nprobe per monitoraggio traffico 4G

Marco Gottardello
Reti Spa

Chi sono

Marco Gottardello

Senior Manager @ Reti spa

@RETI NETworker since 2004

20+ Years in IT

Reti

- System Integrator con sede nel Campus Reti, 20.000 mq di uffici, laboratori e spazi per eventi a Busto Arsizio (VA)
- Fondata nel 1994
- BCorp e Società Benefit
- Quotata in Borsa Italiana - EGM
- 350 dipendenti
- 170 clienti attivi
- 25 Mln fatturato

Requisiti di Business

- Necessità di monitorare in modo puntuale la quantità di traffico di rete generato dai client operanti in modalità «Smart Working», connessi in rete mediante connessione 4G.

- Avere per tempo l'evidenza di consumi anomali per evitare addebiti di costi extra in caso di superamento della soglia contrattuale definita con l'operatore telefonico.

- Disporre di un sistema che permetta di raccogliere le informazioni sull'utilizzo della rete da parte dei client e di poter consultare tali informazioni mediante dei report centralizzati per una successiva analisi.

Requisiti Tecnici

- Le connessioni da monitorare sono WAN 4G, quindi con ip dinamico e dietro NAT/PAT
- Parte del traffico è incapsulato tramite la VPN aziendale, parte diretto verso Internet in split-tunnel. E' richiesto di poter categorizzare correttamente tale traffico.
- Non dovrà comportare impatti sulle prestazioni del client
- Il sistema dovrà permettere l'esportazione delle statistiche su sistemi esterni

Soluzione Implementata

nProbe + ntopng

Alcuni Soluzioni!

Ad inizio progetto (Marzo 2021) ci siamo scontrati con alcuni problemi

- Npcap non supporta la cattura su schede WWAN (4G)

  Npcap dalla versione 1.50 (Giugno 2021) non esclude piu le schede WWAN da quelle disponibili per la cattura

- Nprobe richiedeva di specificare l'id dell'interfaccia in fase di installazione del servizio, e l'id dell'adattatore VPN cambiava ogni volta

  Inserita in nprobe la possibilità di utilizzare il NOME dell'interfaccia (nprobe /c -i"*Juniper") e restare in attesa che l'interfaccia sia up

- Bisognava discriminare su ntopng il traffico dei diversi PC

Observation Point, con possibilità di assegnare una descrizione oltre al id.

- Era necessario poter elaborare i dati su base almeno mensile per produrre i report richiesti

  Integrazione ntopng con ClickHouse

Configurazione nprobe

Abbiamo sviluppato uno script Powershell per l'installazione e configurazione silente di nprobe.

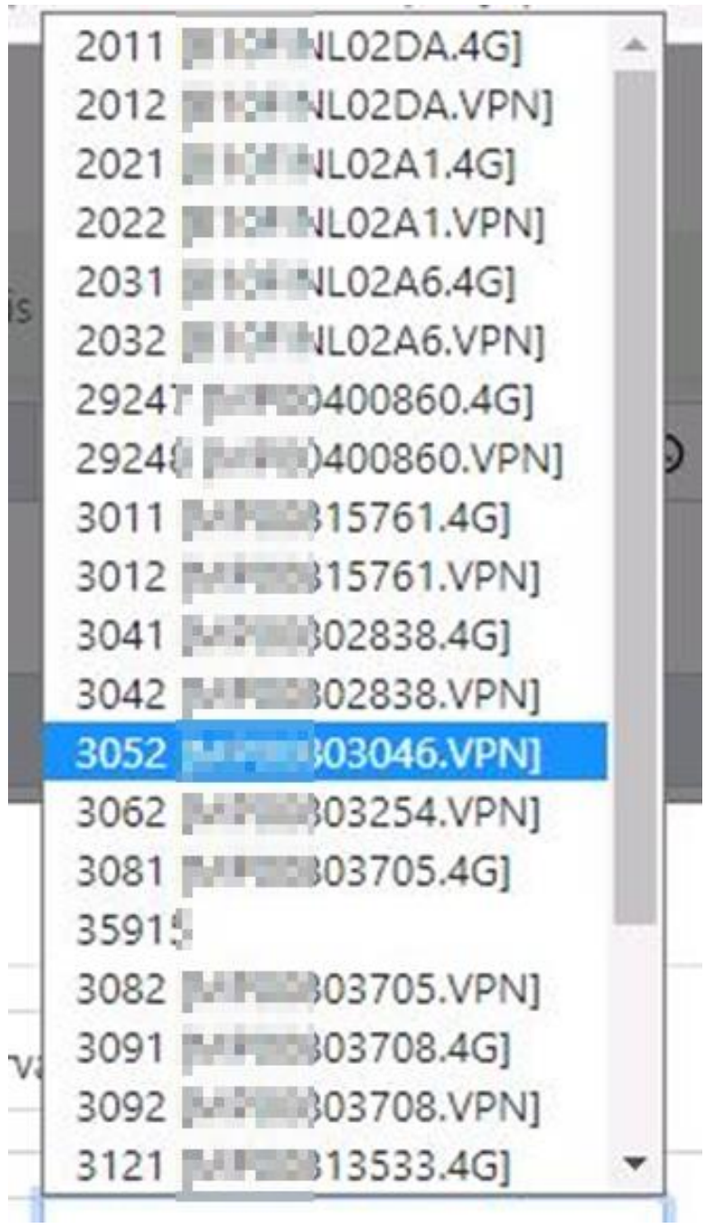
Lo script esegue l'installazione di 2 servizi nprobe: uno in ascolto sull'interfaccia del client VPN (*Juniper), l'altra sull'interfaccia WWAN 3G/4G.

Per la scheda WWAN, dato che il nome cambia in base al modello di macchina, viene fatta una ricerca sui NetAdapter di Windows alla ricerca della scheda corretta.

Configurazione nprobe

Lo script di installazione inserisce due ID univoci per gli observation point nella configurazione di nprobe in ogni PC.

Una volta che la sonda viene censita come observation point da ntopng, si procede all'aggiunta come descrizione del nome macchina e tipologia di interfaccia (VPN / 4G), cosi da semplificare la consultazione



Dettaglio traffico per PC

tcp://*:5556c 0 bps 0 bps

Search

Historical Flow Explorer | Flows Analysis

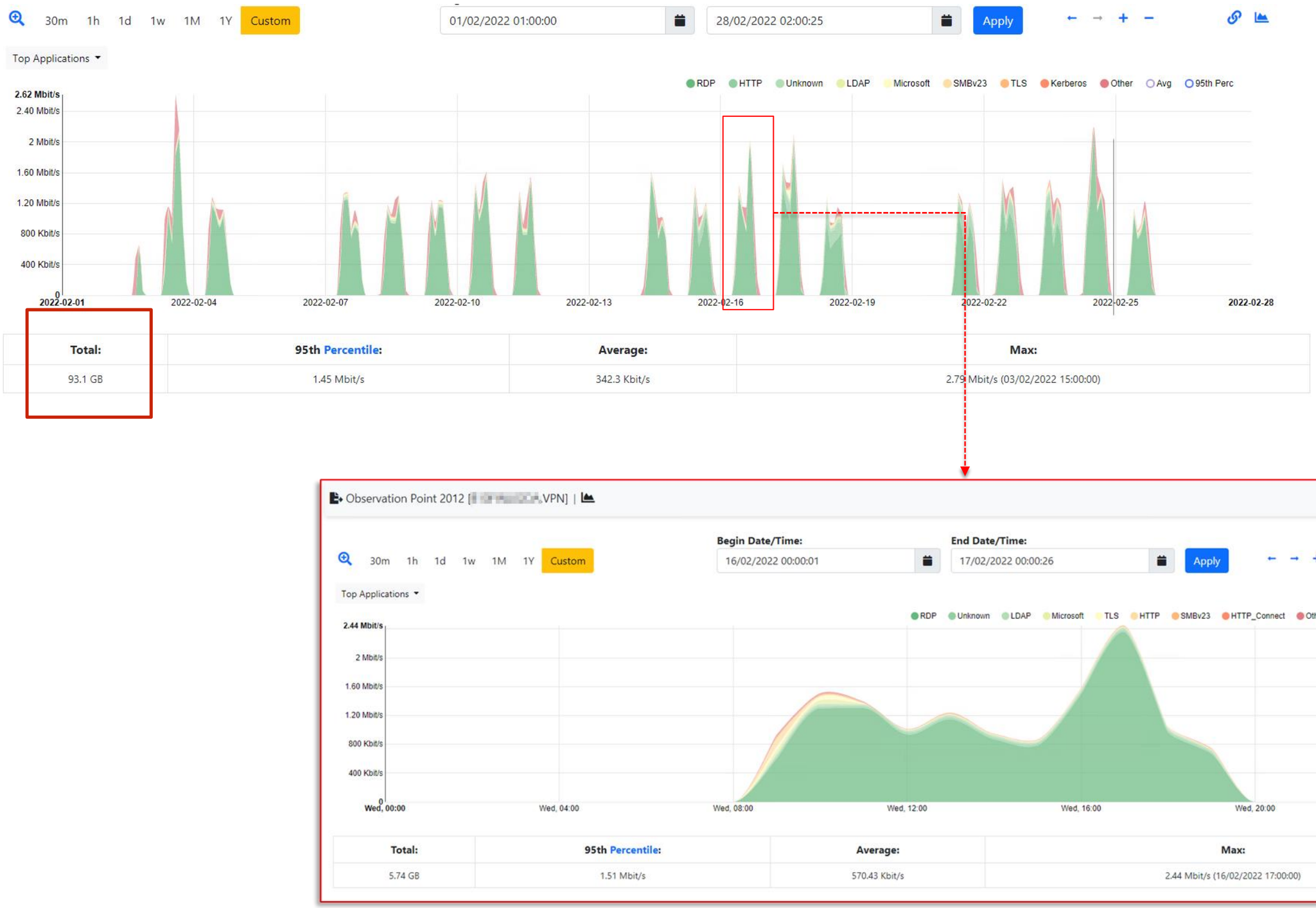
Flows | Custom | /01/2022 01:00 AM → /28/2022 00:00 PM | Apply | Chart View

Observation Point ID = 2012 × Filters

Show 200 entries

Flow	Protocol	Application	Score	Bytes	Thpt	Begin	End	Actions
l04f8.s 61172 ⇄ 10.19.65.124:53	UDP	DNS	0	160 Bytes	1.28 kbit/s	02/28/22 11:59:58	02/28/22 11:59:58	
l04f8.s 58366 ⇄ com:80	TCP	HTTP	100	18.19 KB	37.25 kbit/s	02/28/22 11:59:57	02/28/22 12:00:00	
l04f8.s 58365 ⇄ com:80	TCP	HTTP	100	12.73 KB	26.08 kbit/s	02/28/22 11:59:57	02/28/22 12:00:00	
l04f8.s 58362 ⇄ com:80	TCP	HTTP	100	18.1 KB	49.44 kbit/s	02/28/22 11:59:55	02/28/22 11:59:57	
l04f8.s 58361 ⇄ com:80	TCP	HTTP	100	12.87 KB	35.14 kbit/s	02/28/22 11:59:55	02/28/22 11:59:57	
l04f8.s 58358 ⇄ com:80	TCP	HTTP	100	18.1 KB	37.08 kbit/s	02/28/22 11:59:52	02/28/22 11:59:55	
l04f8.s 58357 ⇄ com:80	TCP	HTTP	100	12.56 KB	25.73 kbit/s	02/28/22 11:59:52	02/28/22 11:59:55	
l04f8.s 58356 ⇄ vsep230.sed :80	TCP	HTTP	0	962 Bytes	1.1 kbit/s	02/28/22 11:59:51	02/28/22 11:59:57	
l04f8.s 50933 ⇄ 10.19.65.124:53	UDP	DNS.Microsoft365	0	217 Bytes	1.74 kbit/s	02/28/22 11:59:51	02/28/22 11:59:51	
l04f8.s 58186 ⇄ sep230 :80	TCP	HTTP	0	200 Bytes	266.67 bit/s	02/28/22 11:59:51	02/28/22 11:59:56	

Andamento traffico



Prossimi passi

- Deploy massivo della soluzione (ad oggi limitato a 20 postazioni in fase di pilota)
- Valutazione di soluzioni per permettere la scalabilità a centinaia/migliaia di nprobe.
- Implementazione di report automatizzati con monitoring delle soglie di traffico mensile e relativi alert in caso di anomalie.

Contatti

marco.gottardello@reti.it

www.reti.it

https://www.linkedin.com/in/gotta/