

UNIVERSITI TEKNOLOGI MARA

**THE DEVELOPMENT OF TRUSTED NETFLOW
PACKET CAPTURING SYSTEM**

AHMAD FUAD MAT SOM

Dissertation submitted in partial fulfillment of the requirements
for the degree of

Master of Science (Computer Networking)

Faculty of Computer and Mathematical Sciences

May 2009

Abstract

Today, with the growing of new applications and software, network managers are keen to know what kind of traffic that flows in their network infrastructure everyday. Many protocols are available such as Simple Network Management Protocol (SNMP), packet sniffing and flow-based technology (NetFlow, JFlow and SFlow) can be used to obtain information about IP traffic.

Security measure must be taken into consideration when deploying these protocols especially the traffic comes from remote sites through public or unsecured channel. The challenge now is how secure this data can be sent to the monitoring server. In this dissertation we propose IPsec transport mode to be used to protect NetFlow packet sent from a Flow Probe to a Flow Collector.

Flow Probe will be tested to run on single machine. Analysis will be carried out to investigate the effect and performance.

Test bed lab has been set-up to experiment the proposed method. The test bed consist of a Flow Probe, a Flow Collector, a Linux router, three network switches and two units of PC acting as sender and receiver which installed each with traffic generator. To ensure that the proposed architecture will work and achieve the highest security computing, some tests are conducted. The traffic will be sniffed to show that the content of the packet is encrypted securely between Flow Probe and Flow Collector.

Acknowledgements

First of all, a gratefulness to Allah S.W.T for giving me willingness, strength and knowledge in completing this master dissertation.

Thank you to my parents, En Mat Som bin Tulus and Pn. Zainab binti Sidek, my wife Hanafiza binti Mohd Ali and my beloved son, Harith Danial for your endless support and love.

I also would like to express my sincere gratitude to my supervisor, En Farok bin Hj Azmat for his continuous support and guidance in completing this dissertation.

To my entire classmates CS778 batch 3, thanks for all the moral support, the knowledge that we shared and experienced together through out the courses.

Thanks again.

Wassalam.

Table of Contents	page
Abstract	iv
Acknowledgements	v
List of Tables	viii
List of Figures	ix
CHAPTER 1: INTRODUCTION	1
1.0 Introduction	1
1.1 Problem Statement	2
1.2 Objective of the research	3
1.3 Aims of the research	3
1.4 Significant of the research	3
1.5 Scope of the research	4
1.6 Thesis Organization	4
1.7 Summary	5
CHAPTER 2: LITERATURE REVIEW	6
2.0 Introduction	6
2.1 Technical Definition	6
2.1.1 Definition of Flow	6
2.1.2 Internet Protocol Security (IPsec)	9
2.1.3 IP Routing	18
2.1.4 Switching	18
2.1.5 Traffic Generator	18
2.1.6 Tcpcap	19
2.1.7 Libpcap	20
2.2 Related Studies	20
2.2.1 Network Monitoring with nProbe	20
2.2.2 nProbe: an Open Source Netflow Probe for Gigabit Networks	21

2.2.3 nFlow: Monitoring Flows on IPv4/v6 Networks	21
2.3 Summary	22
CHAPTER 3: RESEARCH METHODOLOGY	23
3.0 Introduction	23
3.1 Research Method Overview	23
3.1.1 Initiation Phase	27
3.1.2 Planning Phase	27
3.1.3 Network Design Phase	28
3.2 Verification Test Procedure	57
3.2.1 First verification test - IPsec connection turned OFF	57
3.2.2 Second verification test - IPsec connection turned ON	61
CHAPTER 4: RESULT ANALYSIS AND DISCUSSION	66
4.0 Introduction	66
4.1 Flow traffic without IPsec	66
4.2 Flow traffic with IPsec	70
4.3 Summary	74
CHAPTER 5: CONCLUSION AND RECOMMENDATIONS	75
5.0 Introduction	75
5.1 Recommendations and Future works	75
5.2 Limitations and Constrains	76
5.3 Conclusions	77
REFERENCES	78