and ambiguity in policy rules. In regard to this here we proposed an architecture that performs in two levels. Out of these two levels one is offline model and other works on online mode of the SDN. Through the empirical outcomes of the Rule Analyzer, the projected log analysis technique can effectively enhance the execution efficiency for working with dynamic log data.

The experiments evident that the model devised to analyze SDN transactions is scalable and robust, which is due to its core strategy of SDN layer level analysis of the transaction against policy rules. This work would motivate further research such that auto policy framing under the knowledge obtained from the current activities of the SDN transaction evaluation.

## Key References

- N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. Openflow: enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review, 2008.
- S. Ioannidis, A. D. Keromytis, S. M. Bellovin, and J. M. Smith. Implementing a distributed firewall. In CCS'00
- E. E. Schultz. A framework for understanding and predicting insider attacks. Computers & Security, 21(6):526–531, 2002.
- S. A. Mehdi, J. Khalid, and S. A. Khayam. Revisiting traffic anomaly detection using software defined networking. In RAID'11

## Acknowledgments

We thank Prof Chao-li Tarn for providing invaluable expertise, guidance and support.

## For further information

Please contact *Krishna Mohan Lankala and Kartik Moolani* for code and other setup files.