FIREWALL FRAMEWORK FOR MULTI-CLOUD

Kuruppu Arachchilage Ishanka Gayan

209326E

Master of Science in Computer Science

Department of Computer Science and Engineering

University of Moratuwa
Sri Lanka

June 2024

FIREWALL FRAMEWORK FOR MULTI-CLOUD

Kuruppu Arachchilage Ishanka Gayan

209326E

Thesis submitted in partial fulfilment of the requirements for the degree

Master of Science in Computer Science

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

June 2024

DECLARATION OF THE CANDIDATE & SUPERVISOR

I state that this is my own work and this dissertation does not include without acknowledgement anything that was previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and opinion it does not include any material previously published or written by another individual with the exception where the acknowledgement is made in the text.

Also, I hereby give the University of Moratuwa the non-exclusive right to reproduce and disseminate my thesis/dissertation, in whole or in part in print, electronic or, another form. I maintain the right to use this information in whole or part in future works (such as articles or books).

Signature: Date: 2024-06-26

The above candidate has researched for the Master's thesis under my supervision. I confirm that the declaration made above by the student is true and correct.

Name of the supervisor: **Prof. Shantha Fernando**

Signature of the supervisor: Date: 2024-06-27

ACKNOWLEDGEMENT

I would like to express my heartfelt gratitude to Prof. Shantha Fernando for the continuous support given throughout the degree program in imparting knowledge and guiding me throughout the dissertation.

Further, I would like to express my sincere gratitude to all the academic staff of the University of Moratuwa for providing necessary academic support throughout the degree program and sharing their vital knowledge and experience during the lectures. Moreover, I take this opportunity to express my gratitude to all the non-academic staff employees for their support in facilitating a good learning platform throughout my tenure at the university.

Last but not least, I would like to express my heartfelt gratitude to all my family members for providing the necessary support throughout my degree in numerous ways.

ABSTRACT

Multi-cloud systems' dispersed design offers issues in guaranteeing security for multi-cloud application components deployed across various clouds. As security concerns develop, cloud users are more interested in understanding the security state of their apps. The existing environment hinders the opportunity for enterprises to shift to the cloud, which may have provided an appealing alternative for corporations. As a result of this, it is vital to offer proper transparency and security attention in multi-cloud setups. A firewall is the main component that acts as the main shield for cloud assets. Managing a few cloud firewalls is becoming more and more complex when it comes to new cyber threats and concerns. This thesis explores the existing challenges in multi-cloud firewall management like lack of standardization, complexity and difficulty in enforcing security policies. This has been a significant problem due to operational overhead and security risks. The objective is to improve the dependability and trustworthiness of cloud services for organizations by applying appropriate security measures to solve current concerns in multi-cloud computing. This framework mainly includes the components like platform adaptor which converts the firewall rules into cloud-specific API calls and the orchestration engine which works as the heart of the framework. The proof-of-concept demonstrates the framework's ability to enforce context-aware policies, such as global restrictions or tag-driven access controls. This is a policy-driven framework for multi-cloud firewall management which is utilizing Open Policy Agent (OPA) and Terraform for infrastructure provisioning. The framework's effectiveness is demonstrated through a proof-of-concept implementation OPA based policy enforcement and configuration management using NOSQL database. The major goal of this research is to create a standard framework to administer multi-cloud firewalls and also this aims to reduce configuration errors, enhance security posture, and simplify auditability of firewall rules in multi-cloud environments.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	Description
AWS	Amazon Web Service
CSP	Cloud Service Provider
HLVQ	Hierarchical Learning Vector Quantization
IAAS	Infrastructure as a service
KVM	Kernel Virtual Machine
NFV	Network virtual function
NIST	National Institute of Standards and Technology
PAAS	Platform as a service
SAAS	Software as a service
SDN	Software-defined Networking
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNF	Virtual Network Function
WAN	Wide Area Network

LIST OF APPENDICES