SF-TAP: Scalable and Flexible Traffic Analysis Platform

https://github.com/SF-TAP/documents

Yuuki Takano Ryosuke Miura Shingo Yasuda Kunio Akashi Tomoya Inoue

usenix LISA15 Nov. 8 – 13, 2015 | Washington, D.C. SRE CULTURE METRICS
Sponsored by USENIX in cooperation with LOPSA

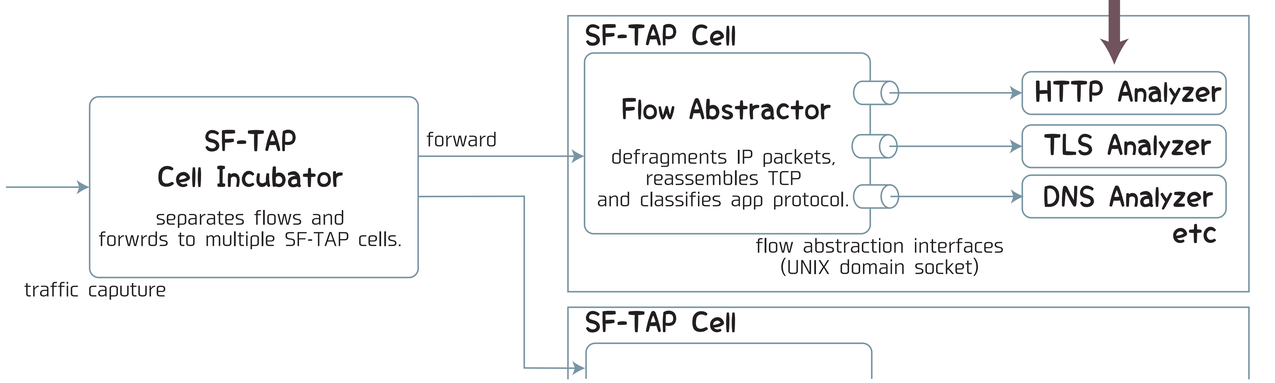
Design and Architechture

Horizontal Scalability!

SF-TAP separates high-bandwidth traffic and forwards to multiple pyshical machines.

Modularity!

You can implemente analyzers in any programming languages for IDS/IPS, forensic, machine larning, etc.



Commodity!

SF-TAP is available on commodity hardware environments.

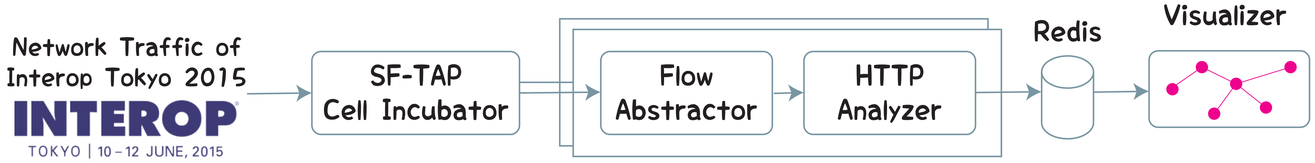
Multicore Scalability!

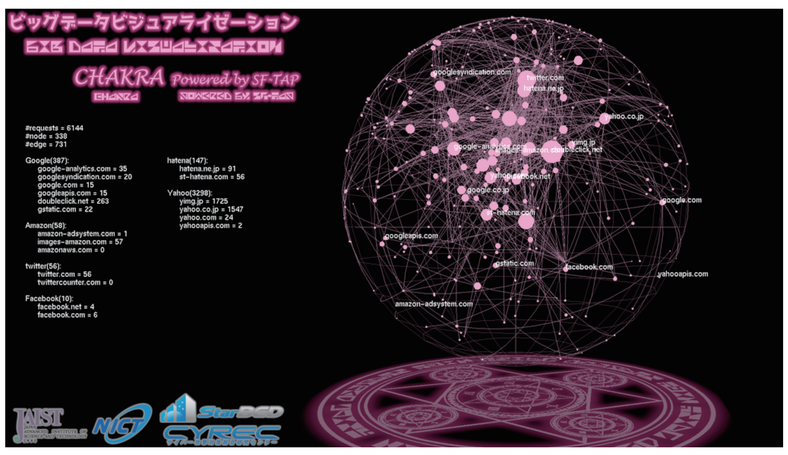
SF-TAP takes advantage of multi-threading.

Application-level Traffic Analysis

You do not have to handle compicated TCP/IP behavior. Just do analyze appication protocol!

Example Application: Realtime Web Graph Visualization on Interop Tokyo 2015





We captured network traffic of Interop Tokyo 2015, which is a huge business show for network technology, and analyzed HTTP traffic for visualizing web graph.

It revealed that SF-TAP can handle 10 Gbps network!

We took advantage of the modularity to implement the visualization tool.

Related Work

Yuuki Takano, Satoshi Ohta, Takeshi Takahashi, Ruo Ando, Tomoya Inoue, "MindYourPrivacy: Design and Implementation of a Visualization System for Third-Party Web Tracking", IEEE Twelfth Annual Conference on Privacy, Security and Trust, PST 2014, ISBN 978-1-4799-3503-1, pp 48-56

Configuration Example of Flow Abstractor

```
http:
  up:      '^[-a-zA-Z]+ .+ HTTP/1\.(0\r?\n|1\r?\n([-a-zA-Z]+: .+\r?\n)+)'
  down:    '^HTTP/1\.[01] [1-9][0-9]{2} .+\r?\n'
  proto:   TCP  # TCP or UDP
  if:      http # path to UNIX domain socket
  nice:    100  # priority
  balance: 4    # balanced by 4 IFs

torrent_tracker: # BitTorrent Tracker
  up:      '^GET .*(announce|scrape).*\?.*info_hash=.+&.+ HTTP/1\.(0\r?\n|1\r?\n([-a-zA-Z]+: .+\r?\n)+)'
  down:    '^HTTP/1\.[01] [1-9][0-9]{2} .+\r?\n'
  proto:   TCP
  if:      torrent_tracker
  nice:    90   # priority, higher than http

dns_udp:
  proto:   UDP
  if:      dns
  port:    53   # specify port number of TCP or UDP
  nice:    200
```

Implementation

SF-TAP Cell Incubator

https://github.com/SF-TAP/sf-incubator

C++ available on FreeBSD and Linux using netmap

Flow Abstractor

https://github.com/SF-TAP/flow-abstractor

C++ available on *BSD, Linux and MacOS X

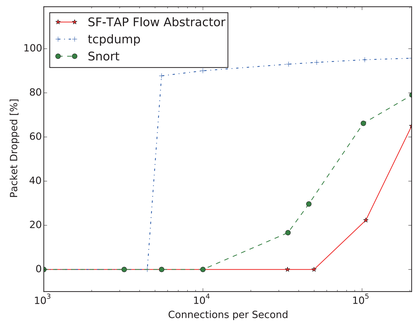
Example Analyzers

https://github.com/SF-TAP/protocol-parser

HTTP: Python3 DNS: C++

Performance Evaluation

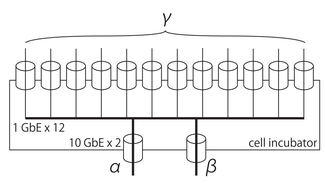
packet drop rate of the flow abstractor

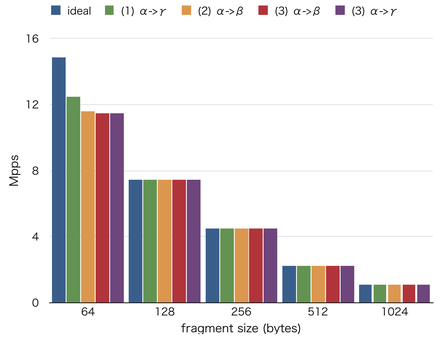


The flow abstractor can handle up to about 50 K connections per second.

The cell incubator can handle up to 12.49 M packets per second.

forwarding performance of the cell incubator





JAIST JAPAN ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY 1990
NICT National Institute of Information and Communications Technology
StarBED
CYREC サイバー攻撃対策総合研究センター