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].

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

Design Approach

Key Points

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

Results

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 thesis, 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

- 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.