Scalable and Flexible Traffic Analysis Platform

SF-TAP（すうたっぷ！）

Yuuki Takano　Ryosuke Miura　Shingo Yasuda
Kunio Akashi　Tomoya Inoue

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

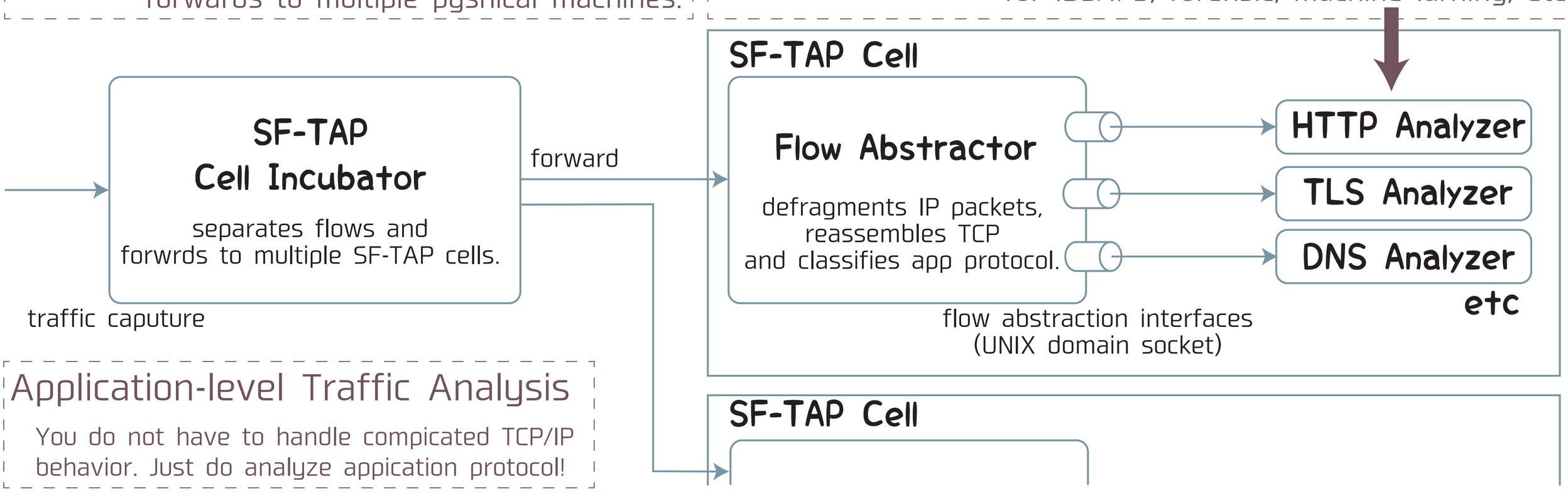
Design and Architechture

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.



Application-level Traffic Analysis

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

Commodity!

SF-TAP is available on commodity hardware environments.

Multicore Scalability!

SF-TAP takes advantage of multi-threading.

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++

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.