Getting More Information On Your Network Performance

Luca Deri <deri@ntop.org>

Network Traffic is a Moving Target

- For years network administrators have identified traffic protocols and services using IP address and ports:
  - Port 80 = HTTP.
  - Network x.y.z.0/24 identifies users of factory site Rome.
  - HTTPS is a secure connection to a web site.

- Unfortunately the above statements do not longer hold:
  - Protocols might use dynamic ports.
  - Well known ports might not carry the traffic we expect (80 != http).
  - Encryption does not always mean security (SSL vs OpenVPN).
  - Users moves and often do not need to connect back to the home network for carrying on their job.

The Cloud is Here

- Up to some years ago, software companies wanted to sell their products (e.g. word processors and spreadsheets).
- Today many people use collaborative services based on the cloud (e.g. Google Docs or MS Office 365).
- Remote conferencing (e.g. Webex or GoToMeeting) are all cloud-based.
- Popular apps such as EverNote used to keep track of notes on computers and mobile devices, storing your (private) data onto the cloud and not on your data centers (where you can enforce the security policy).

Network Health Monitoring is Complex

- Traditional network monitoring systems can limit their supervision activities to “home” networks.
- Mobile users, intra-VM data exchange, or cloud services are often invisible to network monitoring systems.
- Traditional firewalls are becoming blind as:
  - Generic (e.g. HTTP) protocols can be used to tunnel non-hypertext services (e.g. music streaming).
  - HTTPS is not checked so often it flows unrestricted.
- Cloud services access can’t be monitored with simple “periodic pings” as provides IPs are often unresponsive and change according to our location.

Traffic Performance Requirements

- Make sure that:
  - Locally provided services are in good health.
  - Remote services can be reachable with limited network latency.
  - Cloud services are accessed with good performance.
  - The management console can:
    - Passively track all traffic flows.
    - Identify the application used by each flow so that we can characterize the nature of the traffic flowing onto the network.
    - Compute KPI (Key Performance Indicators) so that network administrators can have a flavor of what is the current network health.

Network KPIs

- Literature and Internet RFCs defined base indicators including bandwidth, packet loss, latency and jitter.
- Those indicators however need to be associated with a protocol, so that we can trigger alerts:
  - VoIP callers notice roundtrip voice delays of 250 ms (G.114 recommends no more than 150 ms one-way latency) whereas they can operate on networks of limited bandwidth (e.g. 80 Kbit for G.711).
  - HTTP users can tolerate higher latency but pretend larger bandwidth.
- On a nutshell, application protocol detection is mandatory.

The need for DPI

- DPI (Deep Packet Inspection) is a technique for inspecting the packet payload for the purpose of extracting metadata (e.g. protocol).
- There are many DPI toolkits available but they are not what we looked for as:
  - They are proprietary (you need to sign an NDA to use them).
  - They are pretty costly for both purchase and maintenance.
  - Adding a new protocol requires vendor support (i.e. it has a high cost and might need time until the vendor supports it) = you're locked-in.
- Linux L7-filter is quite slow and error prone.
- On a nutshell DPI is a requirement but the market does not offer an alternative for open-source.

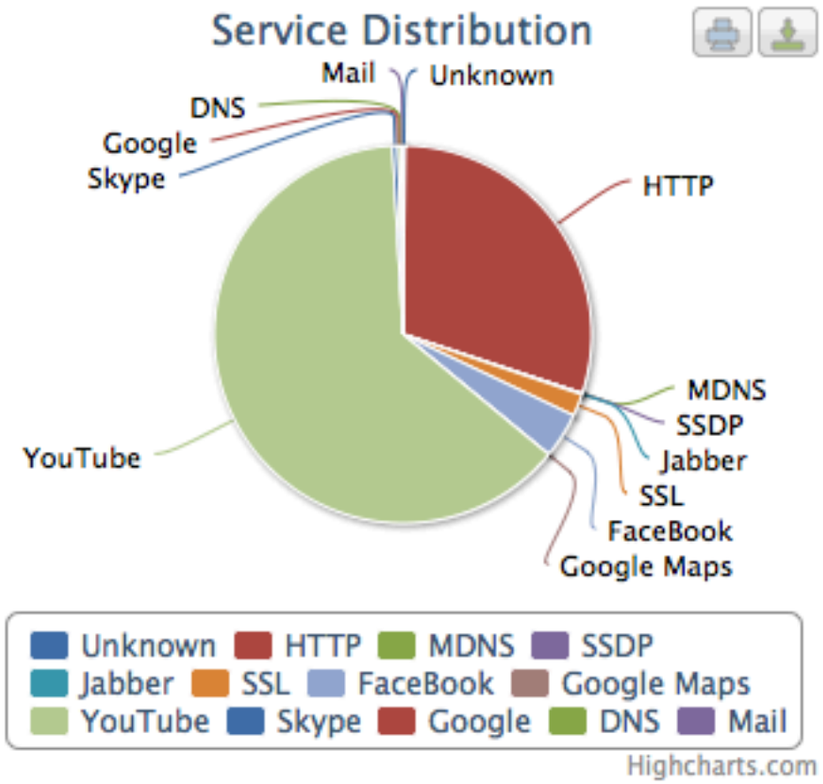
Say hello to nDPI

- ntop has decided to develop its own GPL DPI toolkit (based on a DPI toolkit OpenDPI.org now popped off the Internet) in order to build an open DPI layer for ntop and third party applications.

- Supported protocols (over 140) include:
  - P2P (Skype, BitTorrent)
  - Messaging (Viber, Whatsapp, MSN, The Facebook)
  - Multimedia (YouTube, Last.gm, iTunes)
  - Conferencing (Webex, CitrixOnLine)
  - Streaming (Zattoo, Icecast, Shoutcast, Netflix)
  - Business (VNC, RDP, Citrix, *SQL)

ntop/nProbe with nDPI

Application Protocol	Data	Percentage



Tracking Generic KPIs with nProbe [1/2]

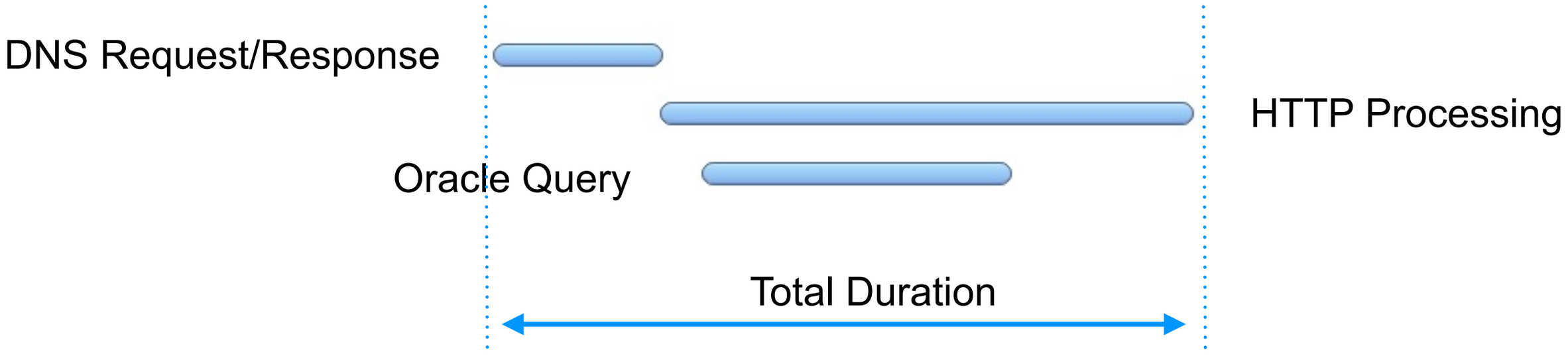
- nProbe is an open source network traffic probe developed by ntop and used in many products such as Würth-Phoenix NetEye.
- Recently nProbe has been enhanced for continuously tracking KPIs and not just at the beginning of each connection as in past versions.
- KPIs are complemented with protocol information detected by the nDPI toolkit.
- This enables network administrators to evaluate the application performance for the whole duration of the communication.

Tracking Generic KPIs with nProbe [2/2]

- Monitored Generic KPIs (per flow) include:
  - Network and application delay, partitioned in client and server delay (i.e. you know if the bottleneck is on the client or on the server side).
  - TCP packet retransmission (i.e. your network is leaking packets)
  - IP packets out-of-order (i.e. you have congestion issues)
  - TCP window change (i.e. monitor how healthy the TCP layer believes your connection is)

- All these KPIs are enough for giving a baseline of the connection healthiness and thus of your users perceive the provided network quality.

Monitoring Nested Communications [1/2]



- When customers experience slow service response, it is necessary to rebuild all communication elements, and identify the source of the delay.
- Correlation of network events helps to figure out which component(s) is responsible for the poor performance.

DNS Monitoring in nProbe

[NFv9 57677][IPFIX 35632.205] %DNS_QUERY	DNS query
[NFv9 57678][IPFIX 35632.206] %DNS_QUERY_ID	DNS query transaction Id
[NFv9 57679][IPFIX 35632.207] %DNS_QUERY_TYPE	DNS query type (e.g. 1=A, 2=NS..)
[NFv9 57680][IPFIX 35632.208] %DNS_RET_CODE	DNS return code (e.g. 0=no error)
[NFv9 57681][IPFIX 35632.209] %DNS_NUM_ANSWER	DNS # of returned answers
[NFv9 57558][IPFIX 35632.86] %APPL_LATENCY_SEC	Application latency (sec)
[NFv9 57559][IPFIX 35632.87] %APPL_LATENCY_USEC	Application latency (usec)

```
#
# When|DNS_Client|AS|ClientCountry|ClientCity|DNS_Server|Query|NumRetCode|RetCode|NumAnswer|
NumQueryType|QueryType|TransactionId|Answers|AuthNSs
#
1326819546.137|A.B.C.D|XXXX|US||192.12.192.5|blogsearch.google.it|0|NOERROR|0|1|A|52017||
ns2.google.com;ns1.google.com;ns4.google.com;ns3.google.com
```

HTTP Monitoring in nProbe [1/2]

[NFv9 57652][IPFIX 35632.180] %HTTP_URL	HTTP URL
[NFv9 57653][IPFIX 35632.181] %HTTP_RET_CODE	HTTP return code (e.g. 200, 304...)
[NFv9 57654][IPFIX 35632.182] %HTTP_REFERER	HTTP Referer
[NFv9 57655][IPFIX 35632.183] %HTTP_UA	HTTP User Agent
[NFv9 57656][IPFIX 35632.184] %HTTP_MIME	HTTP Mime Type

```
#
# Client   Server       Protocol     Method       URL            HTTPReturnCode       Location
           Referer      UserAgent    ContentType                 Bytes          BeginTime EndTime    Flow
Hash       Cookie       Terminator   ApplLatency(ms)             ClientLatency(ms)
           ServerLatency(ms)         Application BalancerHostServerIP RetransmittedPkts
#
192.168.1.92          www.facebook.com     http         GET          /ajax/presence/reconnect.php?
__a=1&reason=6&iframe_loaded=false&post_form_id=efe1a067adb2f9db341d72d56ce42c5b&__user
=675644907            200                  www.facebook.com/Repubblica?
v=wall&ref=HRHT-3 Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_1) AppleWebKit/534.48.3 (KHTML,
like Gecko) Version/5.1 Safari/534.48.3     application/x-javascript3181
           1318023905.364       1318023905.990       10622429241840       C
           367          0.038        128.810      Unknown                 69.171.224.40        0
```

Oracle/MySQL Monitoring in nProbe

```
[NFv9 57667][IPFIX 35632.195] %MYSQL_SERVER_VERSION    MySQL server version
[NFv9 57668][IPFIX 35632.196] %MYSQL_USERNAME          MySQL username
[NFv9 57669][IPFIX 35632.197] %MYSQL_DB                MySQL database in use
[NFv9 57670][IPFIX 35632.198] %MYSQL_QUERY             MySQL Query
[NFv9 57671][IPFIX 35632.199] %MYSQL_RESPONSE          MySQL server response
[NFv9 57672][IPFIX 35632.200] %ORACLE_USERNAME         Oracle Username
[NFv9 57673][IPFIX 35632.201] %ORACLE_QUERY            Oracle Query
[NFv9 57674][IPFIX 35632.202] %ORACLE_RSP_CODE         Oracle Response Code
[NFv9 57675][IPFIX 35632.203] %ORACLE_RSP_STRING       Oracle Response String
[NFv9 57676][IPFIX 35632.204] %ORACLE_QUERY_DURATION   Oracle Query Duration (msec)

#
# Client  Server      User        Query       ResponseCode        ResponseMsg
          Bytes       BeginTime   EndTime     QueryDuration(sec)  ClientLatency(ms)
          ServerLatency(ms)
#
0.62.4.118            10.62.6.211                     select * from COMPANY where JDOID
=78544    0                       310037      1333461770.861      1333461795.892
          0.024       0.000       0.000
```

Characterizing Encrypted Traffic

- As SSL usage is becoming pervasive, we cannot assume that SSL traffic is safe.
  - HTTPS can flow through proxies as follows:
    - CONNECT server.example.com:80 HTTP/1.1
  - CONNECT is insecure when:
    - It is used for bypassing the security as with Skype (connect with numeric IPs).
  - HTTPS/SSL is insecure when:
    - It is used as faked HTTP(s), e.g. used in OpenVPN for creating long-standing tunnels with the external sites.

How to Discriminate Good from Bad SSL ?

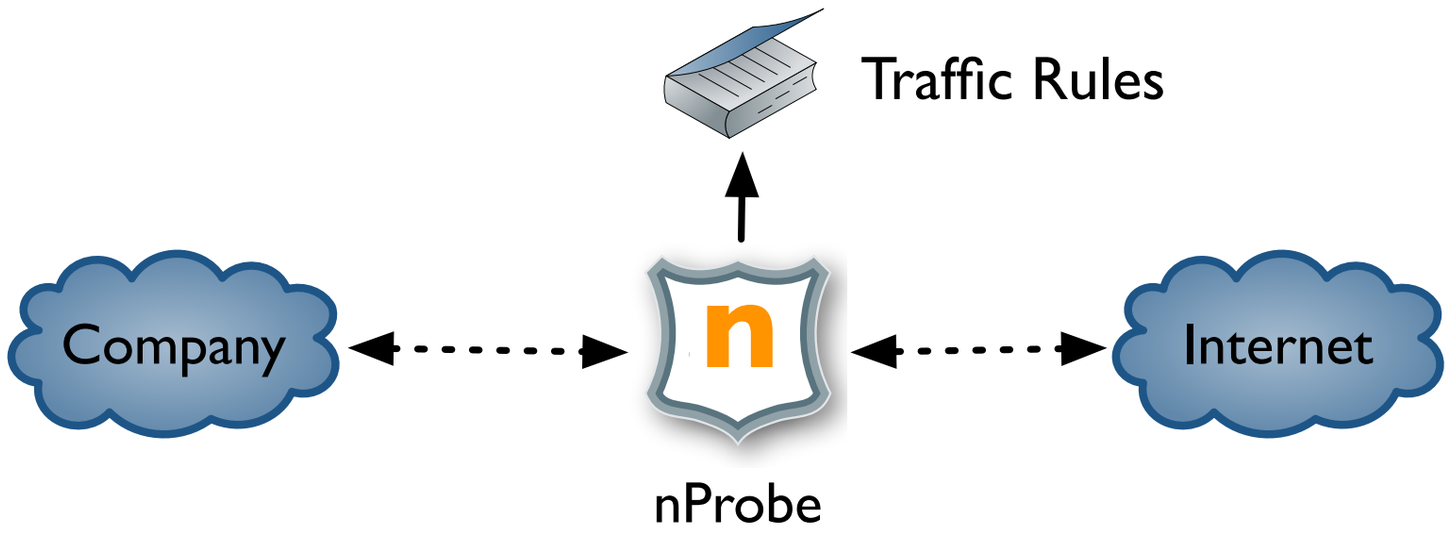
- It is necessary to:
  - Decode the SSL certificate in order to find out the symbolic name of the server we're connecting to.
  - Find out on the certificate, who has signed it in order to figure out if it's a self-signed certificate (thus not trustable)

- As of today nProbe and nDPI decode the certificate and use it for giving network administrators evidence.

```
192.168.1.92 www.facebook.com      https      0   99552  1335613695.591
             1335613700.723        106229198  0   C      0      0.090   74.162
192.168.1.92 www.mps.it            https      0   4925   1335613685.470
             1335613686.557        2209353430 0   C      0      0.039   36.204
192.168.1.92 www.intesasanpaolo.com https      0   19512  1335613677.972
             1335613708.776        2178073166 0   S      0      0.029   37.234
192.168.1.92 p05-caldav.icloud.com https      0   6274   1335613713.652
             1335613714.340        3528810468 0   C      0      0.071   84.526
```

What's next?

- We're developing an extension to nProbe that allows people to both
  - Generate flow records on monitored traffic.
  - Use the probe as application firewall that can block/pass/shape traffic based on layer 7 protocols.
  - You can for instance (per IP, MAC address) say "block Skype, shape Facebook to 32 KB, let all the other traffic pass"



Conclusions

- Generic KPI give administrators the ability to understand how the network is behaving.
- nDPI allows you to associate these KPIs with an application protocol and thus an application.
- nProbe provides protocol-specific information (e.g. URL, cookie, SQL query, called VoIP number, voice quality indicators) in order to enable information correlation and thus better visibility.

- All you have read on this presentation is immediately available onto every nBox/NetEye box as well for your virtualized environments.