BLS CONSULTING
Consulenza e sviluppo informatico

Traffic Analyzer

Tutto il traffico di rete sotto controllo

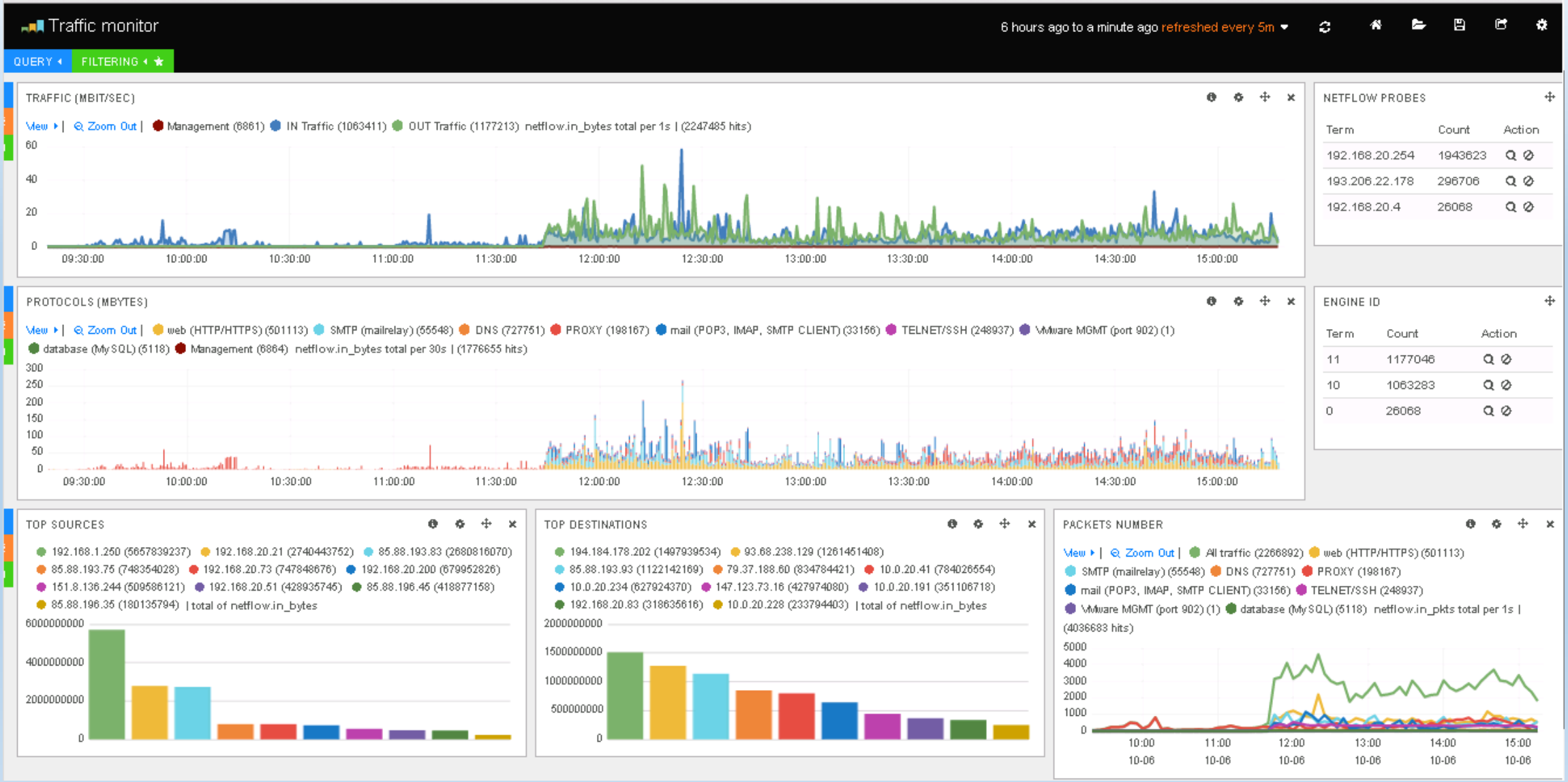
B.L.S. Consulting s.r.l. – www.bls.it **Tel. 0382/413825** **Mail: commerciale@bls.it**

L’appliance per il Traffic Analysis di BLS è uno strumento semplice e innovativo per monitorare il traffico della propria Rete.

Una volta collegata la sonda, il traffico viene immediatamente reso visibile sull’interfaccia grafica.

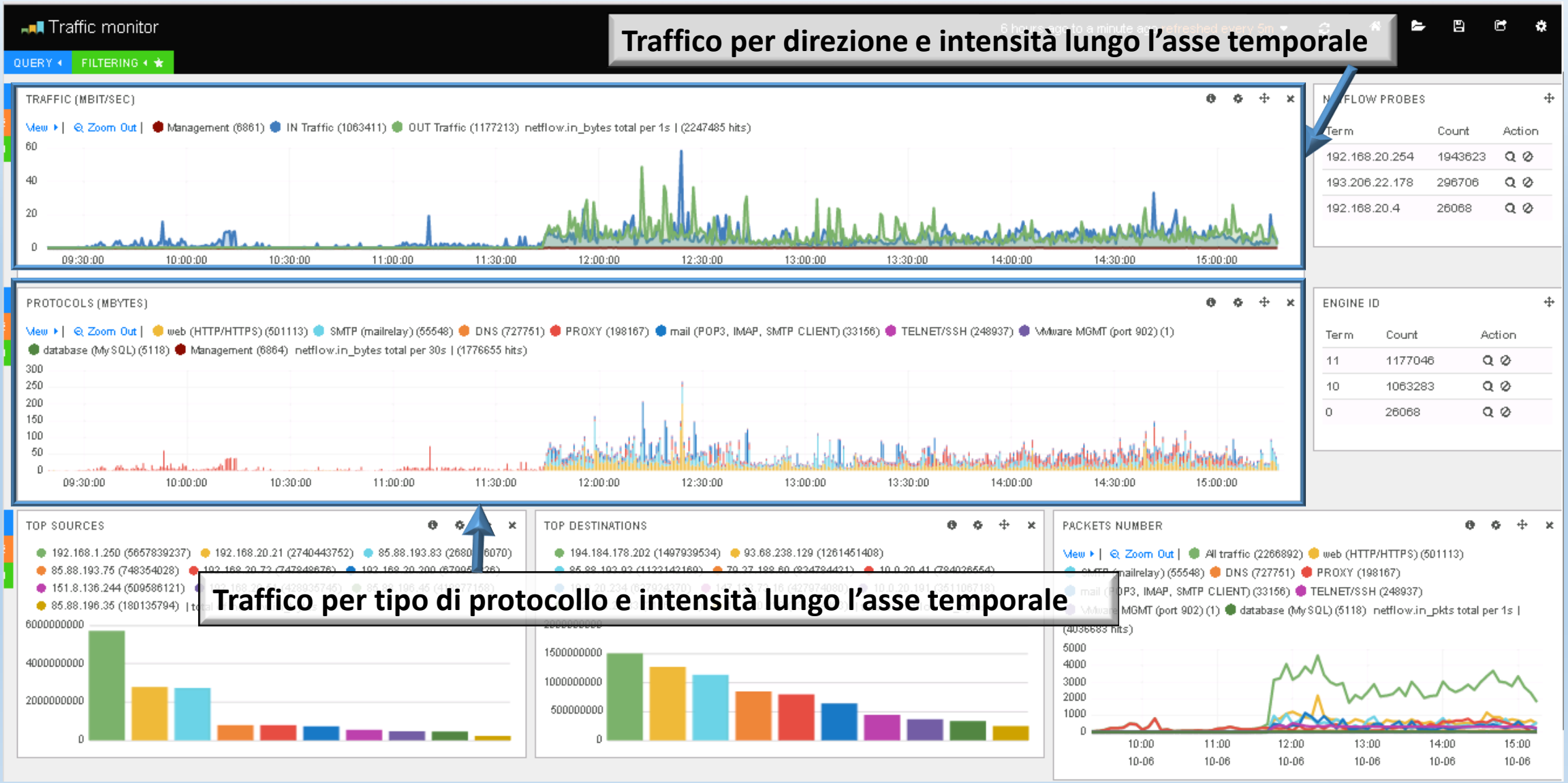
L’interfaccia grafica è molto intuitiva, permette di ottenere con pochi clic e a colpo d’occhio le informazioni ricercate.

Dashboard Principale

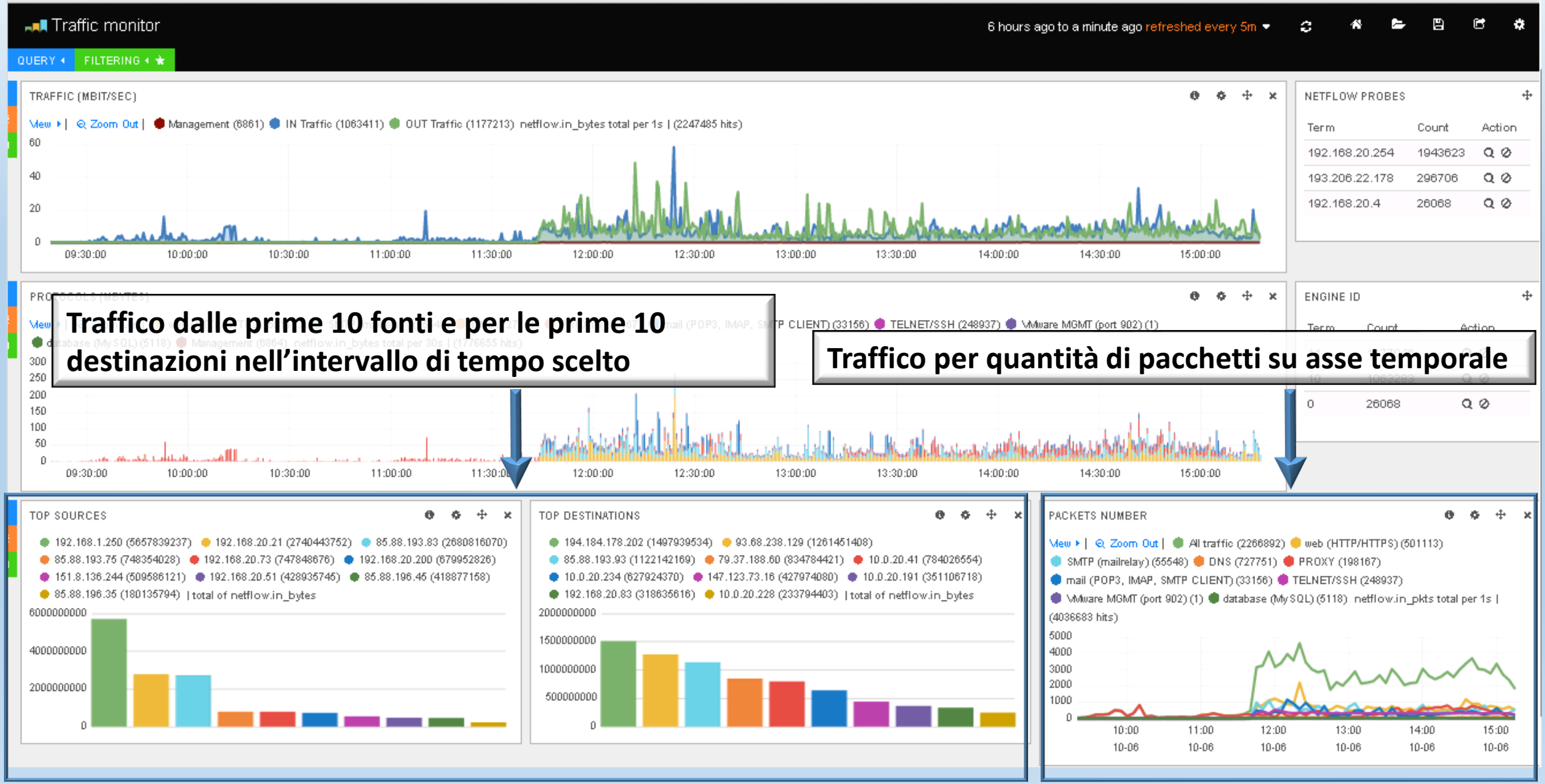


Dashboard Principale

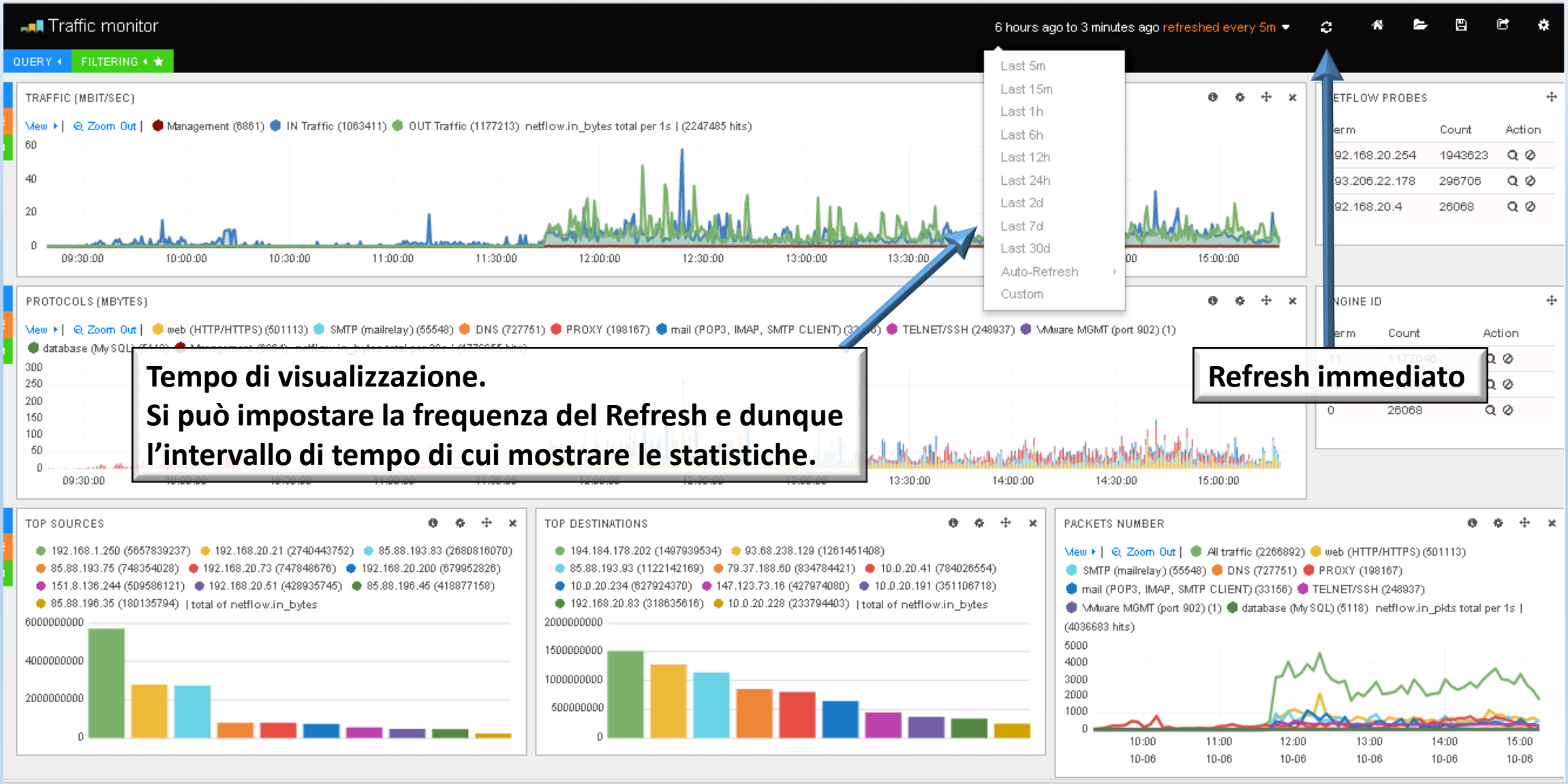
Dashboard Principale



Dashboard Principale

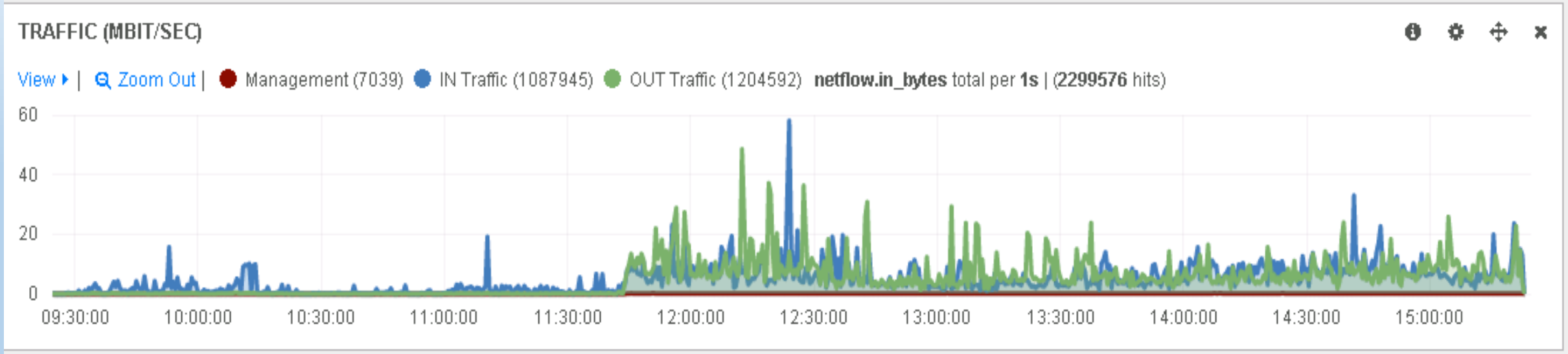


Dashboard Principale



Dashboard Principale

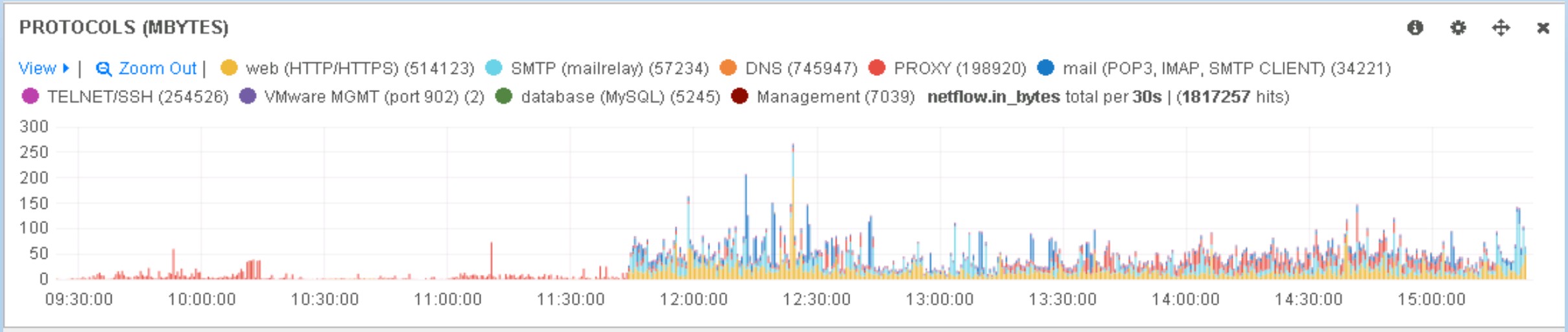
Dettaglio del traffico in entrata e in uscita nel periodo richiesto



Il traffico di Management è quello prodotto dal TA per gestire i dati.
Come si può notare, è incommensurabilmente piccolo rispetto al traffico analizzato.

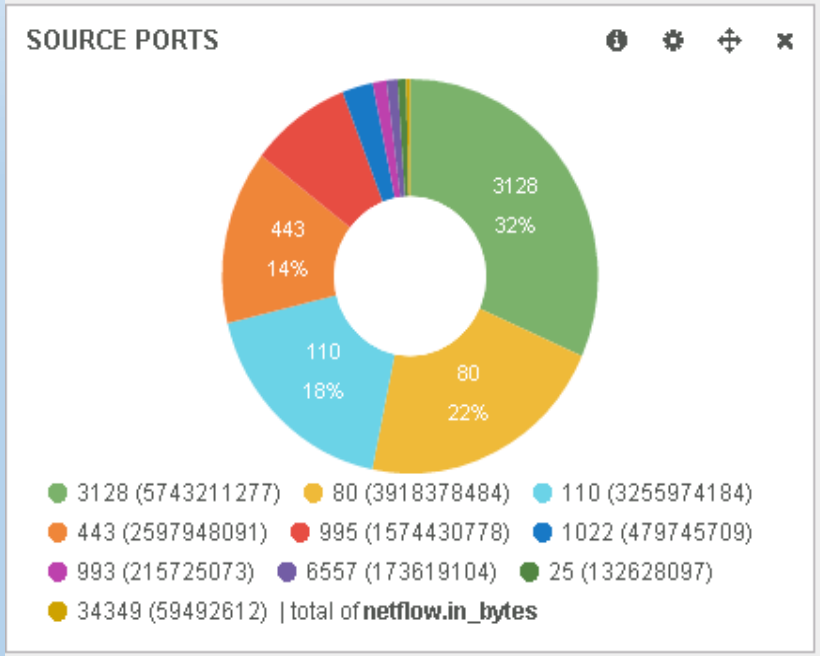
Dashboard Principale

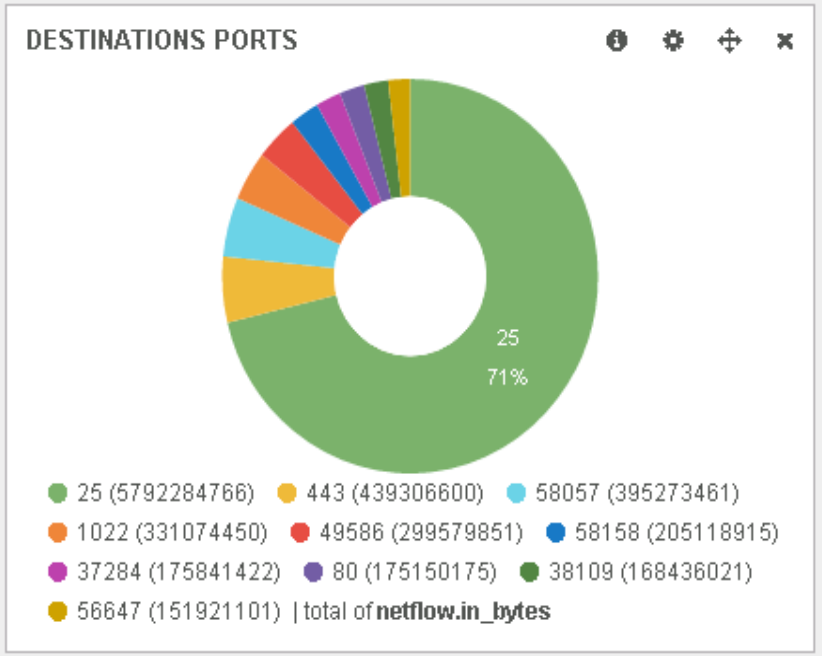
Dettaglio del traffico per tipologia di protocollo

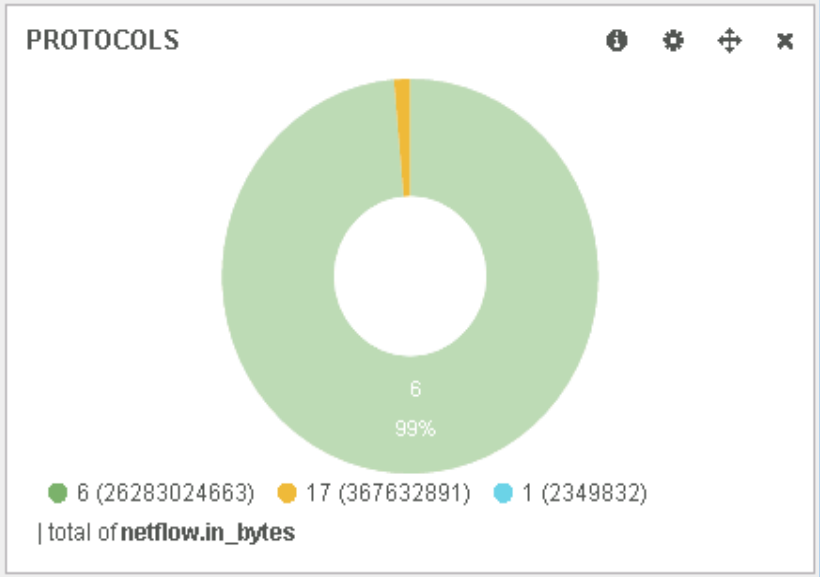


Dashboard Principale

Dettaglio del traffico per porta d'entrata ed uscita

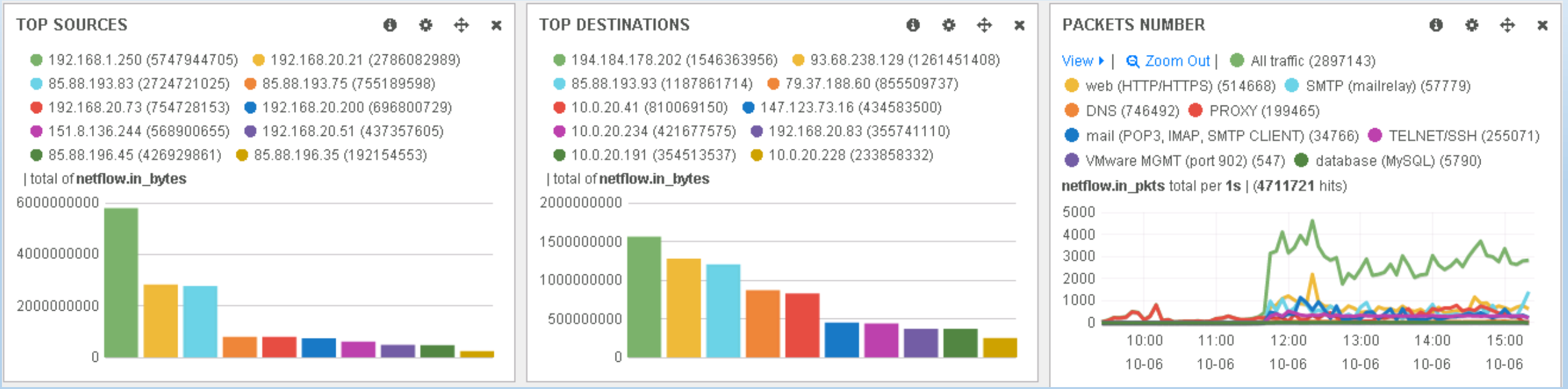






Dashboard Principale

Dettaglio del traffico per fonte e destinazione e quantità di pacchetti nel tempo

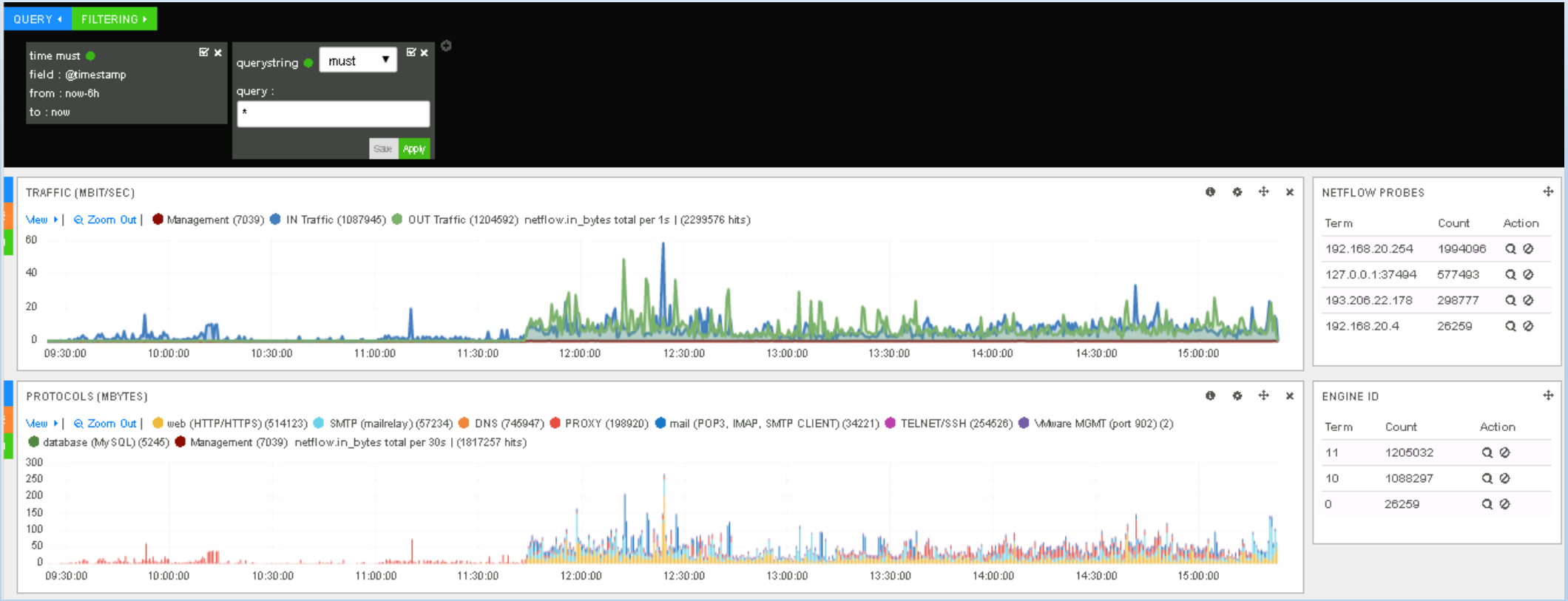


Con questa visualizzazione è già possibile, senza necessità di Queries più approfondite, individuare le principali fonti e destinazioni di traffico.

Immaginiamo che la nostra rete rallenti improvvisamente.
Con questa schermata è possibile vedere immediatamente quale macchina sta occupando la connessione disponibile e per quale tipo di traffico.

Funzioni

Visualizzazione filtri

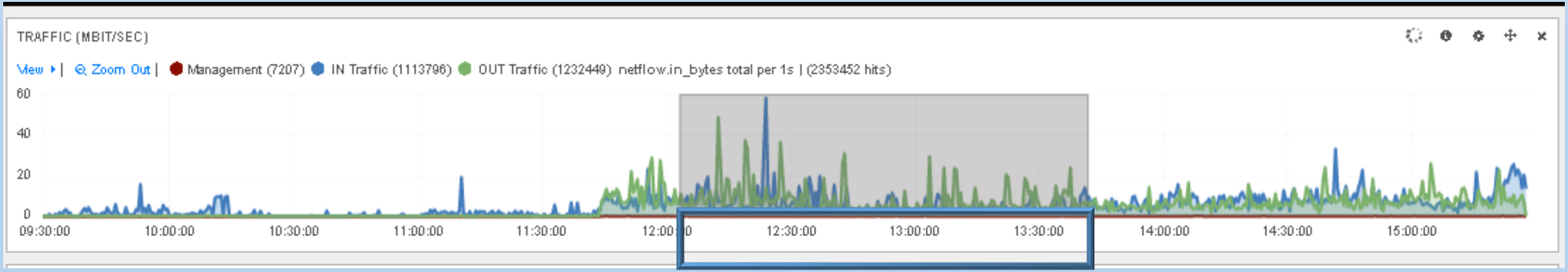


Cliccando il tasto Filtering appaiono i filtri impostati, che si possono immediatamente cancellare o modificare.

Funzioni

Filtraggio per periodo

Una delle caratteristiche più innovative e comode del Traffic Analyzer BLS è la semplicità di impostazione dei filtri, che avviene su base grafica.



Per visualizzare in dettaglio l'andamento del traffico di un dato periodo, è sufficiente selezionarlo graficamente come indicato nell'immagine.

Gli altri grafici della schermata principale si aggiornano immediatamente, indicando i valori relativi a quel periodo

Funzioni

Filtraggio per periodo

Gli altri grafici della schermata principale si aggiornano immediatamente, indicando i valori relativi a quel periodo

Funzioni

Filtraggio per fonte

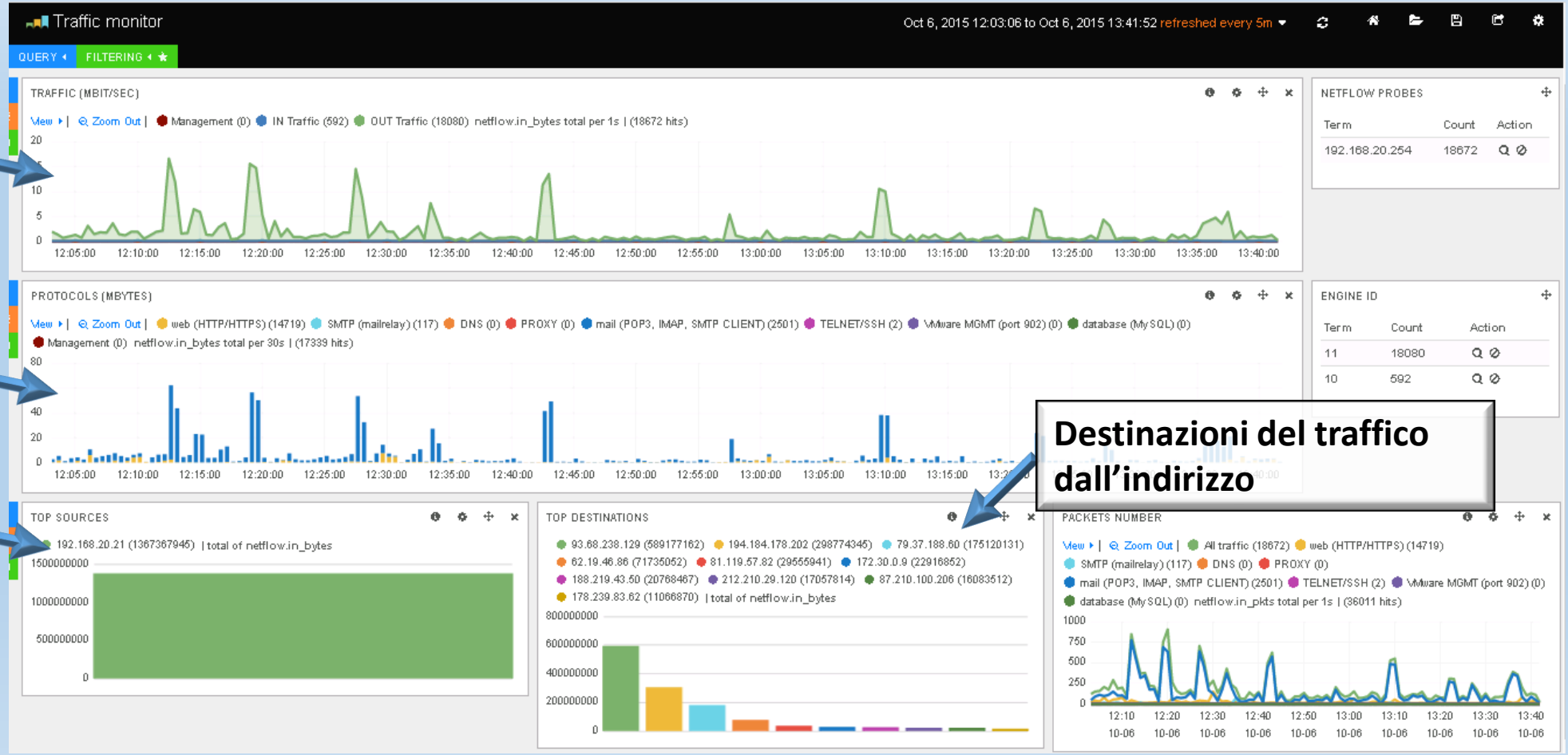
Selezionando Source possiamo individuare graficamente una serie di informazioni sul traffico proveniente da un indirizzo IP esterno

Quantità di traffico dall'indirizzo

Tipologia del traffico dall'indirizzo

Indirizzo selezionato

Destinazioni del traffico dall'indirizzo



Funzioni

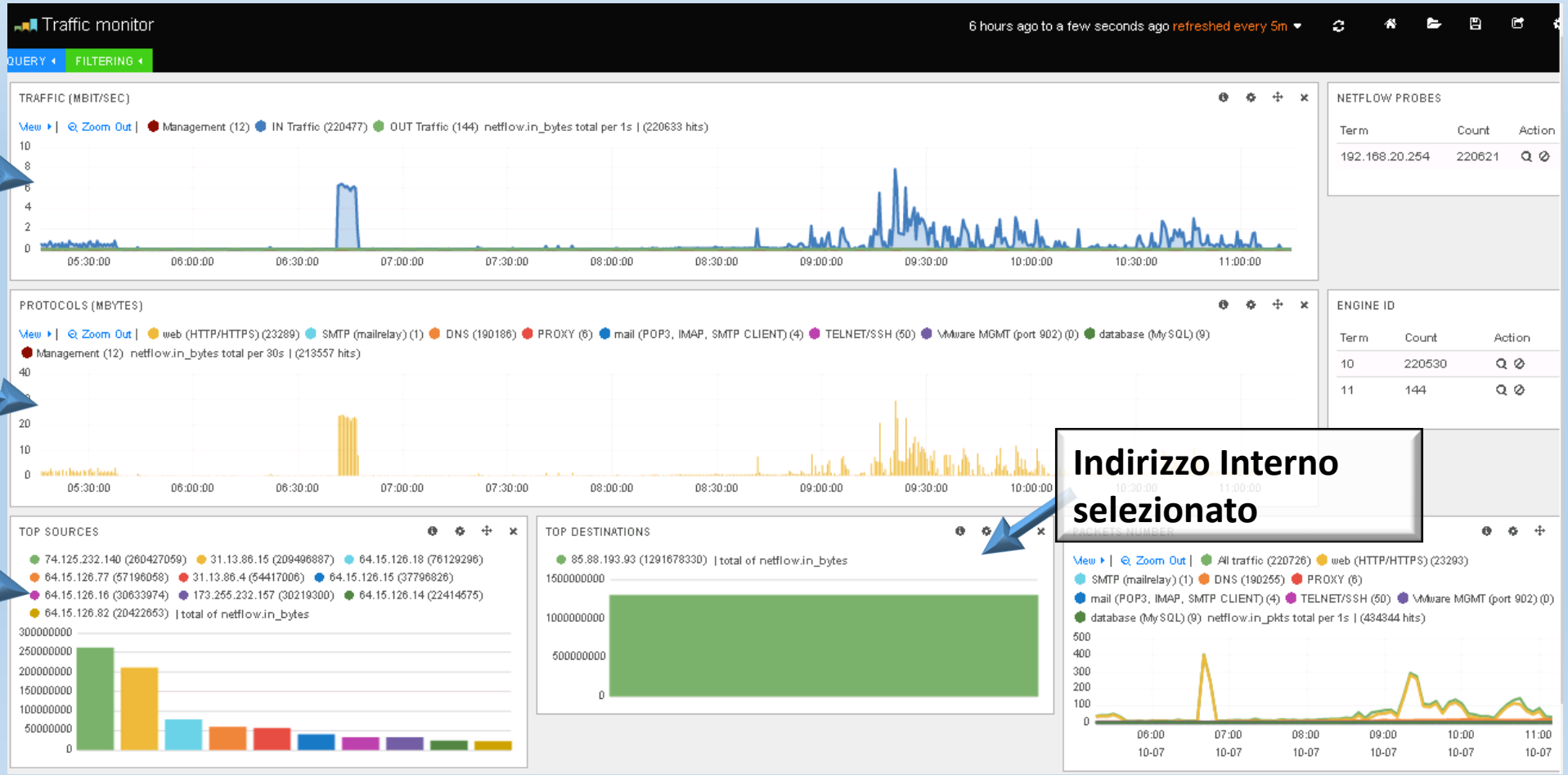
Filtraggio per Destinazione

Selezionando Destinations possiamo individuare graficamente una serie di informazioni sul traffico verso un indirizzo IP della nostra rete

Quantità di traffico verso l'indirizzo

Tipologia di traffico verso l'indirizzo

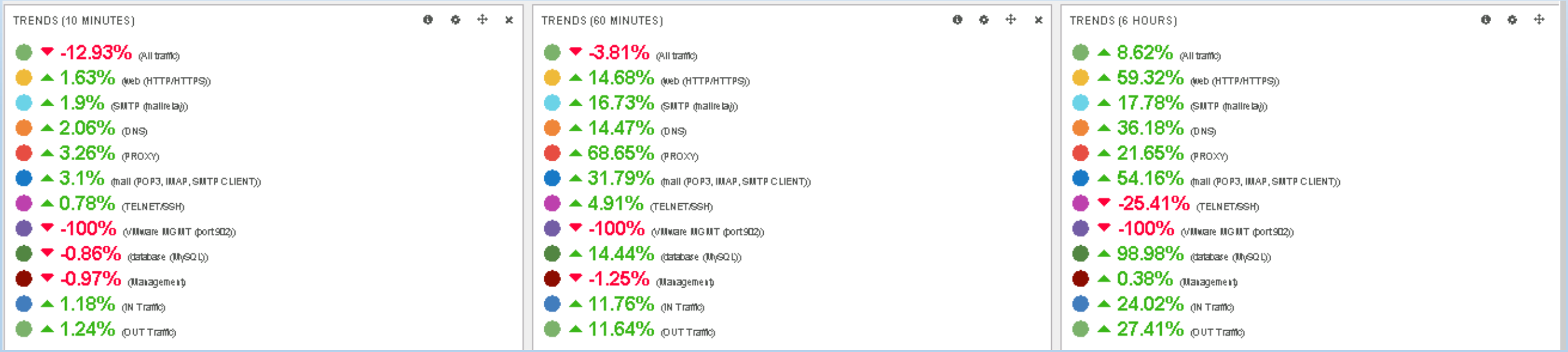
Origine del traffico verso l'indirizzo



Funzioni

Trends

Nella parte inferiore della Dashboard principale si può aprire la finestra dei Trends.



Questa ci fornisce le variazioni delle varie tipologie di traffico per vari intervalli temporali.

Funzioni

Flussi

Sempre nella parte inferiore della Dashboard principale si possono visualizzare i dettagli dei Flussi di traffico.

FLOWS

0 to **100** of 500 available for paging

netflow.last_switched	netflow.ipv4_src_addr	netflow.l4_src_port	netflow.ipv4_dst_addr	netflow.l4_dst_port	netflow.in_bytes	netflow.in_pkts	netflow.protocol	host	netflow.engine_id
2015-10-09T09:07:04.000Z	192.168.1.250	3128	10.0.20.36	50606	75472930	30054	6	193.206.22.178	10
2015-10-09T06:53:51.130Z	192.168.20.76	3389	172.30.201.4	49218	46102282	33683	6	192.168.20.254	10
2015-10-09T06:53:51.130Z	192.168.20.76	3389	172.30.201.4	49218	46088056	33673	6	192.168.20.254	11
2015-10-09T05:53:05.999Z	192.168.1.250	3128	10.0.20.168	62806	45244773	15678	6	193.206.22.178	10
2015-10-09T09:14:51.004Z	85.88.193.68	80	195.65.184.230	22043	35857454	23910	6	192.168.20.254	11
2015-10-09T07:13:33.002Z	151.8.136.244	4660	192.168.20.83	25	33228906	31156	6	192.168.20.254	10
2015-10-09T07:18:07.054Z	192.168.20.214	38181	212.227.17.5	25	29921991	19959	6	192.168.20.254	11
2015-10-09T07:18:07.054Z	85.88.196.35	38181	212.227.17.5	25	29921991	19959	6	192.168.20.254	11
2015-10-09T07:18:11.000Z	85.88.196.35	45114	213.33.87.13	25	29721740	20940	6	192.168.20.254	11
2015-10-09T07:18:11.000Z	192.168.20.214	45114	213.33.87.13	25	29672040	20905	6	192.168.20.254	11

Funzioni

Flussi

La scelta dei campi da visualizzare è molto ampia e personalizzabile.

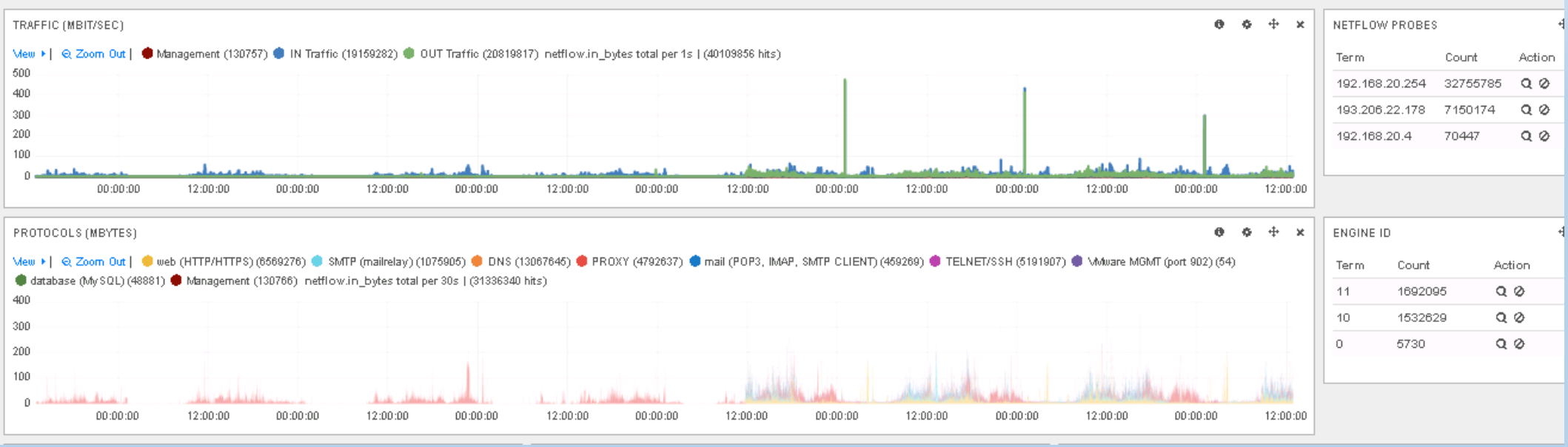
netflow.last_switched	netflow.ipv4_src_addr	netflow.l4_src_port	netflow.ipv4_dst_addr	netflow.l4_dst_port	netflow.in_bytes	netflow.in_pkts	netflow.protocol	host	netflow.engine_id
2015-10-09T03:48:16.004Z	99.99.99.134	53	192.168.20.27	30162	150	1	17	192.168.20.254	10
2015-10-09T03:48:16.008Z	99.99.99.134	53	85.88.193.93	30162	150	1	17	192.168.20.254	10
2015-10-09T03:48:22.028Z	99.99.99.134	53	192.168.20.27	22031	150	1	17	192.168.20.254	10
2015-10-09T03:48:22.028Z	99.99.99.134	53	85.88.193.93	22031	150	1	17	192.168.20.254	10
2015-10-09T05:12:59.012Z	99.99.99.134	53	85.88.193.93	44220	150	1	17	192.168.20.254	10
2015-10-09T05:12:59.012Z	99.99.99.134	53	192.168.20.28	44220	150	1	17	192.168.20.254	10
2015-10-09T08:20:40.000Z	99.99.99.134	53	192.168.20.27	38425	588	1	17	192.168.20.254	10
2015-10-09T08:20:40.000Z	99.99.99.134	53	85.88.193.93	38425	588	1	17	192.168.20.254	10
2015-10-09T05:27:22.002Z	99.99.99.132	53	85.88.193.93	31261	153	1	17	192.168.20.254	10
2015-10-09T05:27:22.002Z	99.99.99.132	53	192.168.20.28	31261	153	1	17	192.168.20.254	10
2015-10-09T05:27:25.009Z	99.99.99.132	53	192.168.20.27	4456	142	1	17	192.168.20.254	10
2015-10-09T05:27:25.011Z	99.99.99.132	53	85.88.193.93	4456	142	1	17	192.168.20.254	10
2015-10-09T05:49:00.001Z	99.99.99.132	53	85.88.193.93	46553	235	1	17	192.168.20.254	10
2015-10-09T05:49:00.000Z	99.99.99.132	53	192.168.20.27	46553	235	1	17	192.168.20.254	10
2015-10-09T08:03:57.005Z	99.99.99.132	53	192.168.20.27	62755	236	1	17	192.168.20.254	10

Per ogni flusso è possibile visualizzare gli indirizzi IP tra cui è avvenuto lo scambio, la quantità di Pacchetti e Bytes trasmessi, il tipo di protocollo e molte altre informazioni.

Funzioni

Confronto temporale

Ampliando l'intervallo di tempo in cui visualizzare i flussi è possibile accorgersi di traffico anomalo che cade regolarmente



Nella schermata d'esempio, in cui la linea temporale è di 7 giorni, si possono notare negli ultimi 3 giorni delle impennate del traffico in uscita sempre alla stessa ora, attorno alla mezzanotte

Con il sistema Bls si può immediatamente individuare origine, destinazione e tipo di traffico e capire se, ad esempio, si tratta di un Backup schedulato, un aggiornamento regolare oppure qualcosa di anomalo che necessita di intervento.