IPFIX
Internet Draft
Intended status: Informational
Expires: December 2013
June 16, 2013

R. Krishnan
Brocade Communications
Ning So
Tata Communications

Flow-state dependent packet selection techniques

draft-krishnan-ipfix-flow-aware-packet-sampling-05.txt

Status of this Memo

Copyright Notice

Abstract

The demands on the networking infrastructure and thus the switch/router bandwidths are growing exponentially; the drivers are bandwidth hungry rich media applications, inter data center communications etc. Using sampling techniques, for a given sampling rate, the amount of samples that need to be processed is increasing exponentially especially for applications like security threat detection. This draft elaborates on flow-state dependent packet selection techniques and the relevant information models. It describes how these techniques can be effectively used to reduce the number of samples for applications like security threat detection.

Table of Contents

1. Introduction

This draft expands on the flow-state dependent packet selection techniques described in [FLSEC] for identifying long-lived large

flows and the relevant information models. This draft also describes a practical use case for efficient behavioral security detection, like Denial of Service (DOS) attacks etc., using flow-state dependent packet selection techniques.

1.1. Acronyms

DOS: Denial of Service

GRE: Generic Routing Encapsulation

MPLS: Multi Protocol Label Switching

NVGRE: Network Virtualization using Generic Routing Encapsulation

TCAM: Ternary Content Addressable Memory

STT: Stateless Transport Tunneling

VXLAN: Virtual Extensible LAN

1.2. Terminology

Large flow(s): long-lived large flow(s)

Small flow(s): long-lived small flow(s) and short-lived small/large flow(s)

2. Flow-state dependent packet selection techniques

Expanding on the work in [FLSEC] and [RFC 5475], this draft suggests additional techniques for flow-state dependent packet selection for identifying large flows. One of these techniques is called Multistage Filters which is described in [ESVA]. This technique helps in automatically identifying large flows with a low false positive rate. This technique can be implemented as an inline solution in switches/routers and would be expected to operate at line rate.

Besides the Multistage filters technique described in [ESVA],

1) The technique suggested in [VRM] is also applicable. [VRM] suggests techniques for automatically identifying large flows using rotating conservative counting Bloom filters with periodic decay. This technique has a low false positive rate in large flow misidentification.

2) The sample and hold technique suggested in [ESVA] is also applicable. This technique has a low false positive rate in large flow misidentification.

The large flows which are automatically identified using the above techniques are populated in the IPFIX flow cache [RFC 6728]. If a large flow already exists in the IPFIX flow cache, the above techniques are not applied - this is the reason these are called flow-state dependent packet selection techniques.

Please note that there is a finite probability of small flows being misidentified as large flows. These are handled as described in the section 2.2 "Handling Inactive/Misidentified Large Flows".

2.1. Information Model for flow-state dependent packet selection technique con

From a bandwidth and time duration perspective, in order to identify large flows we define an observation interval and observe the bandwidth of the flow over that interval. A flow that exceeds a certain minimum bandwidth threshold over that observation interval would be considered a large flow.

The two configuration parameters -- the observation interval, and the minimum bandwidth threshold over that observation interval -- should be programmable in a switch or a router to facilitate handling of different use cases and traffic characteristics are defined below.

largeFlowObservationInterval: The minimum time interval to observe a flow before performing further processing of the flow. Unit is in milliseconds.

largeFlowBandwidthThreshold: The minimum bandwidth of the flow during the observation interval for declaring the flow a large flow. Unit is in Mbps.

For example, a flow which is at or above 10 Mbps for a time period of

at least 30 seconds could be declared a large flow.

Below is the list of flow-state dependent packet selection technique Information Elements:

ID	Name	ID	Name
TBD 1	largeFlowObservationInterval	TBD 2	largeFlowBandwidthThresho

2.2. Handling Inactive/Misid entified Large Flows

Once a flow has been recognized as a large flow, it should continue to be recognized as a large flow as long as the traffic received during an observation interval exceeds some fraction of the bandwidth threshold, for example 80% of the bandwidth threshold. If the traffic received during an observation interval falls below a fraction of the bandwidth threshold, the large flow should be removed from the IPFIX flow cache.

2.3. Flow-state dependent packet selection - sample and hold

[FLSEC] suggests some information model parameters for the sample and hold technique suggested in [ESVA]. The large flow information model parameters suggested in section 2.1 are complementary to these.

2.4. IANA Considerations

2.4.1. Registration of Information Elements

IANA will register the following IEs in the IPFIX Information Elements registry at http://www.iana.org/assignments/ipfix/ipfix.xml

IANA Note: please replace TBD1, TBD2, with the assigned values, throughout the document.

2.4.1.1. largeFlowObservationInterval

Description:

The minimum time interval to observe a flow for performing further processing of the flow.

Abstract Data Type: unsigned64

ElementId: TBD1

Units: milliseconds

Status: Current

2.4.1.2. largeFlowBandwidthThreshold

Description:

The minimum bandwidth of the flow during the observation interval (largeFlowObservationInterval)for declaring the flow a large flow. Unit is in Mbps.

Abstract Data Type: unsigned64

ElementId: TBD2

Units: Mbps

Status: Current

3. Current sampling techniques for security threat detection

Packet sampling techniques e.g. PSAMP -- [RFC 5474], [RFC 5475], [RFC 5476], [RFC 5477], in switches and routers provide an effective mechanism for approximate detection of various types of flows -- long-lived large flows and other flows (which include long-lived small flows, short-lived small/large flows) with minimal packet replication bandwidth overhead. The packet sampling techniques sample all flows equally.

A large percentage of the packet samples comprise of long-lived large (aka large) flows and a small percentage of the packet samples comprise of other (aka small) flows. The large flows aka top-talkers consume a large percentage of the bandwidth and small percentage of the flow space.

The small flows, which are the typical cause of security threats like Denial of Service (DOS) attacks, scanning attacks etc., consume a small percentage of the bandwidth and a large percentage of the flow space.

4. Application of flow-state dependent packet selection techniques for security

Using the flow-state dependent packet selection techniques described in Section 2, the large flows or top-talkers can be detected in real-time with a high degree of accuracy. Only the small flows need to be sampled -- this makes security threat detection more effective with minimal sampling overhead.

The steps in security threat detection are described below

1) Large Flow Identification:

For identifying large flows, use the flow-state dependent packet selection techniques described in Section 2. This helps in identifying the large flows aka top-talkers in real-time with a high degree of accuracy.

2) Large Flow Classification:

The identified large flows can be broadly classified into 2 categories as detailed below.

a. Well behaved (steady rate) large flows, e.g. video streams

b. Bursty (fluctuating rate) large flows e.g. Peer-to-Peer traffic

The large flows can be sampled at a low rate for further analysis or need not be sampled. If desired, the large flows could be exported to a central entity, e.g. Netflow Collector, using IPFIX protocol [RFC 5101] for further analysis.

3) Small Flow Processing:

The small flows (excluding the large flows) can be sampled at a normal rate. The small flows can be examined for determining security threats like DOS attacks (for e.g. SYN floods), Scanning attacks etc. [FDDOS, PDSN, and ALDS]

Thus, we can see that, security threat detection is possible with minimal sampling overhead.

4.1. Analysis of various flow-state dependent packet selection techniques

The multistage filter technique suggested in [ESVA] for automatic identification works well for standard applications generating large flows, for e.g. video content like movies and catch-up episodes, backup transactions etc. with a detection time of approximately 30-60

seconds. These detection times ensure that short-lived large flows, for e.g. HD video clips, are not unnecessarily recognized.

If faster large flow identification times are desired (much shorter than 30s), the multistage filter technique suggested in [ESVA] may pose the following problem that the effective filtered flow size is phase-dependent: that is, relatively smaller constant-rate flows, for e.g. HD video clips, beginning early within a counting Bloom filter reset interval would be unnecessarily detected with the same probability as relatively larger flows beginning toward the interval. [VRM] suggests techniques for addressing the above problem using rotating conservative counting Bloom filters with periodic decay.

4.2. Simulation

Simulation results for these flow-state dependent packet selection techniques are presented in Appendix A. The goal of the simulation is to demonstrate the effectiveness of these techniques for security

threat detection in a multi-tenant video streaming data center.

5. Security Considerations

This document does not directly impact the security of the Internet infrastructure or its applications. In fact, it proposes techniques which could help in identifying a DOS attack pattern.

6. Operational Considerations

For effectively using the flow-state dependent packet selection techniques, the operator should adjust the programmable parameters largeFlowObservationInterval and largeFlowBandwidthThreshold in switches/routers based on the applications which are being deployed.

7. Acknowledgements

The authors would like to thank Juergen Quittek, Brian Carpenter, Michael Fargano, Michael Bugenhagen, Jianrong Wong, Brian Trammell and Paul Aitken for all the support and valuable input.

8. References

8.1. Normative References

8.2. Informative References

[RFC 5474] N. Duffield et al., "A Framework for Packet Selection and Reporting", March 2009.

[RFC 5475] T. Zseby et al., "Sampling and Filtering Techniques for IP Packet Selection", March 2009.

[RFC 5476] B. Claise, Ed. et al., "Packet Sampling (PSAMP) Protocol Specifications", March 2009.

[RFC 5477] T. Dietz et al., "Information Model for Packet Sampling Exports", March 2009.

[RFC 5101] B. Claise, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information", January 2008

[RFC 6728] G. Muenz et al., "Configuration Data Model for the IP Flow Information Export (IPFIX) and Packet Sampling (PSAMP) Protocols"

[VRM] G. Bianchi et al., "Measurement Data Reduction through Variation Rate Metering", INFOCOM 2010

[PDSN] Ignasi Paredes-Oliva et al., "Portscan Detection with Sampled NetFlow", TMA 2009

[ALDS] Z. Morley Mao et al., "Analyzing Large DDoS Attacks Using Multiple Data Sources", SIGCOMM 2006

[FDDOS] David Holmes, "The DDoS Threat Spectrum", F5 White paper 2012

[ESVA] C. Estan and G. Varghese, "New Directions in Traffic Measurement and Accounting", ACM SIGCOMM Internet Measurement Workshop 2001, San Francisco (CA) Nov. 2001.

Appendix A: Simulation of Flow aware packet sampling

Goal:

Demonstrate the effectiveness of flow aware packet sampling in a practical use case, for e.g. multi-tenant video streaming in a data center.

Test Topology:

Multiple virtual servers (server hosted on a virtual machine) connected to a virtual switch (vSwitch) which in turn connects to the data center network using a 10Gbps ethernet interface.

2 virtual servers are active.

First virtual server

- Traffic types
    - HD MPEG-4 video streams (bit rate 10Mbps) - 100 - 1Gbps
    - SD MPEG-2 video streams (bit rate 4Mbps) - 300 - 1.2Gbps
    - Other traffic - 500Mbps (Video clips, DOS attacks (for e.g. SYN floods), Scanning attacks etc.)
- Aggregate traffic - 2.7Gbps

Second virtual server

- Traffic types
    - HD MPEG-4 video streams (bit rate 10Mbps) - 50 - .5Gbps
    - SD MPEG-2 video streams (bit rate 4Mbps) - 500 - 2.0Gbps
    - Backup transaction - 100Mbps
    - Other traffic - 500Mbps (Video clips, DOS attacks (for e.g. SYN floods), Scanning attacks etc.)
- Aggregate traffic - 3.1Gbps

Total traffic on 2 servers - 5.8Gbps

Existing techniques:

Normal sampling rate - 1:1000

Total sampled traffic = 5.8Gbps/1000 = 5.8Mbps

Flow aware sampling technique:

Large flow recognition parameters

- Observation interval for large flow - 60 seconds
- Minimum bandwidth threshold over the observation interval - 2Mbps

Aggregate bit rate of large flows = 4.8Gbps

Aggregate bit rate of small flows = 1Gbps

Low sampling rate of large flows - 1:10000

Normal sampling rate of small flows - 1:1000

Total sampled traffic = 4.8Gbps/10000 + 1Gbps/1000 = 1.48Mbps

Percentage improvement in sampling (most of the samples are only small flows) = (5.8 - 1.48)/5.8 ~= 78%

The small flows can be examined in a central entity like Netflow Collector for determining security threats like DOS attacks, Scanning attacks etc. Thus, we can see that, security threat detection is possible with minimal sampling overhead.

Authors' Addresses

Ram Krishnan
Brocade Communications
San Jose, 95134, USA

Phone: +001-408-406-7890
Email: ramk@brocade.com

Ning So
Tata Communications
Plano, TX 75082, USA

Phone: +001-972-955-0914
Email: ning.so@tatacommunications.com