NFQL: The Swiss-Army Knife of Efficient Flow-Record Processing

Vaibhav Bajpai, Johannes Schauer, Jürgen Schönwälder
School of Electrical and Computer Science
Campus Ring 1, Jacobs University Bremen
{v.bajpai, j.schauer, j.schoenwaelder}@jacobs-university.de

***Abstract*—Cisco's NetFlow protocol and IETF's IPFIX open standard have contributed heavily in pushing IP flow export as the de-facto technique for collecting aggregate network traffic statistics. These flow records have the potential to be used for billing and mediation, bandwidth provisioning, detecting malicious attacks and network performance evaluation. However, understanding certain traffic patterns requires sophisticated flow analysis tools that can mine flow records for such a usage. We recently proposed a flow query language that can cap such flow-records. In this paper, we introduce Network Flow Query Language (NFQL). an efficient implementation of the query language. NFQL can process flow records, aggregate them into groups, apply absolute (or relative) filters, invoke Allen interval algebra rules, and merge group records. The implementation has been evaluated by suite of benchmarks against contemporary flow-processing tools.**

I. Introduction

II. Design

III. Implementation

A. Filter

B. Grouper

1) Group Aggregations:

C. Group Filter

D. Merger

E. Ungrouper

IV. Performance Evaluation

V. Related Work

VI. Conclusion

The NFQL conclusion goes here [1]

References

[1] V. Marinov and J. Schönwälder, "Design of a Stream-Based IP Flow Record Query Language," in *Proceedings of the 20th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management: Integrated Management of Systems, Services, Processes and People in IT*, ser. DSOM '09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 15–28. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-04989-7$_2$