Monitoraggio di rete Enterprise e la ricerca dell'araba fenice

Vecchiatti Federico

fvecchiatti@unicomm.it

Di cosa tenterò di parlare

Della *nostra esperienza di monitoraggio, cercherò di illustrare alcuni passi fatti, gli errori e la strada che pensiamo di dover percorrere ancora ...*

E perché siamo arrivati a ntopng !

Chi è Unicomm

Azienda della Grande Distribuzione Organizzata che opera nel Nord-Est e Centro Italia con vari marchi e società controllate e gestite.

250 negozi di proprietà
8000 dipendenti
12 centri logistici

Che per l'informatico sono:
- circa 400 server, 13.000 ip in rete;
- 18Tb DB2 movimenti logistici;
- 3 PetaByte storage;
- circa 2000 access-point
- ...

L’infrastruttura

Unico centro stella fornisce servizi a tutte le sedi periferiche su MPLS (fibra, 4G, xDSL, ponti radio, etc.) e accesso a Internet.

Fondamentali tempi di risposta e uptime:

- logistica lavora a colli e i tempi sono sempre limitati;

- «just in time» da per scontato che i ritardi se ci sono non sono nella infrastruttura che è per definizione (loro..) sempre presente ☺;

- le vendite si basano sulle code alle casse .. se il Bancomat non funziona i carrelli rimangono abbandonati con costi esponenziali;

- sempre più servizi online: bollettini, buoni sconto, Green Pass (sigh!);

La sfida del monitoraggio - 1

Ogni sede periferica ha criticità e contribuisce al traffico e ai problemi;

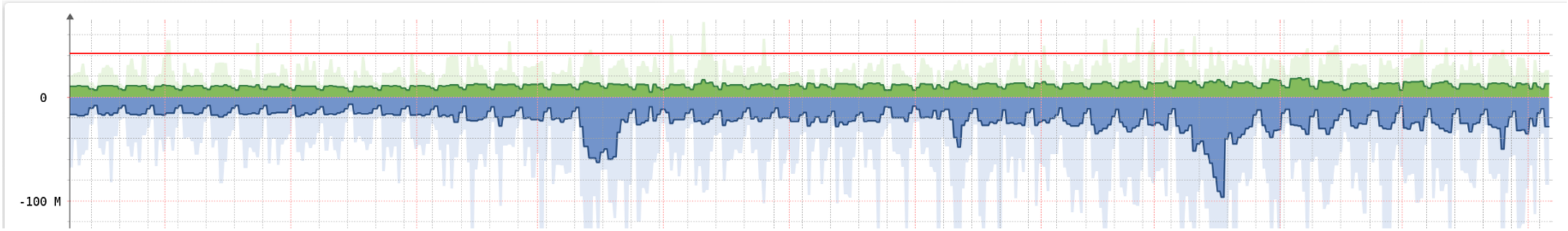
-> serve soluzione altamente scalabile in grado di gestire numeri significativi di informazioni con retention abbastanza lunga

Uno scontrino ogni 20-30 secondi di media per negozio: problemi rilevati in tempo reale in periferia con rientro anomalia lungo causa richieste, ticket, etc .

-> rapidità nell'individuare il problema perché il fault ha impatto esponenziale

La sfida del monitoraggio - 2

Tipologia di traffico nota, quello che si discosta dalla baseline è «anomalo» e con alta probabilità da analizzare.



-> Posso fare scelte semplificative entro certi limiti (es. firewall con policy da AS Italiani ..)

Il monitoraggio è in equilibrio tra Operation e Security.

-> Operation ha bisogno di sapere cosa sta impattando sulle performance attese

-> Security ha bisogno di sapere se qualcosa non è compliant con quanto atteso.

La sfida del monitoraggio - 3

Quello che servirebbe è un controllo continuo per Operation e allarmi mirati per Security.

-> «Vedono» dati simili ma gli output non sono necessariamente uguali (un flusso video per la formazione a distanza impatta Operation ma non Security, un download anomalo viceversa)

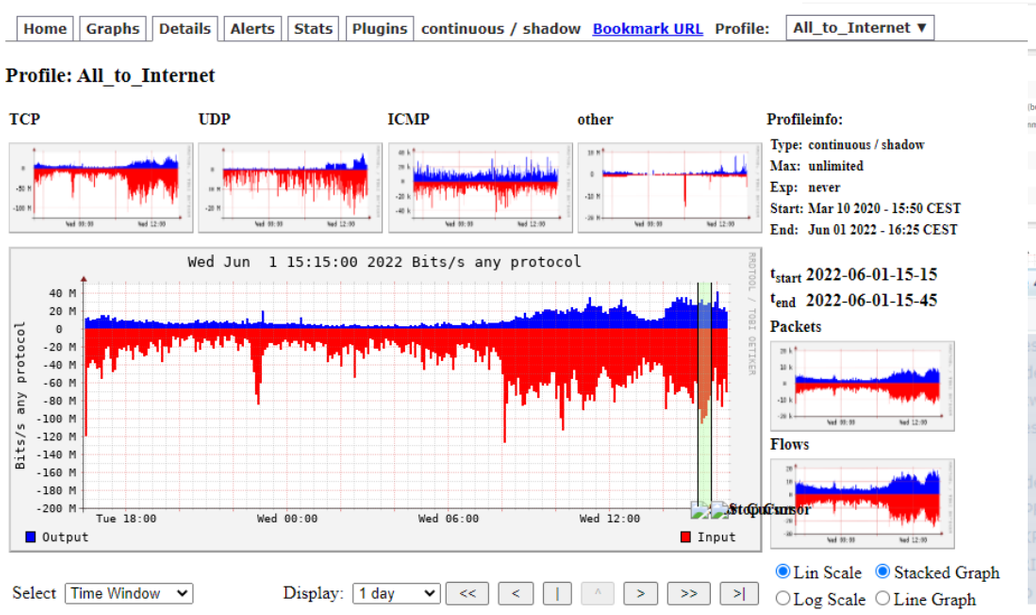
Il tutto con risorse anche umane limitate e con l'aggiunta o la rimozione di reti/sedi praticamente settimanale …

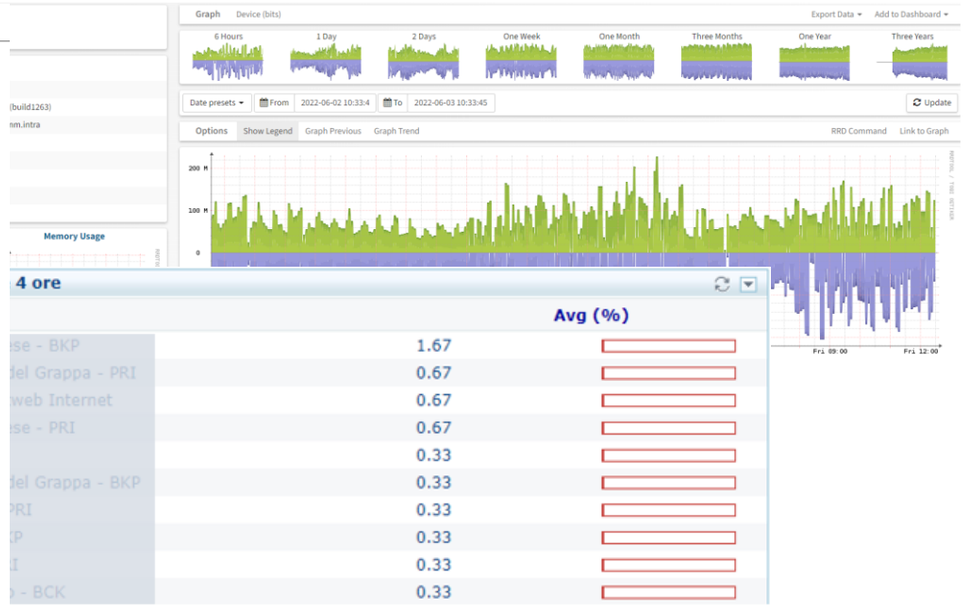
Cosa abbiamo usato e perché

Negli anni abbiamo aggiunto a soluzioni SNMP la raccolta di sFlow e NetFlow dai punti strategici della rete:

- *Aumentare costantemente la «visibilità» del traffico;*

- *Aggiungere «viste» sui flussi con specifiche caratteristiche*

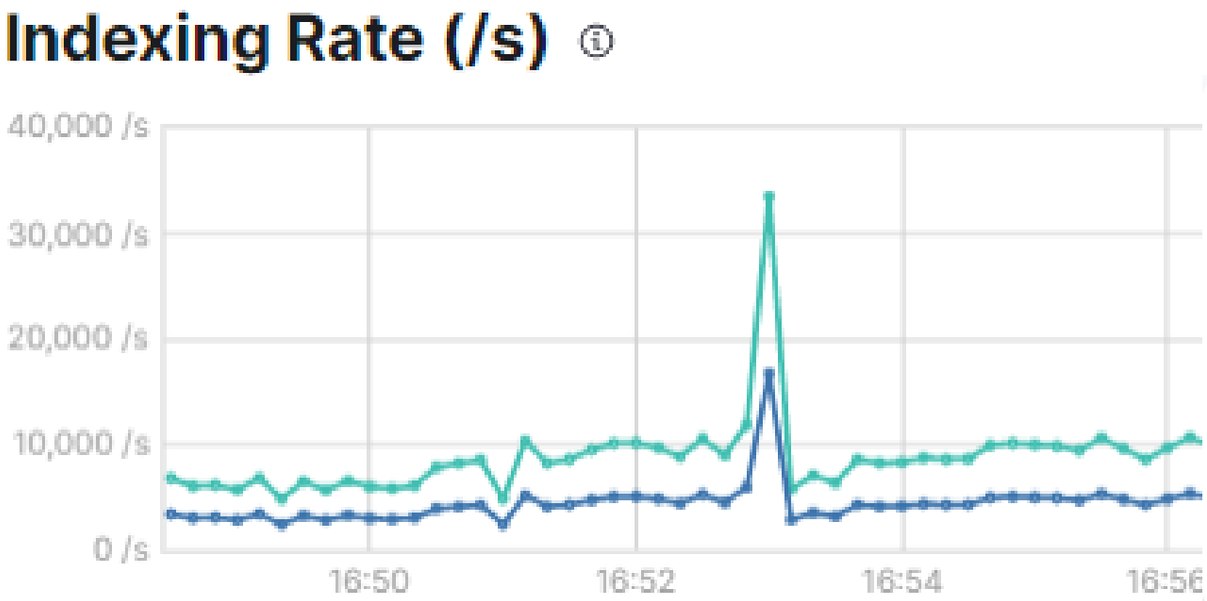


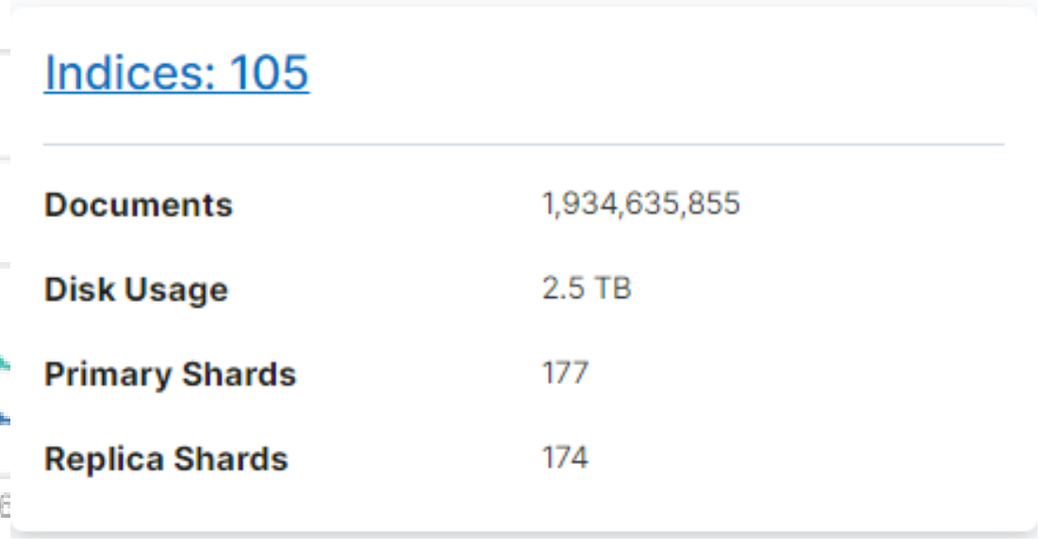


Cosa abbiamo usato e perché

Avendo un unico centro stella la cattura del traffico con porta di mirror è «semplice».

L'ingest su Elastisearch ha permesso di aumentare la raccolta di dati prodotti da Bro/Zeek & C.





Mantengo dati come vlan, etc che permettono rapidamente di «filtrare» la ricerca e l'analisi;

Dove siamo arrivati

Utilizzato SNMP e sFlow/NetFlow in ogni contesto applicabile, non c'è molto da aggiungere salvo che ha un onere di gestione e manutenzione;

Abbiamo raggiunto alto livello di successo nella verifica e controllo Operation, meno nella segnalazione Security.

Abbiamo più GUI ma non abbiamo intenzione di sviluppare, non è il nostro lavoro...

Dove siamo arrivati

Con Elasticsearch configurazioni e architettura sono “magia nera”; se devi cambiare qualcosa può capitare di ripartire da zero ….

Sconsigliati investimenti in integrazione perché sviluppo oggi ma domani se c’è un problema devo ripartire.

Ho una base dati formidabile ma la ricerca è ancora complessa.

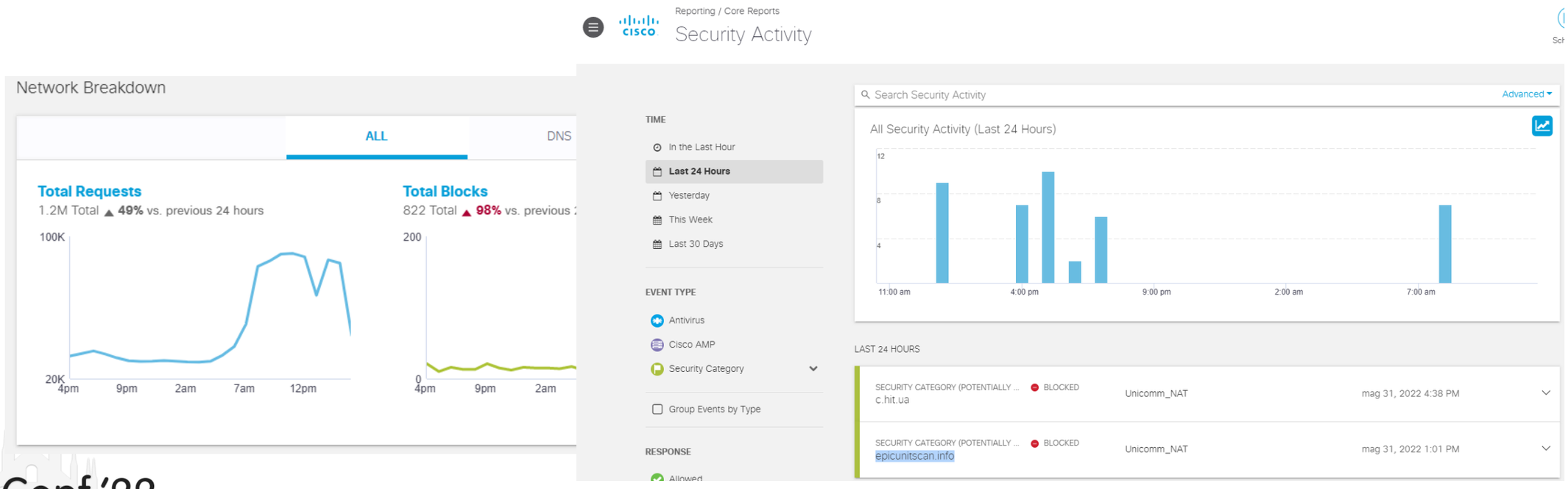
Esempio 1 – Cisco Umbrella

Accesso diretto a Internet limitatissimo, navigazione via proxy autenticato, posta elettronica ragionevolmente in sicurezza (solo italiano..)

-> se impedisco di arrivare al contenuto pericoloso che dovesse raggiungere il client mi evito alla radice problemi.

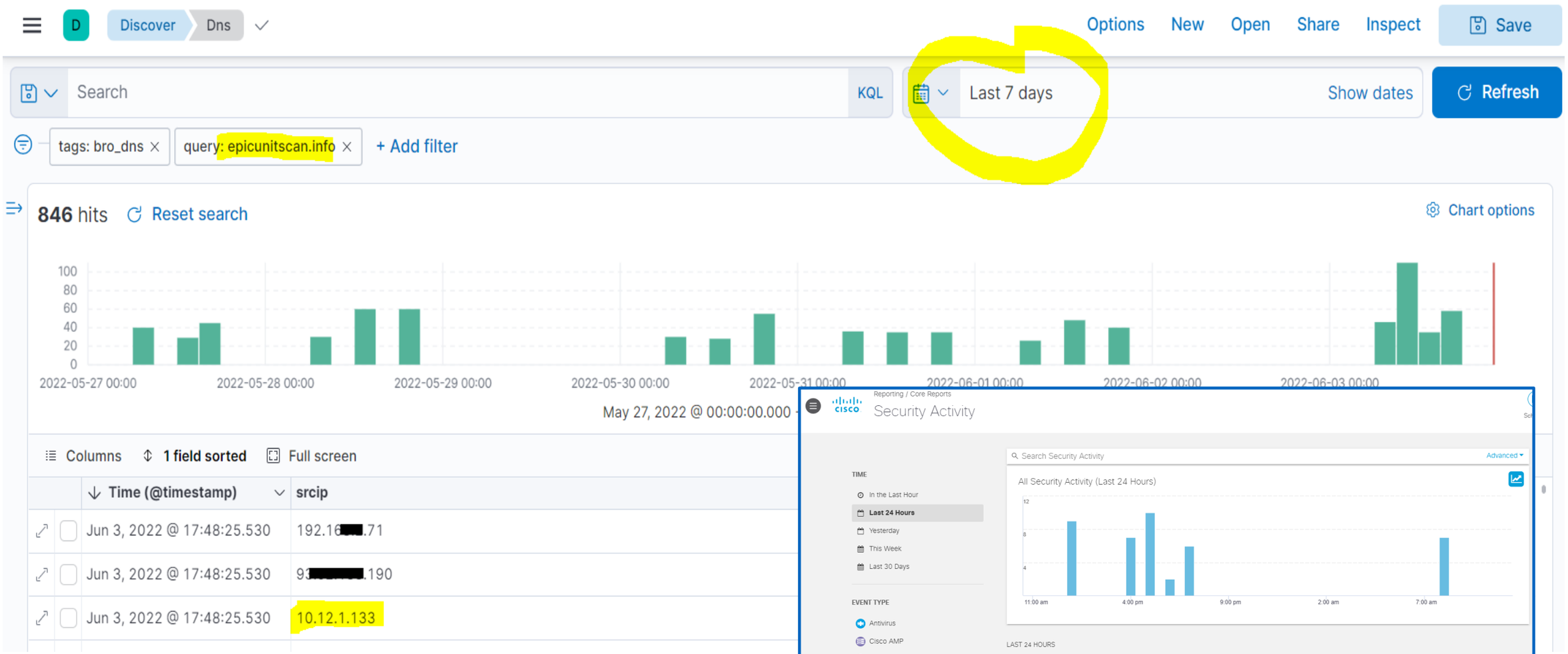
Il DNS limita il pericolo ma devo sapere chi aveva fatto la query

Serve uno strumento che raccolga le richieste DNS per ricostruire la catena DNS Cisco <> server DNS interni <> Client



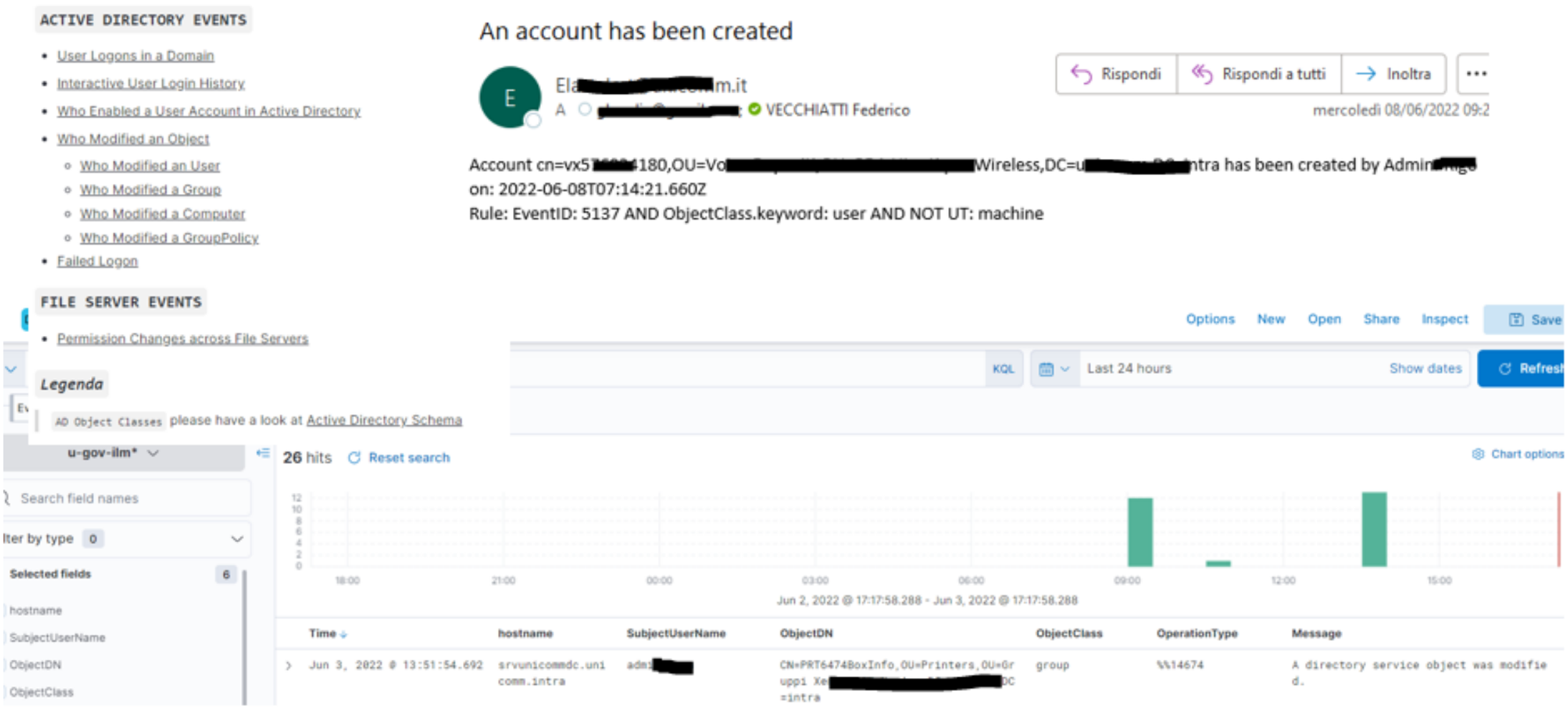
Esempio 1 – Cisco Umbrella

Con una semplice query (automatizzabile) risalgo alla catena di richiesta DNS e al client sorgente.



Esempio 2 - Log

Riusciamo a trovare l'informazione che interessa anche per altri ambiti come il controllo GDPR per il DPO, accessi VPN, autenticazione, etc anche con alerting.



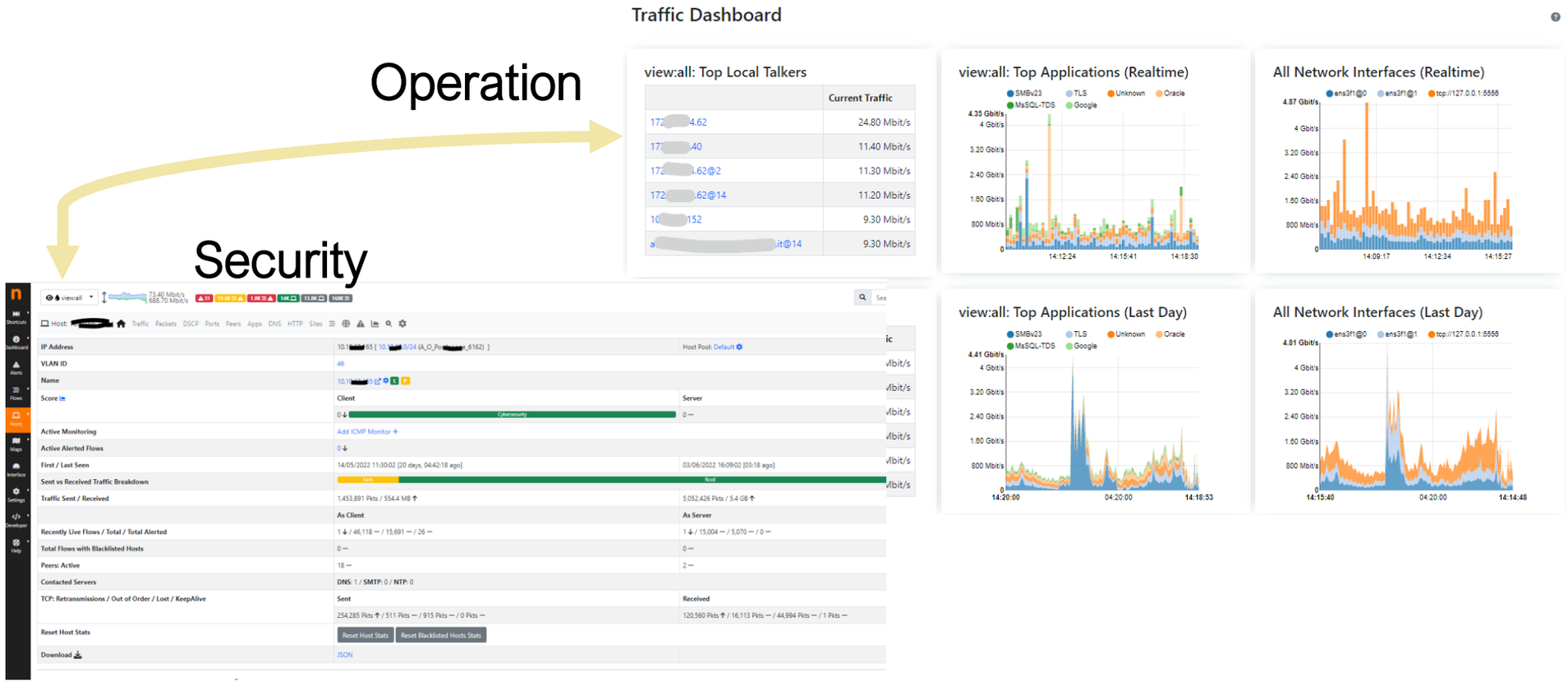
Si può fare meglio ?

Sicuramente ma c'è un problema di costi e ma non è detto che non si possa imparare …

Ntopng può essere il prodotto che risponde alle esigenze di centralizzazione del monitoraggio.

Quindi ntopng

La sfida è duplice per ntopng che si pone sia come strumento di Operation che di Security.

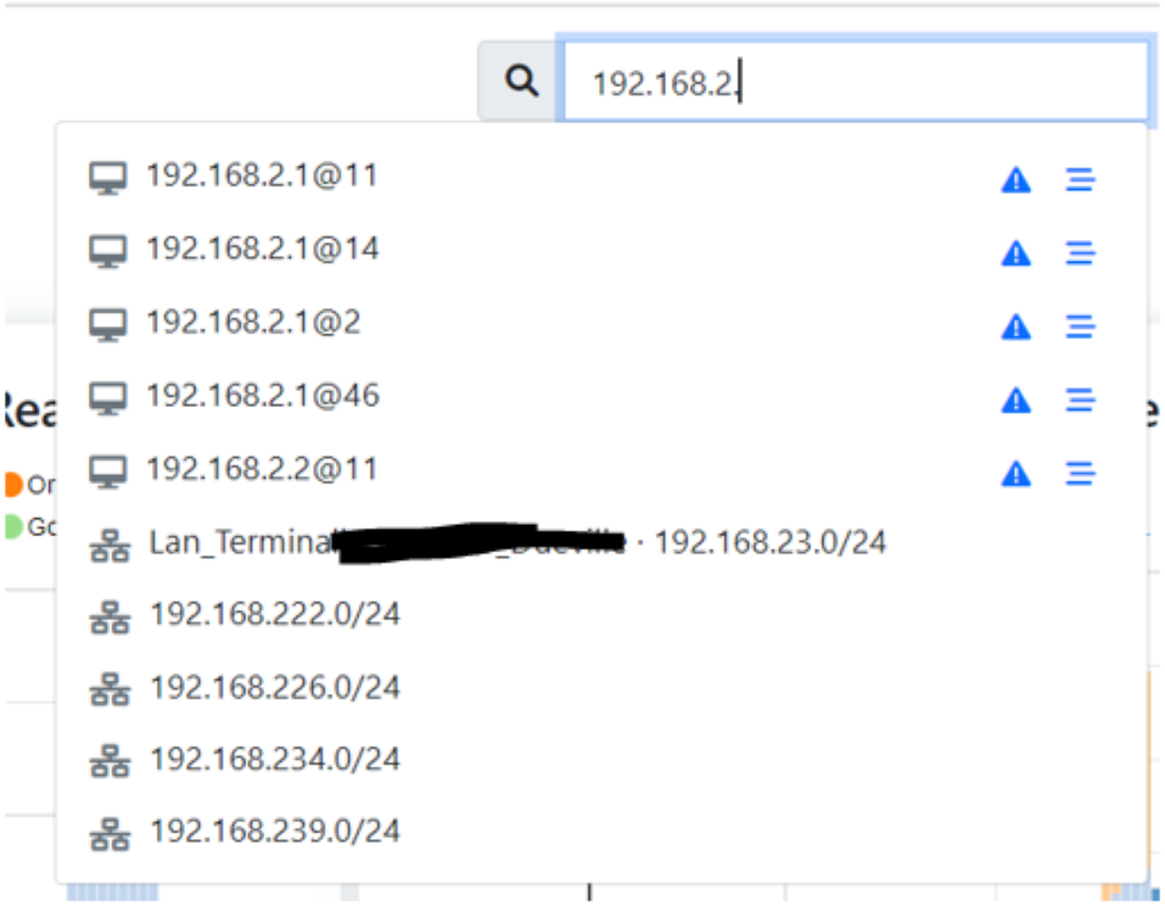


C'è il rischio di cambiare contesto e perdere l'analisi che si sta facendo.

Ntopng: la ricerca

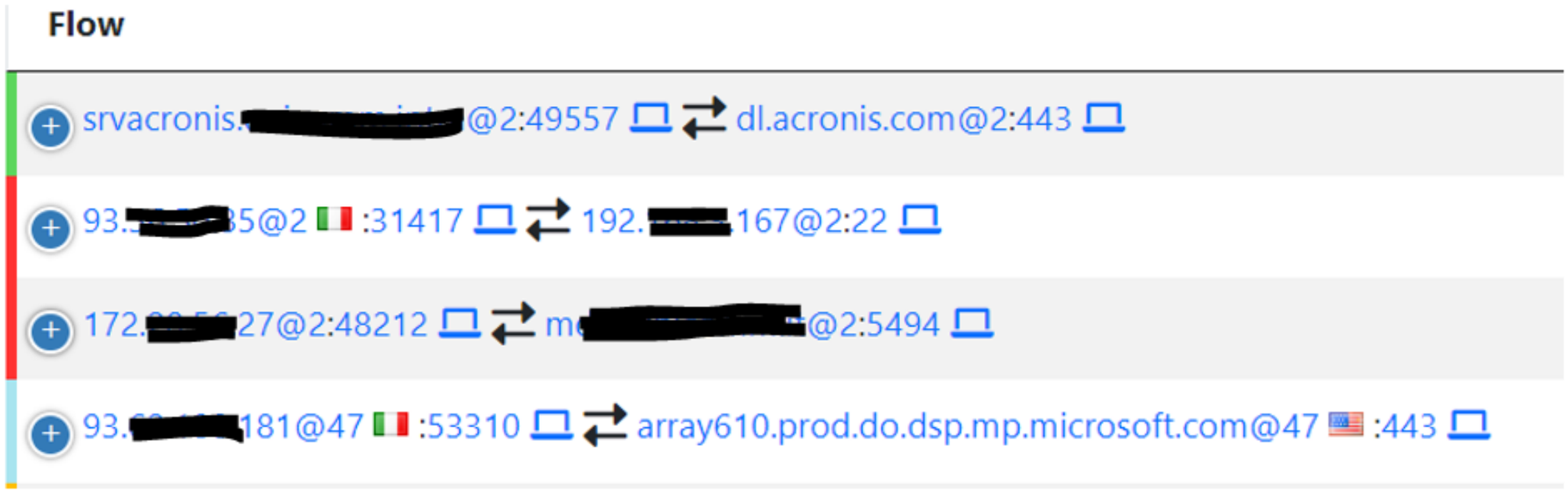
Con il team ntopng individuati dei punti di attenzione:

- *Migliorare la ricerca supportando le network e le VLAN*



Ntopng: il DNS

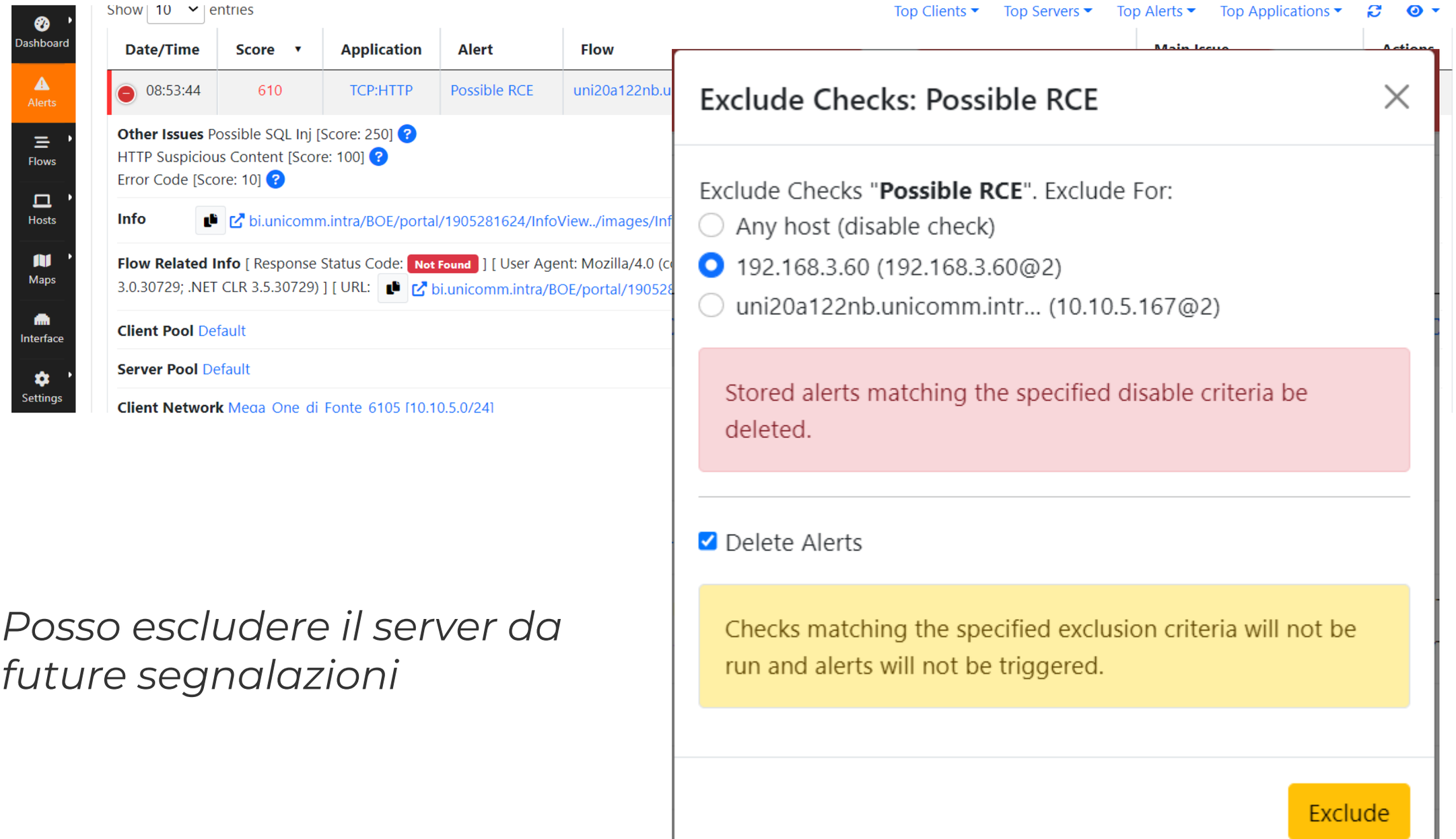
- *Curato la risoluzione DNS per evitare di associare a IP nomi DNS errati (proxy, IP pubblici)*



Evito falsi allarmi e allarmismi ...

Ntopng: alerting

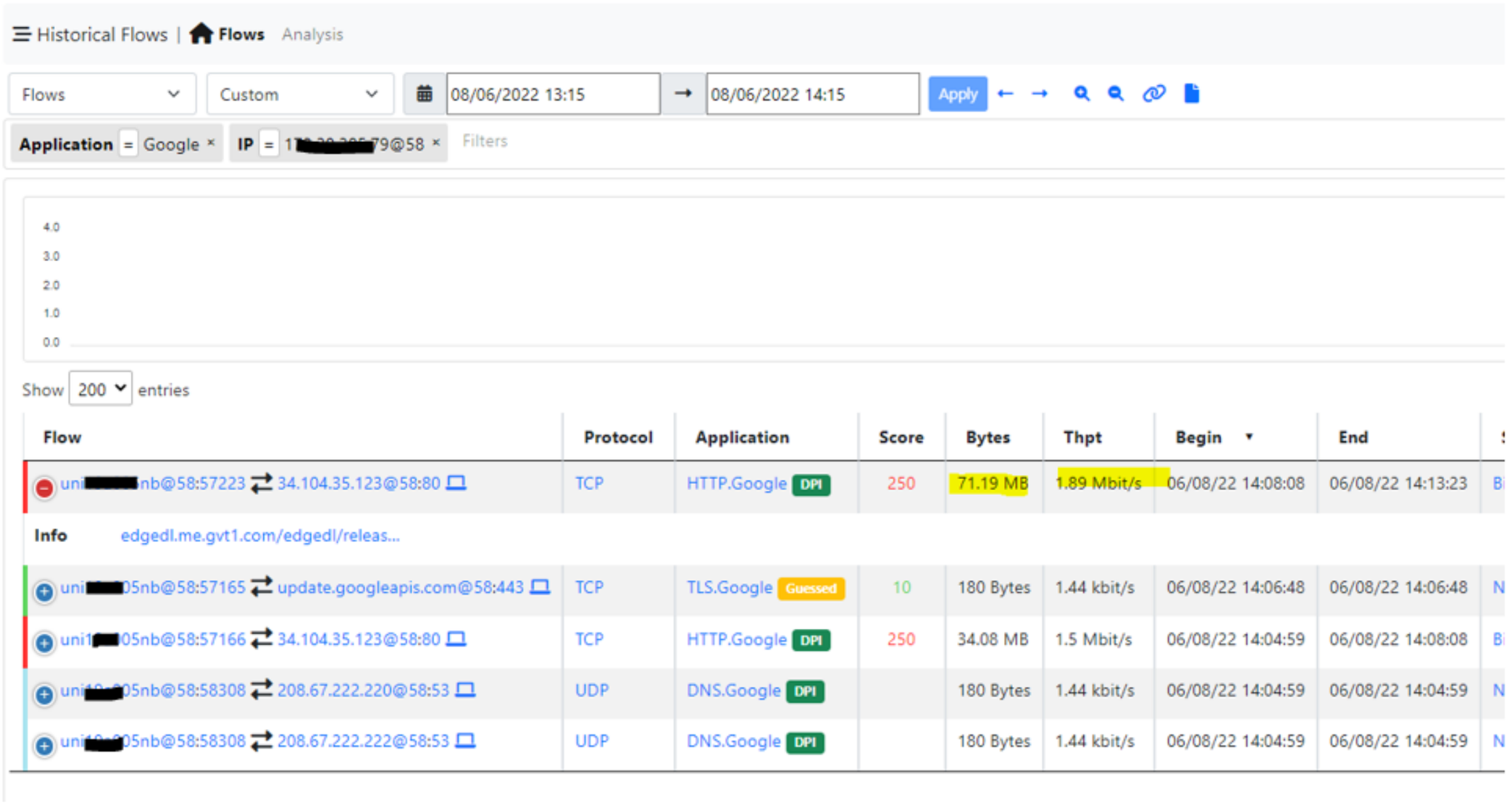
- *Lavoro su Alert e sulla possibilità di filtrare*



Posso escludere il server da future segnalazioni

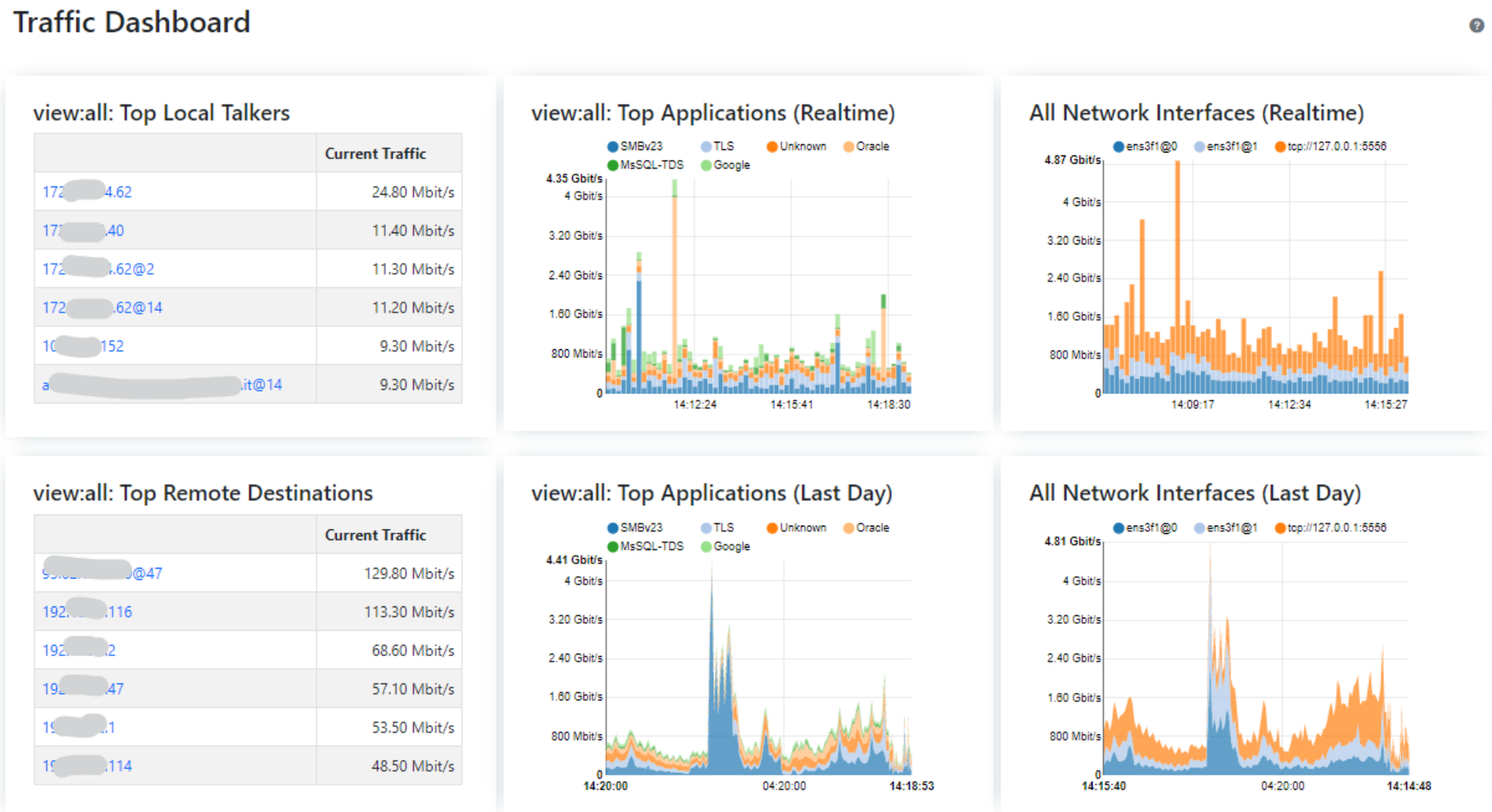
Ntopng: info

- *Esposizione di informazioni pertinenti all'indagine*



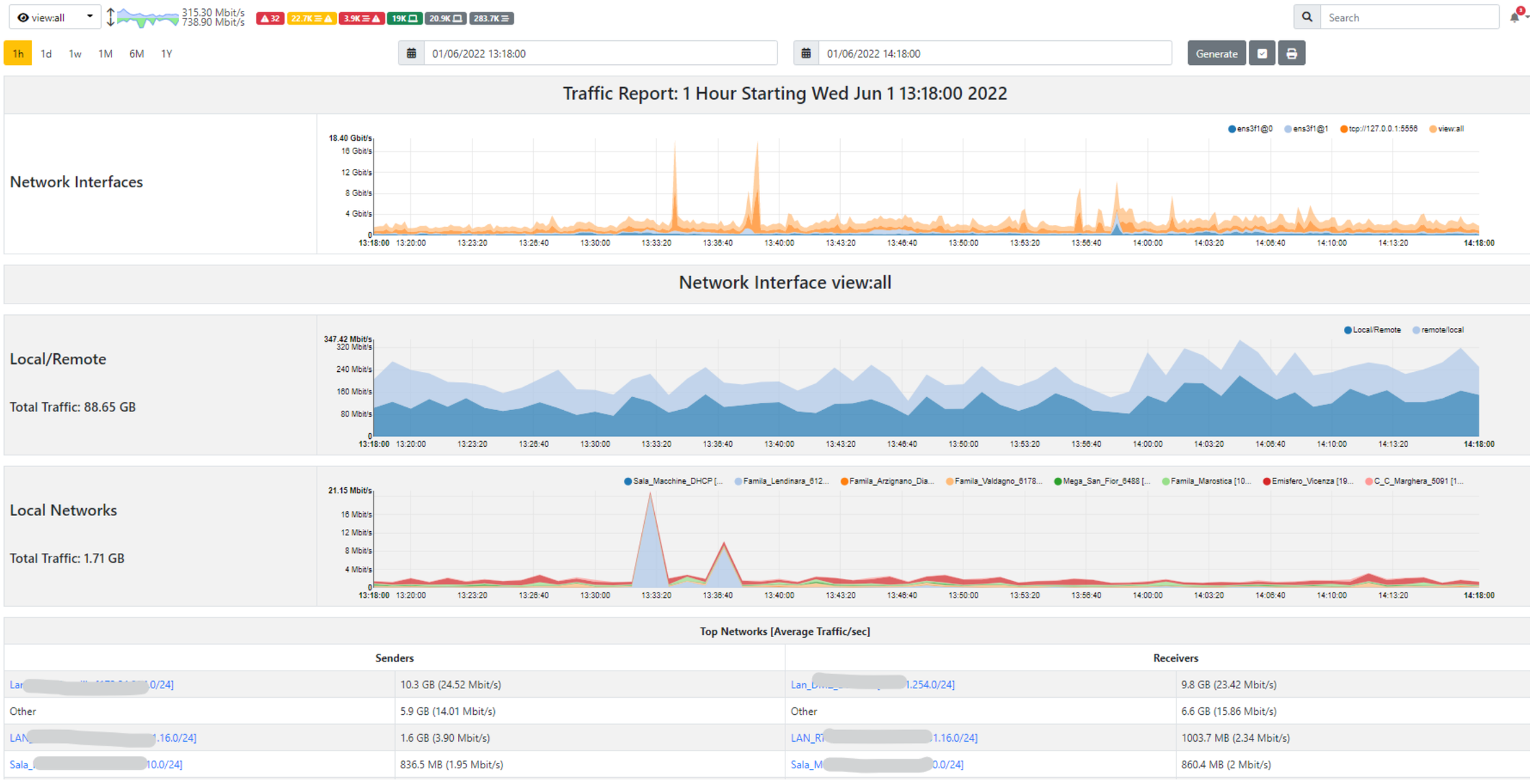
Ntopng per Operation

La Traffic Dashboard è perfetta per Operation perché è in real time. Ma io arriverò sempre qualche istante dopo, serve la storia o almeno un range temporale …



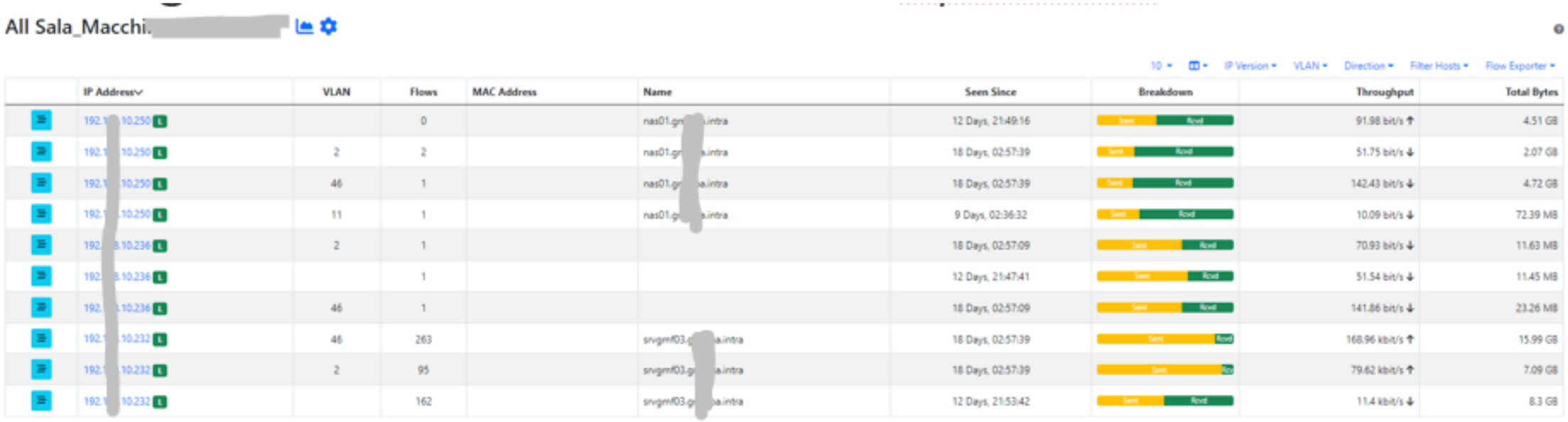
Ntopng per Operation

Quindi abbiamo lavorato sul report storico.



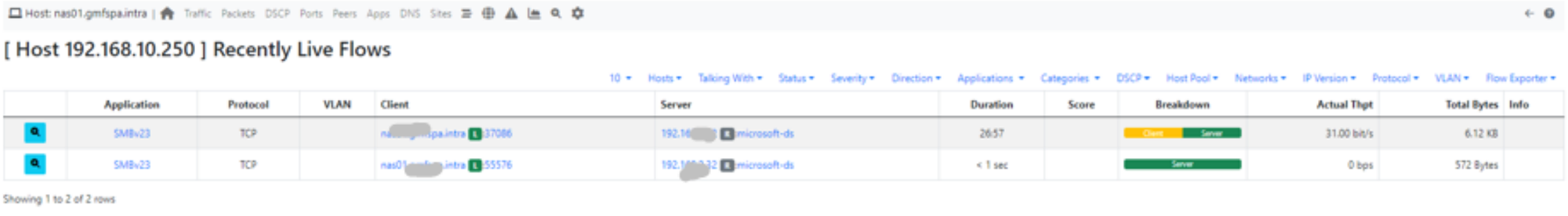
Ntopng per Operation

Analizzando il traffico di una rete indicata nel report rimango ad una vista che è ancora Operation.



	IP Address	VLAN	Flows	MAC Address	Name	Seen Since	Breakdown	Throughput	Total Bytes
	192.1 .10.250 L		0		nas01.gm .intra	12 Days, 21:49:16	Sent Rcvd	91.98 bit/s ↑	4.51 GB
	192.1 .10.250 L	2	2		nas01.gm .intra	18 Days, 02:57:39	Sent Rcvd	51.75 bit/s ↓	2.07 GB
	192.1 .10.250 L	46	1		nas01.gm .intra	18 Days, 02:57:39	Sent Rcvd	142.43 bit/s ↓	4.72 GB
	192.1 .10.250 L	11	1		nas01.gm .intra	9 Days, 02:36:32	Sent Rcvd	10.09 bit/s ↓	72.39 MB
	192. .10.236 L	2	1			18 Days, 02:57:09	Sent Rcvd	70.93 bit/s ↓	11.63 MB
	192. .10.236 L		1			12 Days, 21:47:41	Sent Rcvd	51.54 bit/s ↓	11.45 MB
	192. .10.236 L	46	1			18 Days, 02:57:09	Sent Rcvd	141.86 bit/s ↓	23.26 MB
	192. .10.232 L	46	263		srvgmf03.g .intra	18 Days, 02:57:39	Sent Rcvd	168.96 kbit/s ↑	15.99 GB
	192. .10.232 L	2	95		srvgmf03.g .intra	18 Days, 02:57:39	Sent Rcvd	79.62 kbit/s ↑	7.09 GB
	192. .10.232 L		162		srvgmf03.g .intra	12 Days, 21:53:42	Sent Rcvd	11.4 kbit/s ↓	8.3 GB

Rimango sempre in un contesto di Operation, anche se "esplodo" un host per vedere i suoi peers.

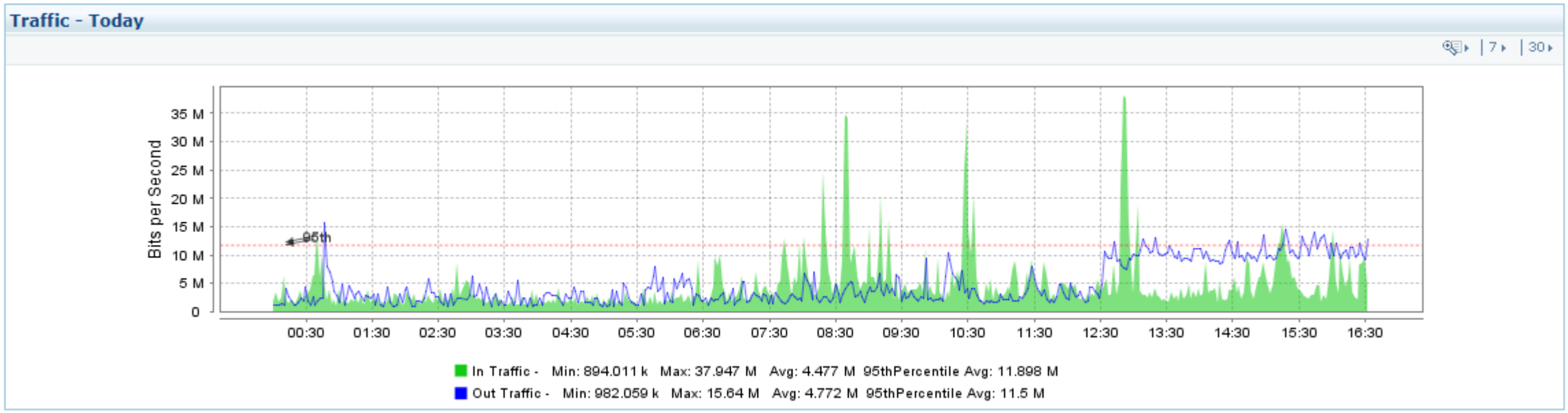


	Application	Protocol	VLAN	Client	Server	Duration	Score	Breakdown	Actual Thpt	Total Bytes	Info
	SMBv23	TCP		.intra L 37086	192.16 .microsoft-ds	26:57		Client Server	31.00 bit/s	6.12 KB	
	SMBv23	TCP		nas01. .intra L 55576	192.168.0.32 .microsoft-ds	< 1 sec		Server	0 bps	572 Bytes	

Ma funziona ?

«Il monitoraggio almeno nella nostra realtà è in equilibrio tra Operation e Security»

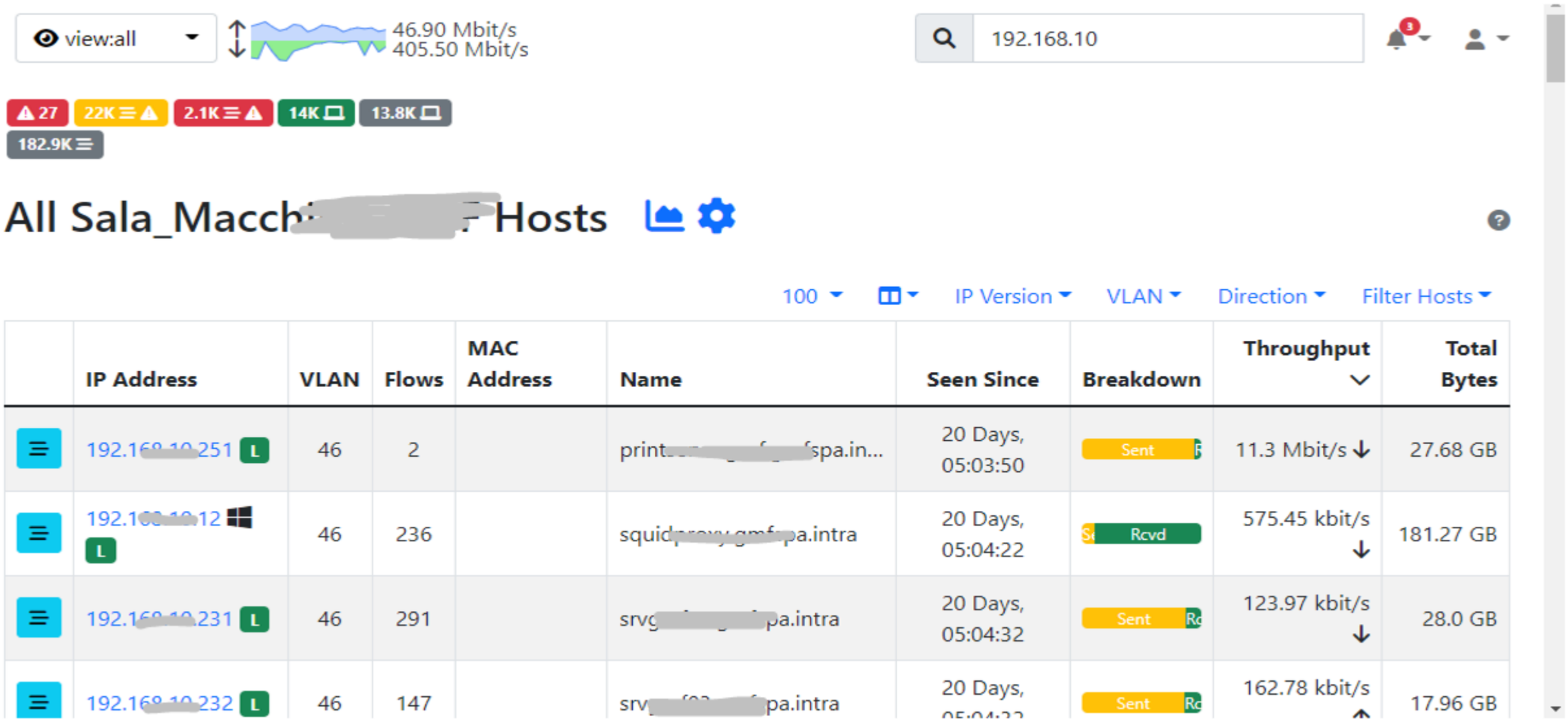
Esempio: c'è decisamente una anomalia in un router periferico.



Ho tutte le informazioni su rete, sede, etc. quindi posso condurre l'analisi.

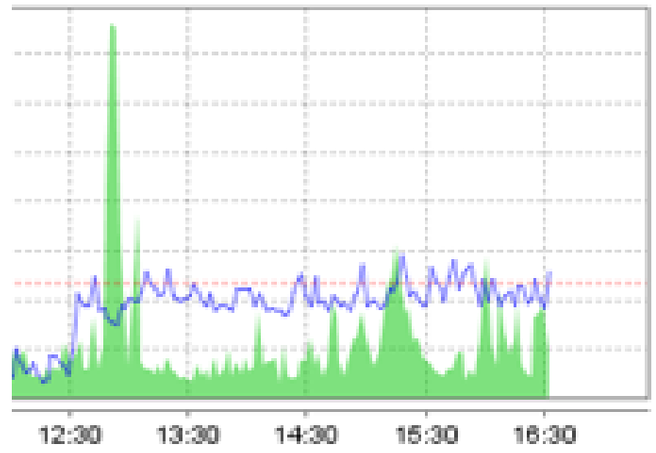
Ma funziona ?

Con la possibilità di filtrare per reti rapidamente trovo l'host con traffico anomalo.



. . .

La scheda host del server conferma ...



E i flow recenti mi dicono chi sono i peer coinvolti

[Host 192.168.10.251@46] Recently Live Flows

100 ▾ Hosts ▾ Talking With ▾ Status ▾ Severity ▾ Direction ▾ Applications ▾ Categories ▾ DSCP ▾ Host Pool ▾ Networks ▾ IP Version ▾

	Application	Protocol	VLAN	Client	Server	Duration	Score	Breakdown	Actual Thpt	Total Bytes	Ir
	NetBIOS.SMBv...	TCP	46	172.31.184.6 R :50276	192.168.10.251 L :microsoft-ds	41:46	10	Server	7.10 Mbit/s ↓	4.31 GB ↑	
	TLS	TCP	46	172.31.184.6 R :50418	192.168.10.251 L :62920	15:58		Client Server	12.00 kbit/s —	2.39 MB ↑	
	TLS	TCP	46	172.31.184.6 R :50739	192.168.10.251 L :62920	00:19 sec		Client Server	0 bps —	93.02 KB —	

Risultato

Si tratta di un utente in VPN, posso risalire al login, etc ..

E quale era il problema ?

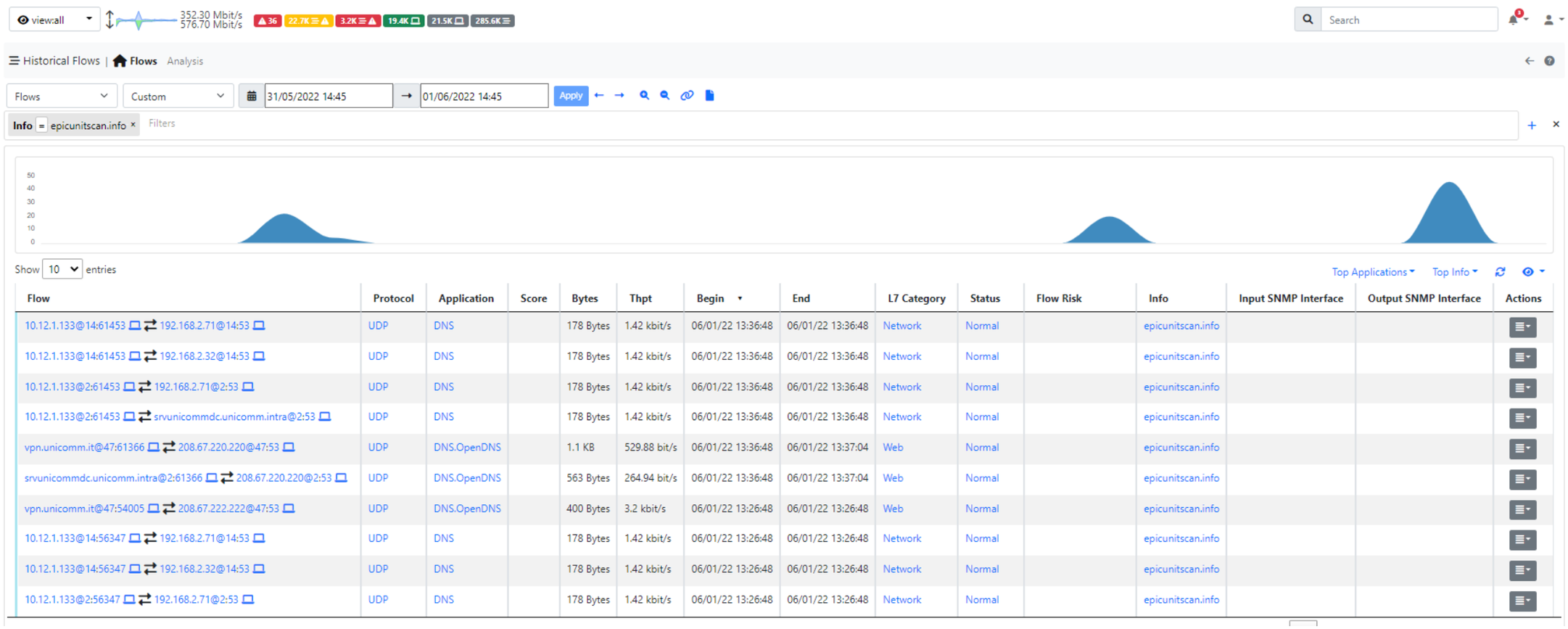
Un collega (ex ?) si stava «recuperando» un po' di storia personale copiandosi qualche giga di files ...

Operation e Security in una rete «nota» si incontrano spesso.

E' questa la ricerca che stiamo facendo, avere lo strumento che integri Operation e Security in modo agevole permettendo navigazione nei due contesti in modo coerente e ntopng ci sta accompagnando in questo percorso.

L’esempio del DNS

Facile …



Flow	Protocol	Application	Score	Bytes	Thpt	Begin	End	L7 Category	Status	Flow Risk	Info	Input SNMP Interface	Output SNMP Interface	Actions
10.12.1.133@14:61453 ⇄ 192.168.2.71@14:53	UDP	DNS		178 Bytes	1.42 kbit/s	06/01/22 13:36:48	06/01/22 13:36:48	Network	Normal		epicunitscan.info			
10.12.1.133@14:61453 ⇄ 192.168.2.32@14:53	UDP	DNS		178 Bytes	1.42 kbit/s	06/01/22 13:36:48	06/01/22 13:36:48	Network	Normal		epicunitscan.info			
10.12.1.133@2:61453 ⇄ 192.168.2.71@2:53	UDP	DNS		178 Bytes	1.42 kbit/s	06/01/22 13:36:48	06/01/22 13:36:48	Network	Normal		epicunitscan.info			
10.12.1.133@2:61453 ⇄ srvunicommdc.unicomm.intra@2:53	UDP	DNS		178 Bytes	1.42 kbit/s	06/01/22 13:36:48	06/01/22 13:36:48	Network	Normal		epicunitscan.info			
vpn.unicomm.it@47:61366 ⇄ 208.67.220.220@47:53	UDP	DNS.OpenDNS		1.1 KB	529.88 bit/s	06/01/22 13:36:48	06/01/22 13:37:04	Web	Normal		epicunitscan.info			
srvunicommdc.unicomm.intra@2:61366 ⇄ 208.67.220.220@2:53	UDP	DNS.OpenDNS		563 Bytes	264.94 bit/s	06/01/22 13:36:48	06/01/22 13:37:04	Web	Normal		epicunitscan.info			
vpn.unicomm.it@47:54005 ⇄ 208.67.222.222@47:53	UDP	DNS.OpenDNS		400 Bytes	3.2 kbit/s	06/01/22 13:26:48	06/01/22 13:26:48	Web	Normal		epicunitscan.info			
10.12.1.133@14:56347 ⇄ 192.168.2.71@14:53	UDP	DNS		178 Bytes	1.42 kbit/s	06/01/22 13:26:48	06/01/22 13:26:48	Network	Normal		epicunitscan.info			
10.12.1.133@14:56347 ⇄ 192.168.2.32@14:53	UDP	DNS		178 Bytes	1.42 kbit/s	06/01/22 13:26:48	06/01/22 13:26:48	Network	Normal		epicunitscan.info			
10.12.1.133@2:56347 ⇄ 192.168.2.71@2:53	UDP	DNS		178 Bytes	1.42 kbit/s	06/01/22 13:26:48	06/01/22 13:26:48	Network	Normal		epicunitscan.info			

L’informazione fornita da Ntopng è disponibile in un contesto di informazioni più complete e ricche da cui l’analisi può procedere molto più velocemente anche per personale non «formato».

Next step

Il team ntopng sta aggiungendo funzionalità rapidamente;

Dopo un periodo di test ntopng viene introdotto per lo specifico monitoraggio al posto delle soluzioni custom;

Cercare di aumentare la qualità delle segnalazioni Security con una «baseline» o simile per non dover ripetere le analisi;

Poter classificare gli Alert in base a criteri diversi da source e destination (es URL, etc)

Grazie !