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