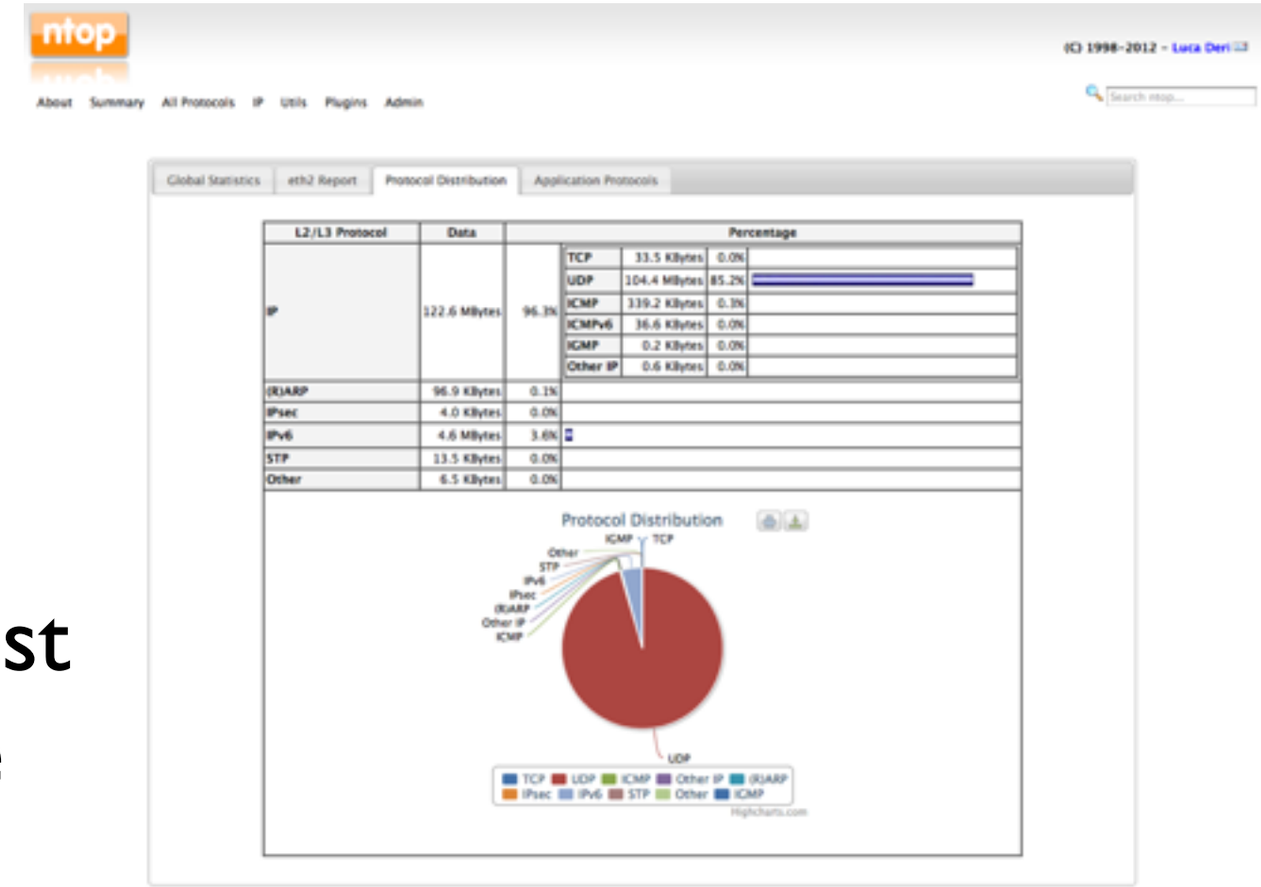
Il Monitoraggio del Traffico di Rete con Strumenti Open Source: ntop

Luca Deri <deri@ntop.org>

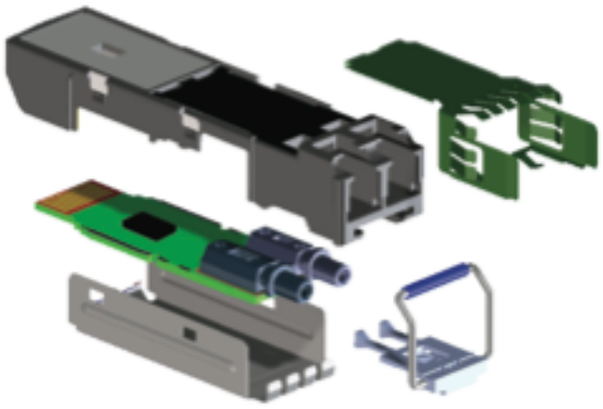
Open Source From The Source [1/2]

- ntop è un progetto di software libero iniziato nel 1998 da Luca Deri ed orientato al monitoraggio del traffico di rete.
- L'idea di rendere disponibile il codice sorgente è stato il modo migliore per promuovere il suo utilizzo, sviluppo, e test negli ambienti di rete più diversi.



Open Source From The Source [2/2]

Attualmente ntop è utilizzato da migliaia di aziende, funziona dentro prodotti di rete commerciali.



Integrated ASIC with JDSU technology

Alcuni Clienti che Usano ntop

Agilent Technologies
JDSU
intel
YAHOO!
AUTOGRILL
endace
power to see all
hp invent
Google
CISCO
swisscom
vodafone
TILERA
There's no better way to fly.
Lufthansa
eutelsat
COMMUNICATIONS
BT
WÜRTHPHOENIX
NetEye
solve problems, before they arise
cpacket
NETWORKS
plixer
International
Banca Intesa
CARABINIERI
consag
DANIELI
MONTE DEI PASCHI DI SIENA
BANCA DAL 1472
Ferrari
RACING
coop
IBM
Registro.it
THUN

Sistemi di Monitoraggio Commerciali [1/2]

- Gli strumenti di monitoraggio commerciali (es. Juniper, Cisco) sono costosi, limitati (di solito analizzano solo le intestazioni dei pacchetti) e raramente sono estensibili.
- Conseguenze:
  - L'evoluzione del monitoraggio è limitato dai produttori di apparati di misura.
  - I sistemi di monitoraggio hanno visibilità di ciò che il produttore vuole (es. Cisco TelePresence) e non di quello che gli utenti vorrebbero.

Sistemi di Monitoraggio Commerciali [2/2]

- Internet cambia troppo velocemente in termini di protocolli (Twitter, YouTube, NetFlix...) e versione di protocollo.
- I sistemi di misura commerciali cambiano in base al rilascio di nuovi prodotti hardware, e non quando nuovi paradigmi di monitoraggio si rendono disponibili.
- Le reti moderne sono pervasive (dal network core alla periferia con il BYOD [Bring Your Own Device]) e sistemi di monitoraggio troppo rigidi, limitati ad un solo produttore, sono ormai insufficienti.

Opportunità per L'Open-Source

- L'open-source ha una grande opportunità data la rigidità dell'offerta commerciale, contrapposta alle continue necessità di monitoraggio dei clienti:
  - Nuovi protocolli o specifici di una azienda.
  - Esigenze peculiari

- ntop+Würth-Phoenix hanno l'obiettivo di creare sistemi di monitoraggio avanzati, a prezzi inferiori rispetto ai vendor commerciali, capaci di monitorare ogni aspetto del traffico utente, senza dover incastrare troppi componenti eterogenei.

La Nostra Architettura di Monitoraggio

ntop nBox

Traffic Flows

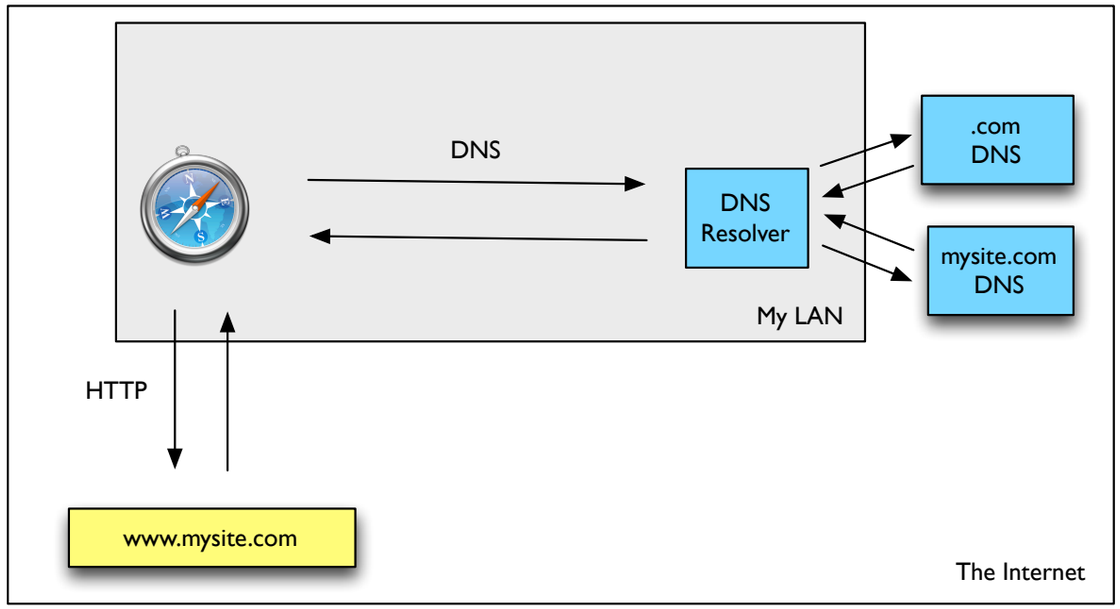
Würth-Phoenix NetEye

Perchè siamo Diversi ?

- Forniamo l'Evidenza dei Problemi di Rete
  - Gli amministratori devono sapere esattamente che cosa è successo.
- Misuriamo i KPM (Key Performance Metrics)
  - Riusciamo a misurare la "salute" della rete.
- Riconosciamo i Protocolli Applicativi
  - Non più IP:porta, ma Luca, Paolo.. DNS, FaceBook..
- Calcoliamo l'Andamento del Traffico di Rete
  - Forniamo gli indicatori di utilizzo per poter evolvere la rete prima che siano gli utenti a chiedercelo.

Evidenza dei Problemi di Rete [1/2]

- *"La navigazione di rete a volte è lenta, e a volte non riesco ad accedere ad un certo URL. Ripetendo l'operazione di solito risolvo il problema."*
- Sono i molti i componenti ed i protocolli coinvolti, come il DNS, l'HTTP.
- Per ciascun protocollo forniamo tutte le infomazioni, tempi di risposta, eventuali fallimenti e riprove dei sistemi di rete.



Evidenza dei Problemi di Rete [2/2]

- DNS

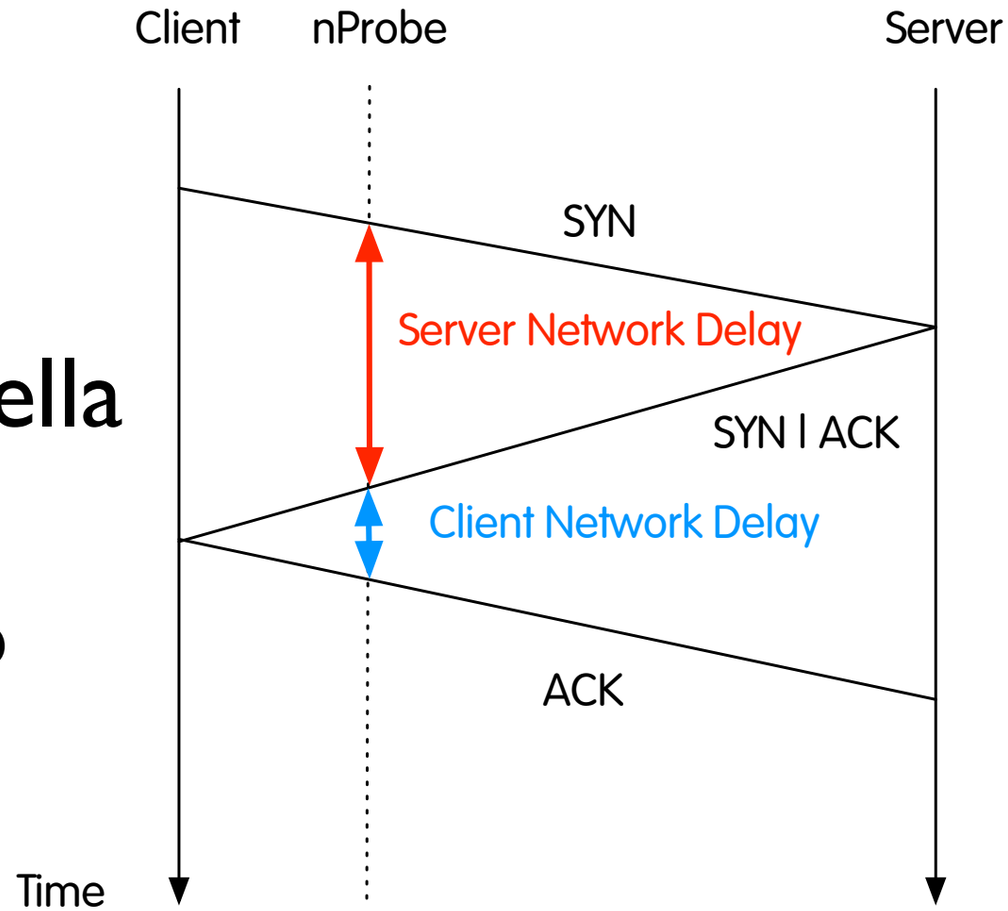
```
#
# When|DNS_Client|AS|ClientCountry|ClientCity|DNS_Server|Query|NumRetCode|RetCode|NumAnswer|NumQueryType|
QueryType|TransactionId|Answers|AuthNSs
#
1326819546.137|A.B.C.D|XXXX|US||192.12.192.5|blogsearch.google.it|0|NOERROR|0|1|A|52017||
ns2.google.com;ns1.google.com;ns4.google.com;ns3.google.com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

- HTTP

```
#
# Client        Server  Protocol        Method  URL     HTTPReturnCode  Location        Referer UserAgent       ContentType
Bytes   BeginTime       EndTime Flow Hash       Cookie  Terminator      ApplLatency(ms) ClientLatency(ms)
ServerLatency(ms)       Application
#
192.168.0.200   www.macintouch.com      http    GET     /images/filewave01.gif  200             www.macintouch.com      Mozilla/
5.0 (Macintosh; U; PPC Mac OS X; en) AppleWebKit/416.12 (KHTML, like Gecko) Safari/416.13
        27750   1133966828.928  1133966830.606  26992029        0       S       0.261   0.080   114.095 HTTP
```

KPI: Network/Application Delay

- Vengono misurate le latenze delle comunicazioni, in modo da identificare dov'è il collo di bottiglia e da chi è stato causato (rete, applicativo, computer).
- Le nostre misure riescono a suddividere i ritardi tra i vari componenti, ed a monitorarli durante tutto il ciclo di vita della comunicazione, in modo da calcolare come questi variano nel tempo.

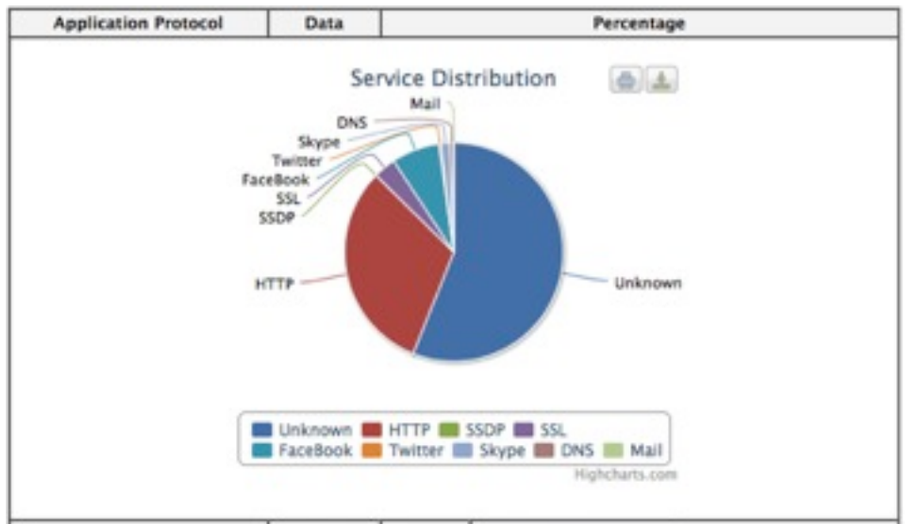


Protocolli Applicativi

- È importante riconoscere i protocolli applicativi:
  - Sapere quali protocolli utili (business) o inutili (es. Facebook) utilizzano la mia rete.
  - Verificare se le assunzioni sono giuste (es. Citrix occupa poca banda).
  - Identificare comunicazioni potenzialmente sospette (es. connessioni SSH di lunga durata).
  - Rilevare potenziali problemi di rete (es. protocolli conosciuti su porte non standard).
  - Stimare il grado di sicurezza delle comunicazioni (es. q.cuno stà usando dei protocolli "pericolosi" ?)

Open Source DPI: nDPI

- nDPI è una libreria open-source per il DPI sviluppata da ntop sulla base di un progetto precedente.
- Riesce a riconoscere oltre 140 protocolli applicativi (e.g. YouTube, Skype, Twitter, FaceBook, Citrix, SSL, email).
- È stata integrata con le sonde di rete in modo da poter offrire visibilità dei protocolli applicativi ai collettori di traffico (es. NetEye) per poter correlare le informazioni e calcolare il consumo di banda.



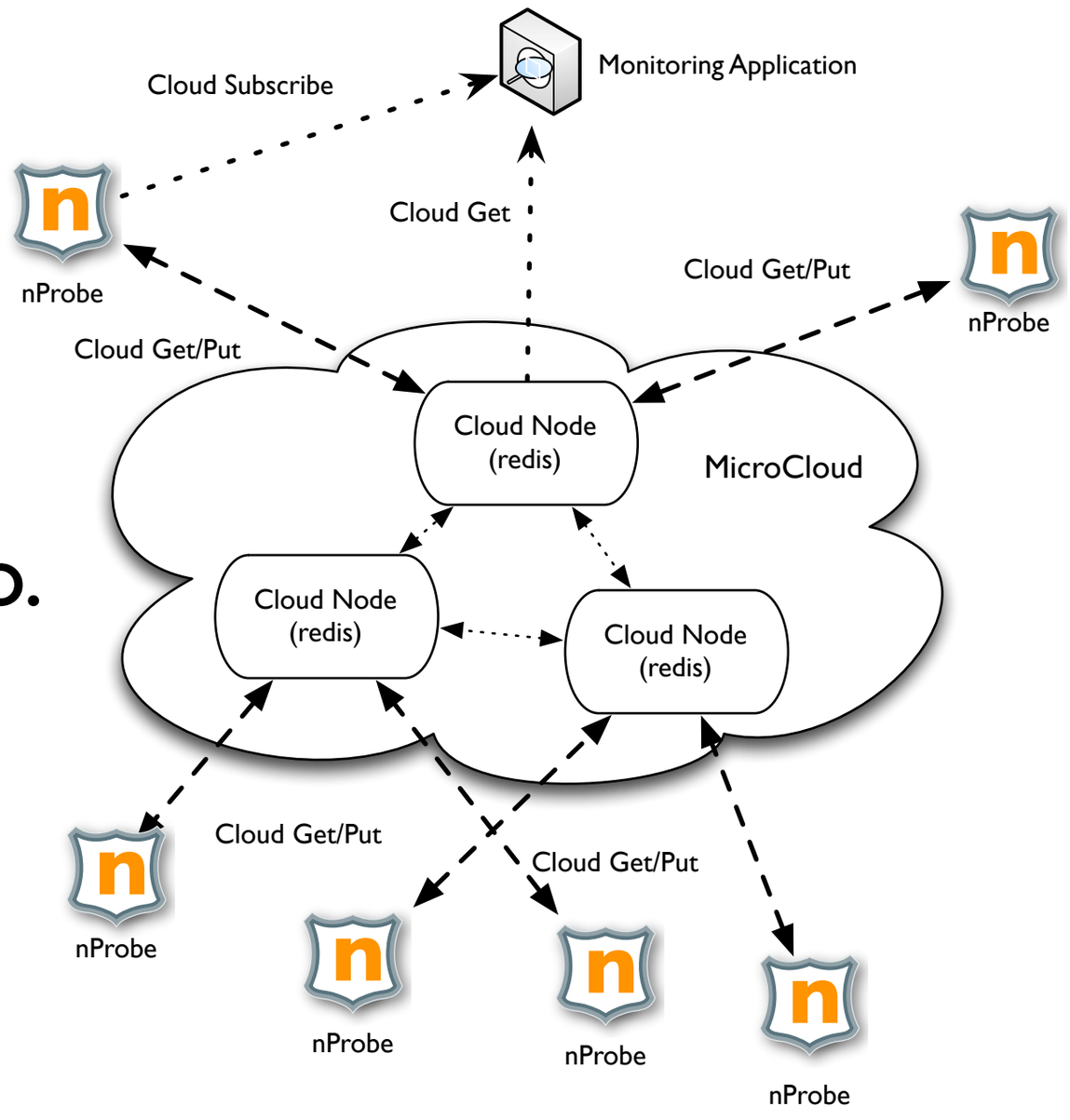
Application Protocol	Data	Percentage
Unknown	5.7 MBytes	56.1%
HTTP	3.2 MBytes	31.4%
SSDP	1.4 KBytes	0%
SSL	322.2 KBytes	3.1%
FaceBook	740.2 KBytes	7.1%
Twitter	32.1 KBytes	0%
Skype	132.3 KBytes	1.3%
DNS	64.4 KBytes	0%
Mail	0.7 KBytes	0%

Utenti+Servizi e non Indirizzi IP+Porte [1/2]

- Gli strumenti di monitoraggio spesso si limitano a riportare informazioni scorrelate (es. DNS, HTTP, latenze).
- È compito dei collezionatori: mettere assieme i pezzi.
- Questo però è molto complicato, non sempre realizzabile, e dispensioso in termini di risorse.
- Le nostre sonde riescono ad associare utenti (via Radius, GTP, Captive Portals e presto Win logon) con il traffico di rete.

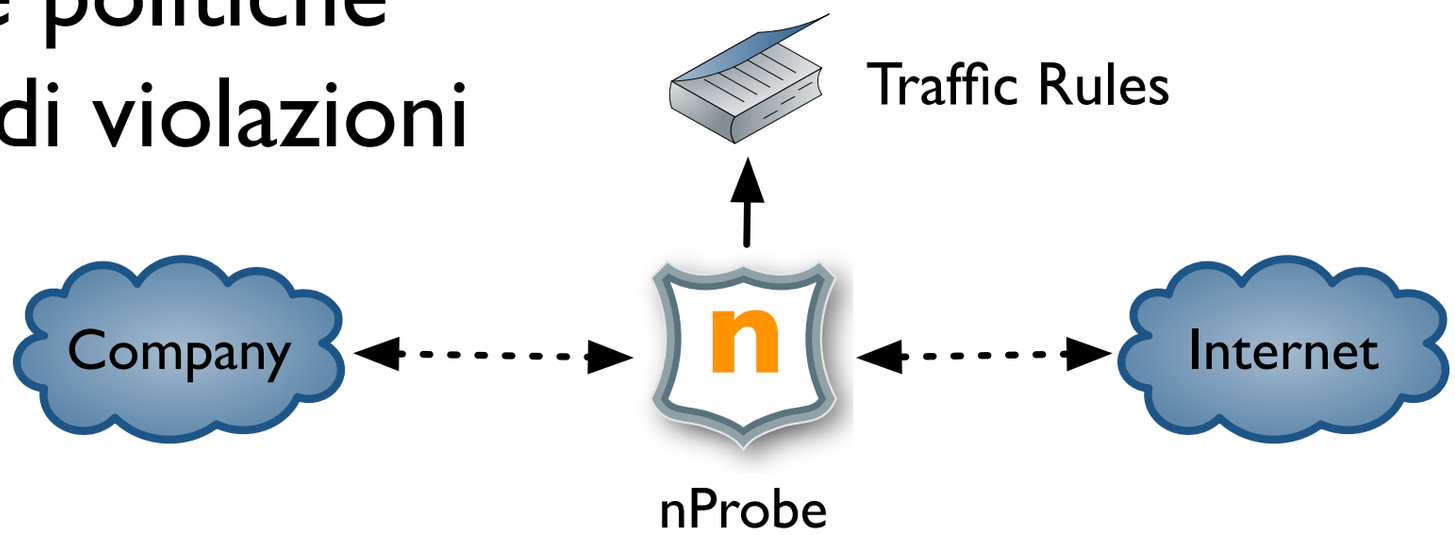
Utenti+Servizi e non Indirizzi IP+Porte [2/2]

- Le associazioni utenti, flussi di rete, protocolli sono memorizzate in una nuvola (*microcloud*).
- Vari componenti vi accedono e la arricchiscono.
- I sistemi di monitoraggio le utilizzano per correlare i dati: "Luca ha scambiato 3 MB con Facebook".



Oltre il Monitoraggio Passivo

- I moderni firewall/shaper sono componenti configurabili ma non programmabili. Ciò vuol dire che le politiche di rete sono rigide e non cambiano in base alle condizioni di traffico.
- È possibile usare le sonde per poter collaborare con il firewall/shaper (Linux) in modo da ripristinare le politiche di rete a fronte di violazioni



Conclusioni

- Il monitoraggio del traffico di rete richiede applicazioni aperte ad evoluzioni e capace di rispondere alle continue esigenze utente.
- Sistemi commerciali sono spesso troppo costosi ma soprattutto rigidi.
- Soluzioni aperte capaci di fornire rispose migliori e più economiche a richieste sempre più complesse.
- ntop e Würth-Phoenix hanno dimostrato che è possibile creare prodotti evoluti/aperti di monitoraggio di rete.