

**Network Intrusion Prevention System Based on Enhanced
Snort Rules to Protect Network Resources from DoS &
DDoS Attacks
(An Empirical Approach)**

G.R.C. Kumara

139193P

Dissertation submitted to the Faculty of Information Technology,
The University of Moratuwa, Sri Lanka for the partial fulfilment of the
requirements of the Degree of Master of Science in
Information Technology.

March 2021

Declaration

I declare that this dissertation is my work and has not been submitted in any form for another degree or diploma at any university or other institution of tertiary education. Information derived from the published or unpublished work of others has been acknowledged in the text and a list of references is given.

Name of Student

Signature of Student (s)

Date:

Supervised by

Name of Supervisor (s)

Signature of Supervisor (s)

Date:

Dedicated to
my parents, my teachers

Acknowledgement

I would like to thank and gratitude the individuals for their contribution and motivation in various ways to make this research project a success.

First of all, I would like to express my gratitude to Dr C.R.J. Amalraj, my Supervisor, for his guidance, encouragement, tact, guidance, mature and intelligent advice, suggestions, positive thoughts and optimistic encouragement to continue to make this project a success. The supervisor also helped me to succeed in my future career as well as academics by encouraging me to overcome difficulties. I was lucky enough to do this research project under his supervision.

As well I am deeply grateful to senior lecturers Mr Saminda C. Premarathna and Mr Chaman P. Wijesiriwardhana for their support and continuous help to succeed in this endeavour.

Further, I would like to offer my special thanks to the senior lecturer of the faculty Mr B.H. Sudantha for his continuous support of the success of the project work.

I gratefully acknowledge Dr Lochandaka Ranatunga for initiating a research project and giving a more effective start on the path to success.

Again, I am also in debt too to the evaluators of the interim presentation of this project, Mr D.K. Withanage, Mr S.C. Premarathne, and Mr B.H. Sudantha for their valuable advice and comments to improve my work.

I am indebted to Mr D.K. Withanage, Mr S.C. Premaratne and Mr B.H. Sudantha, the Interim Project Evaluators, for their advice and suggestions on how to drive the research a success.

Also, I am once again indebted to the final evaluator's Dr C.R.J Amalraj, Mr B.H Sudantha and Dr T. G. I. Fernando of the project for their valuable advice in making the dissertation successful and correcting the shortcomings of the research project.

I would like to offer my special thanks to Professor Asoka Karunanada who taught us the "Research Methodology" subject for this master program on behalf of his guidance and motivations to research thinking and handling.

Furthermore, I would like to extend my sincere thanks to other academic staff, academic support and none academic staff members, those who support me in many ways in the IT faculty, UoM.

Again, I should grateful for Prof. Asoka Karunananda our teacher in “*Literature review & Thesis Writing*” who guided us for better researching and dissertation writing.

I would specially thank Mr Saminda Premaratne the course coordinator, MScIT, UoM for his encouragement and advice on this project.

Furthermore, I would like to extend my sincere thanks to my former director-general Prof. Kapila C.K. Perera who directed me to this M.Sc. program in the Faculty of IT, University of Moratuwa and my present director-general Dr W. Hilary E. Silva for always encouraging academic staff towards the research culture in Sri Lanka Institute of Advanced Technological Education (SLIATE). Further, I would be thankful to the director -Eng. Mr N.K.A. Rupasinghe, staff members and students in my institute, ATI Galle for being patient on my busy schedule. In addition, I would like to specially acknowledge the financial assistance offered by the HETC Project, Ministry of Higher Education.

I am grateful to my wife Manoja for her unwavering support in this endeavour and her patience and support and for the loving son Manula, who lost my attention and love during this period. Moreover, I would like to thank my friends and colleagues in the master program who encouraged me with their ideas and experiences to complete the project.

Finally, I would like to express my gratitude to the authors of the most important scholarly works that have been adopted for this research project. Here, Prof Buchanan B., Flandrin F., Richard Macfarlane, Dr Jamie Graves from Edinburgh Napier University are majors for utilizing their methodology to evaluate rate-based IPS in this research work and I am much graceful to them for their contribution to academia.

Finally, in the face of this scientifically significant research project and dissertation, I thank and thank all the gods who have given me unwavering courage, strength, and guidance.

Abstract

Virtual computers from anywhere in the world are designed to enable any user to access the computer resources contained in the cloud computing (CC) environment. The flour resources in the cloud environment, which pose a great threat to security, are shared so that they can be accessed by users anywhere in the world. Denial of service and denial of distributed services is one of the leading challenges posed by attackers who pose a serious threat to CC's security. Next Generation Invasion Prevention Systems (NGIPS), also known as non-traditional invasion prevention systems or next-generation invasion prevention systems, is being introduced as a tactic to overcome these offensive challenges. Thus, the author intends to find research results on the technological strategies used in NIPS and their evaluation and to find solutions to the challenges of cloud computing (CC).

The author has used a very systematic literature review to explore and identify the latest NIPS techniques using Inspec, IEEE, ACM Digital Library, Wiley, Scopus and Google scholar library databases. Articles are selected based on the acceptance and rejection formula when selecting for literature review. This experimental methodology has been selected as a research methodology for experimental comparison of the source and destination approaches of Snort NIGPS. The experimental bed is designed and deployed using Snort filtering techniques deployed in a virtual machine through a virtual switch in a virtual environment.

In this research, the author involves in finding the answers to the research problems and the first problem was the use of next-generation IPS technologies to protect the cloud computing surrounding from DoS and DDoS attacks. The second and third research questions are identifying different types of measurements to assess the performance of NIPS, and the third is the find the performance skill among both source and destination approaches of Snort Intrusion prevention systems.

Network engineers, network administrators and academia has been considered as users of the research scope. The hypothesis in this research is the filter will never work if the attack is launched on a large number of source IP addresses, and Snort will not be able to distinguish between legal and non-legal packets, even if the filter is functional. Finally, the null hypothesis used is the Snort does not show any difference between both source and destination approaches.

TCP, UDP, HTTP and mixture of the protocols used as attack input using LOIC attack tool and legitimate traffic inputs to the system generated using JMeter tool and Further, TCPReplay has been used to regenerate the same amount of both attack and normal traffic to maintain the justification and all those considered as independent variables. The dependent variables considered as the output of the research results are load on the CPU results, Utilization of the memory, availability of the Bandwidth, Delay (Latency), percentage (rate) of loss of packets.

In this research, the processes are the generating of both normal and attack traffics, detecting and preventing malicious traffic using Snort rate filtering rules. In the source approach, packet-based identification and filtering of packets are done by scanning the source IP address and enabling Snort to activate the filter if a specific packet rate is reached. Destination detection and filtering of packets are done by ordering Snort to swipe packets to the destination IP address and to enable filtering when a predetermined packet rate is reached.

NIPS strategic algorithms can be evaluated using classical metrics such as Load of the CPU, Utilization of Memory, Bandwidth availability, Delay (Latency), Rate of packet loss (both “false positives” and “false negatives”) and Accuracy. This experiment also found that when accessing parameters such as Load of the CPU, Utilization of Memory, Bandwidth availability, Delay (Latency) and Rate of packet loss, destination access was more efficient than source access. That is, the filtration rate system of the destination approach is more efficient.

Most of the NIPS technologies used in the Cloud Computing environment to protect from DoS and DDoS attacks are concluded as similar and interrelated. Furthermore, the author concludes that there is a difference in performance appraisal in the cloud computing environment between Snort's source and destination approaches.

Table of Contents

Chapter 01	14
Introduction.....	14
1.1. Prolegomena.....	14
1.2. Problem Definition.....	16
1.3. Aim & Objective	18
1.4. Brief Introduction of Solution.....	18
1.5. Construction of the Dissertation.....	19
1.6. Summary	19
Chapter 02.....	20
Review of others' work.....	20
2.1. Introduction	20
2.2. Background	20
2.2.1. Introduction to the Background Information.....	20
2.2.1.1. Virtual computing environment in data centers (DC) and the security issues.....	21
2.2.1.1.1. Cloud Computing.....	21
2.2.1.1.2. The Active models of cloud computing.....	22
2.2.1.1.3. Security in the cloud computing aspect.....	23
2.2.1.2. DoS and DDoS Attacks	24
2.2.1.2.1. Classes of DoS and DDoS Attacks	24
2.2.1.2.2. Application Used to Generate DoS And DDoS	26
2.2.1.3. Intrusion Prevention Systems	28
2.2.1.3.1. The Classification of IDS.....	29
2.2.1.4. IPS Types	29
2.3. The Literature Review.....	30
2.3.1. The Scope of the Research	30
2.3.2. A Brief Introduction to Literature Review	31
2.3.3. Plan for better Literature Review	31
2.3.3.1. The Importance of the Literature Review	31
2.3.3.2. Research Question	32
2.3.3.3. Selection of Keywords.....	32
2.3.3.4. Rules of Analyzing the literature	33
2.3.3.5. Selection of Appropriate literature.....	33
2.3.3.6. Method of Academic Study Selection	33

2.3.4.	Others methodology to solve the similar problems	35
2.3.4.1.	The outcome of the Literature Review	35
2.3.4.2.	Techniques Used in NGIPS	35
2.3.4.3.	Parametric for system evaluation.....	40
2.2.	Summary	42
Chapter 03	43
Technology Adopted	43
3.1.	Introduction	43
3.2.	Technology Adopt to Solve the Problem	43
3.3.	TCPreplay.....	43
3.4.	LOIC (Low Orbit Ion Canon):	44
3.5.	JMeter.....	44
3.6.	Snort	45
3.7.	Other tools and Technologies.....	45
3.8.	Why These Techniques are Appropriate to Solve the Problem	46
3.9.	Summary	46
Chapter 04	47
Approach	47
4.1.	Introduction	47
4.2.	How does the author adopt the technology to solve the said problem?	47
4.3.	Hypothesis	48
4.4.	Input (Independent Variable)	48
4.5.	Output (Dependent variables)	49
4.6.	Process.....	50
4.6.1.	Generation of input traffic	50
4.6.1.1.	Generation of attack traffic	50
4.6.1.2.	Generation of normal traffic	50
4.6.2.	Detect & Prevent malicious traffic	50
4.7.	Features / Technology	51
4.8.	Users.....	51
4.9.	Summary	51
Chapter 05	52
Analysis and Design	52
5.1.	Introduction	52
5.2.	Details of Design (analysis & Design).....	52

5.2.1.	High level Design Diagram of the Proposed System	53
5.2.1.1.	The Generation of Traffic	56
5.2.1.2.	Insert capture traffic	56
5.2.1.3.	Passing traffic through IPS	57
5.2.1.4.	drop or pass the network traffic	57
5.2.1.5.	measure the evaluation metrics	57
5.2.1.6.	designing the evaluation	58
5.3.	Theoretical Analysis of the Architecture.	58
5.3.1.	Network Intrusion Detection approach.....	58
5.3.2.	Snort Rule Modification	60
5.4.	Statistical Analysis	63
5.4.1.	Introduction to Design of Data Analysis	63
5.4.2.	Parametric Test	63
5.4.3.	Justifying the Results from Iterated Experiment Sessions (Mean Square Error (MSE)).....	63
5.4.4.	What is Wilcoxon Assessment?	65
5.4.5.	Design of hypothesis	66
5.5.	Summary	66
Chapter 06	67
Implementation	67
6.1.	Introduction	67
6.2.	Overview of the implementation.....	67
6.3.	Experiment Design.....	68
6.3.1.	Construction of the test bed	68
6.3.2.	Construction of two variants of traffic production, legal and non-legal components.....	70
6.3.3.	Determining the evaluation parameters.....	70
6.4.	This section Provide implementation details of each module that is stated in the design diagram.	71
6.5.	The Implementation of Snort IPS	72
6.6.	Generating the legal and illegal data traffic flows	73
6.7.	The Implementation of Metrics.....	74
6.8.	Summary	76
Chapter 07	77
Evaluation and Discussion	77
7.1.	Introduction	77

7.2.	Examination the deployment of the Experiment.....	77
7.3.	Evaluating Strategy	77
7.4.	For both source and destination approaches, finding the Average time of the execution for deployment with distinct protocols.....	78
7.5.	Results representation	78
7.5.1.	The load of the CPU	78
7.5.2.	Utilization of the Memory	81
7.5.3.	Availability of the Bandwidth	84
7.5.4.	Delay (Latency)	86
7.5.5.	Percentage of Loss of Packets	89
7.6.	Conducting the Wilcoxon Test.....	91
7.6.1.	Hypothesis assumption	91
7.7.	Summary	92
Chapter 08.....		93
Conclusion & Further Work		93
8.1.	Introduction	93
8.2.	Conclusion.....	93
8.3.	Problems encountered, limitations of the solution, and some further works.....	93
8.4.	Summary	94

List of Figures

Figure 1: Top-level view of Virtual computing environment in DC.....	21
Figure 2: The scope of the research	30
Figure 3: Regenerate the captured traffic 1.....	43
Figure 4: The command to repeat the traffic captured 2.....	44
Figure 5: Preparing TCP attack traffic toward the targeted Host.	44
Figure 6: An alert message produced with Snort IPS	45
Figure 7: High-level design diagram of the proposed system	53
Figure 8: High-level diagram of the Virtual Environment	54
Figure 9: High-level architecture diagram of the Snort IPS.	55
Figure 10: The arrangement of the testbed	69
Figure 11: The use of LOIC tool to generate a TCP protocol attack to the server	73
Figure 12: The use of JMeter tool to generate legitimate traffic flow toward the server	73
Figure 13: The load on the CPU Results in Source Approach	80
Figure 14: The load on the CPU Results in Destination Approach	80
Figure 15: The utilization of memory in source approach.....	83
Figure 16: The utilization of memory in destination approach.....	83
Figure 17: Availability of Bandwidth results in source approach	85
Figure 18: Availability of Bandwidth results in destination approach	86
Figure 19: Presence of Delay (Latency) results in source approach.....	88
Figure 20: Presence of Delay (Latency) results in destination approach.....	88
Figure 21: Percentage of loss of packets in Source approach.....	90
Figure 22: Percentage of loss of packets in Destination approach	91

List of Tables

Table 1: The academic material selection process.....	34
Table 2: The parametric adopted for assessment of NGIPS methods	40
Table 3: Malicious traffic inputs to the system.....	48
Table 4: Output from the system	49
Table 5: Parametric and the category of the selected parametric for evaluation	58
Table 6: Calculate the MSE corresponding to a ratio of 2000pps at source access for the CPU load parameter.	65
Table 7: The blueprint of machine design	69
Table 8: The hardware and software configurations of machines.	70
Table 9: Application locations for each tool to assess the metrics in the testbed.....	76
Table 10: The load on the CPU for the source approach	79
Table 11: The load on the CPU for the destination approach.....	79
Table 12: The utilization of memory in source approach	82
Table 13: The utilization of memory in the Destination approach	82
Table 14: Availability of Bandwidth in Source approach	84
Table 15: Availability of Bandwidth in Destination approach	85
Table 16: Delay (Latency) results in source approach.....	87
Table 17: Delay (Latency) results in destination approach	87
Table 18: Percentage of loss of packets in Source approach	89
Table 19: Percentage of loss of packets in Destination approach.....	90
Table 20: Statistical analysis of both source and destination approaches for CPU loads (Wilcoxon test).....	92
Table 21: Comparison between attack generation applications of DoS and DDoS	a
Table 22: The load on the CPU for TCP flood	c
Table 23: The load on the CPU for UDP flood	c
Table 24: The load on the CPU for HTTP flood	d
Table 25: The load on the CPU for Mix Protocol flood	d
Table 26: The utilization of memory for TCP floods	e
Table 27: The utilization of memory for UDP floods.....	e
Table 28: The utilization of memory for HTTP floods.....	f
Table 29: The utilization of memory for Mix Protocol floods	f
Table 30: Availability of Bandwidth for TCP flood	g
Table 31: Availability of Bandwidth for UDP flood	g
Table 32: Availability of Bandwidth for HTTP flood	h
Table 33: Availability of Bandwidth for Mix Protocol flood	h
Table 34: Presence of Delay (Latency) for TCP flood	i
Table 35: Presence of Delay (Latency) for UDP flood.....	i
Table 36: Presence of Delay (Latency) for HTTP flood.....	j
Table 37: Presence of Delay (Latency) for Mix Protocol flood	j
Table 38: Percentage of loss of packets in TCP flood	k
Table 39: Percentage of loss of packets in UDP flood	k
Table 40: Percentage of loss of packets in HTTP flood	l
Table 41: Percentage of loss of packets in Mix Protocol flood	l

ACRONYMS

CC	: Cloud Computing
PaaS	: Platform as a service
SaaS	: Software as a Service
IaaS	: Infrastructure as a Service
DoS	: Denial of Service
DDoS	: Distributed Denial of Service
IPS	: Intrusion Prevention Systems
IDPS	: Intrusion Detection Prevention Systems
NGIPS	: Non-Traditional Intrusion Prevention Systems
TIPS	: Traditional Intrusion Prevention Systems
CSP	: Cloud service providers
DC	: Data Center
MITM	: Man in The Middle Attack
NGIPS	: Next-Generation Intrusion Prevention Systems
ICMP	: Internet Control Message Protocol
TCP	: Transmission Control Protocol
UDP	: User Datagram Protocol
HTTP	: Hypertext Transfer Protocol
LOIC	: Low Orbit Ion Canon
GUI	: Graphical User Interface
RTT	: Round Trip Time
PRS	: Packet Resonance Strategy