THE ITALIAN RESEARCH & EDUCATION NETWORK

Consortium GARR

Tutorial Netflow

dall'esportazione dei flussi alla elaborazione avanzata delle statistiche

Nino Ciurleo (GARR)

Workshop GARR, Roma, 18-21.04.2016

Agenda

- Perche' monitorare la rete con Netflow
- Protocolli per l'esportazione dei flussi Netflow
- Architettura del sistema di analisi dei flussi
- Suite Nfsen/Nfdump
- Esempi di utilizzo di Nfsen/Nfdump
- Monitoraggio della LAN con Netflow
- Estendere le funzionlita' di Nfsen/Nfdump
- Hands-on

Perche' usare l'esportazione dei flussi?

- Limiti delle statistiche di traffico tradizionali (MRTG, Cacti, etc.)
- Possibilità offerte dall'analisi dei flussi

Limiti delle statistiche di traffico tradizionali

Il monitoring tradizionale usa come sorgente d'informazione i contatori dei router. Esempio: numero di pacchetti e ottetti.

Le informazioni collezionate sono relative alle interfacce e rappresentano il traffico aggregato in transito su di esse.

Non e' possibile analizzare il traffico in base alle caratteristiche delle comunicazioni quali i protocolli utilizzati, le subnet, le porte di livello di trasporto, etc.

Possibilità offerte dall'analisi dei flussi

L'analisi dei flussi prevede che ogni router invii le intestazioni dei pacchetti che lo attraversano ad un collettore.

Informazioni del livello IP, di quello di trasporto (TCP/UDP): indirizzi IP, protocolli, porte

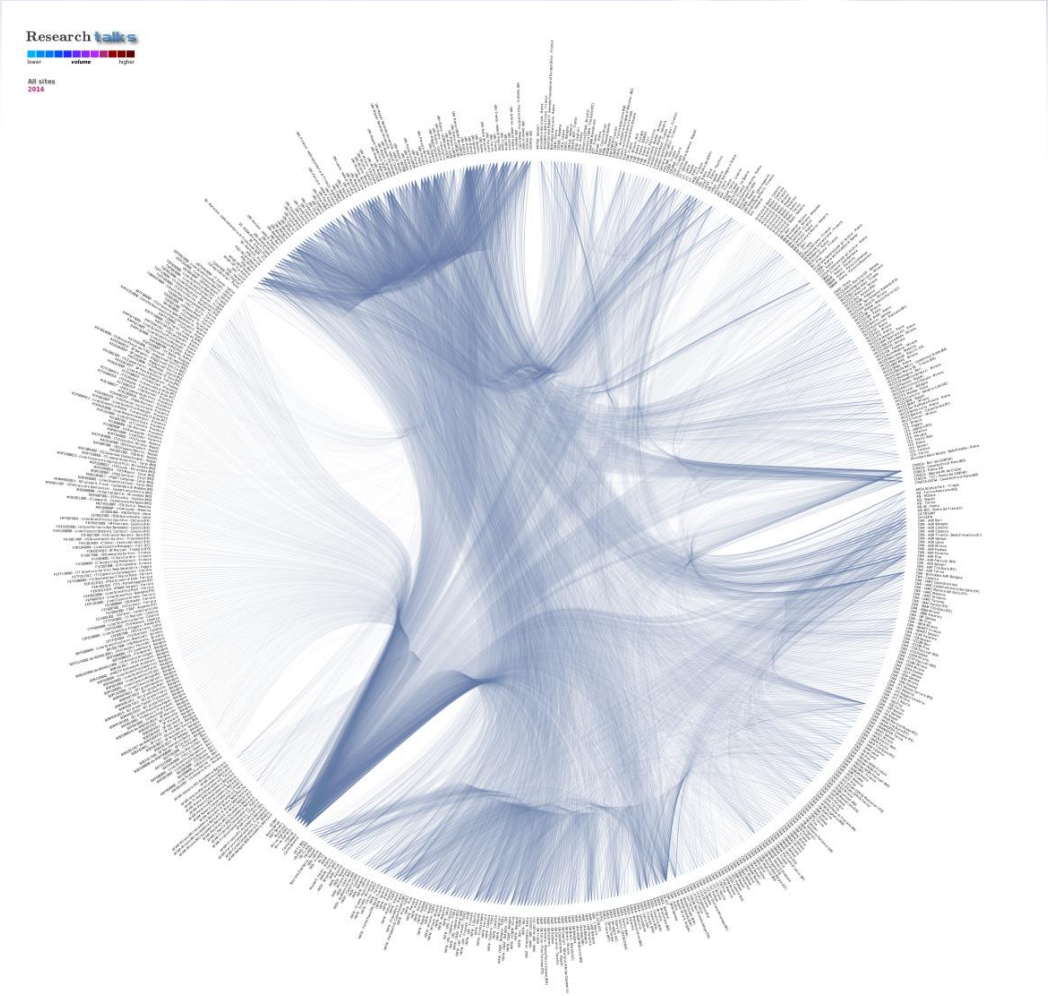
In piu': AS, interfacce, contatori, etc.

Le informazioni raccolte consentono di analizzare dettagliatamente l'attività di rete presente e passata.

Come lo usa GARR? Research talks

Matrice di traffico tra sedi GARR

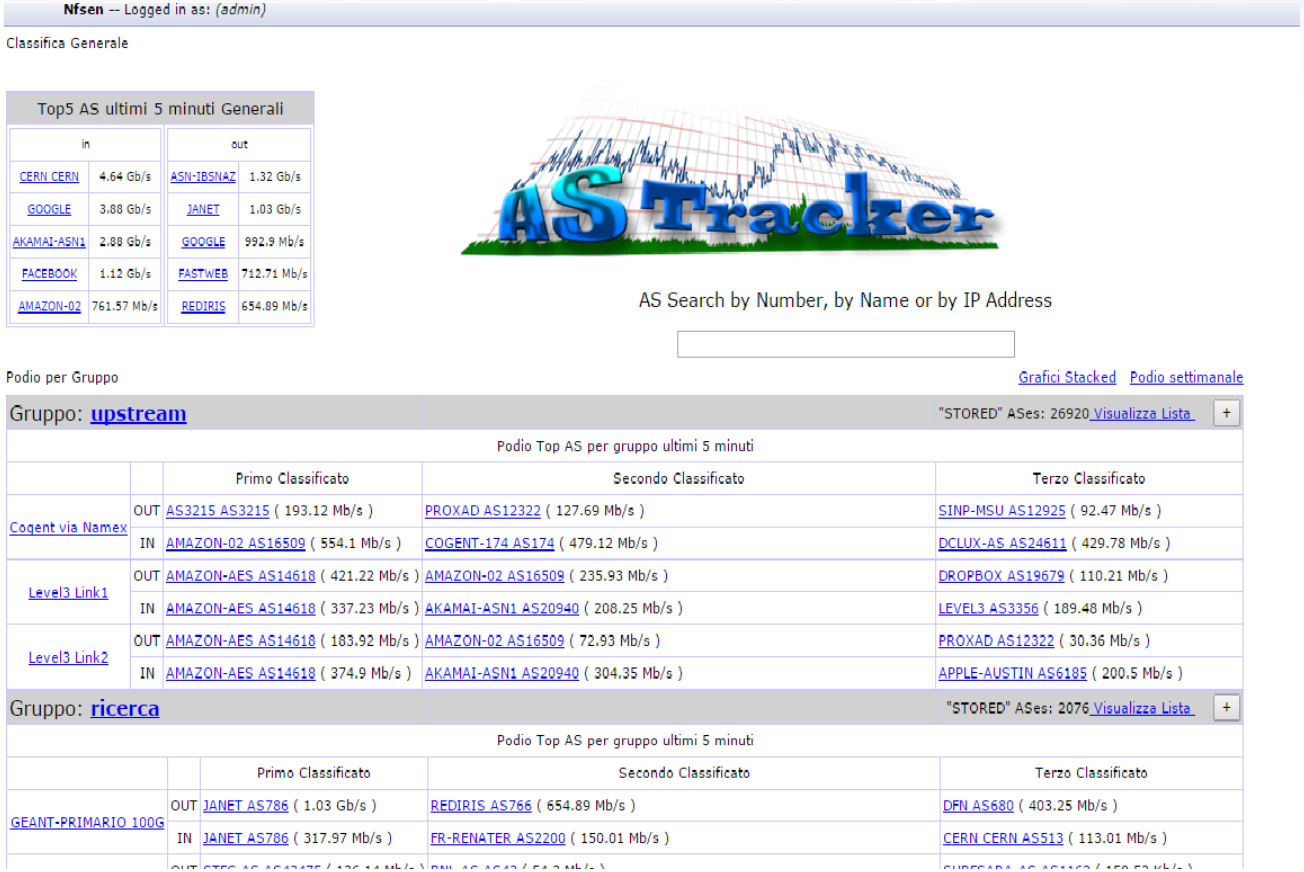
Matrice di tra sedi GARR e AS



Come lo usa GARR? AsTracker

Statistiche di traffico tra la rete GARR e tutti gli altri Autonomous System di Internet

- Troubleshooting politiche di peering BGP
- Analisi categorie di traffico (ricerca, commerciale, peering nazionali, etc)

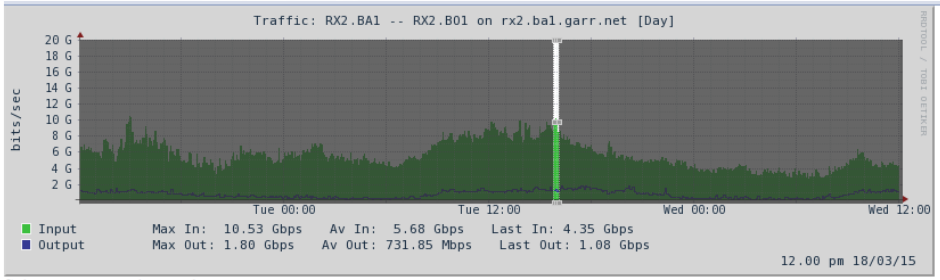


Come lo usa GARR? AsTracker

Come lo usa GARR? GINS

Analisi dettagliata del traffico su tutti i link della rete (backbone, peering e accesso):

- Incidenti di sicurezza
- Anomalie di traffico
- Troubleshooting



Select an area on the graph:
Start Date: Tue Mar 17 2015 15:27:06 GMT+0100 (W. Europe Standard Time)
End Date: Tue Mar 17 2015 15:43:04 GMT+0100 (W. Europe Standard Time)

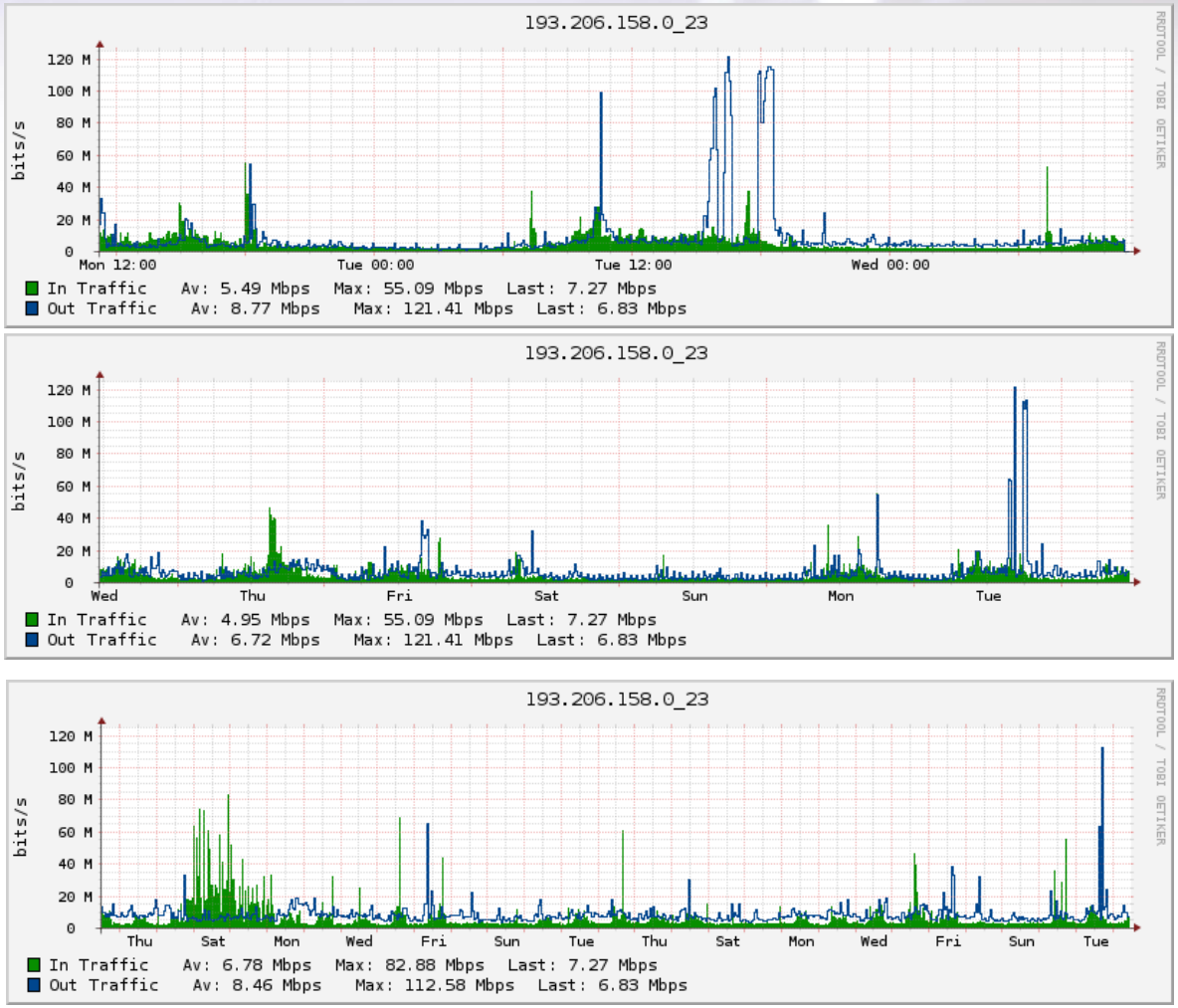
get flow details | get flow list | get flow list no net | get sites details

Posizione	Sorgente	Destinazione	Traffico	% sul totale: 1.42 TB
1	INFN - CNAF - Bologna - TIER1	INFN - Bari - TIER2	500.12 GB	34.36%
2	FNAL-AS(AS3152)	INFN - Bari - TIER2	195.78 GB	13.45%
3	Google-Cache	UNI-Torino	26.8 GB	1.84%
4	Akamai-Cache	UNI-Napoli Federico II	18.87 GB	1.3%
5	Akamai-Cache	UNI-Torino	17.04 GB	1.17%
6	Google-Cache	UNI-Napoli Federico II	16.65 GB	1.14%
7	Akamai-Cache	UNI-Salerno	14.82 GB	1.02%
8	Akamai-Cache	UNI-Roma3	13.85 GB	0.95%
9	Google-Cache	POLI-Torino	13.39 GB	0.92%
10	Google-Cache	UNI-Salerno	12.3 GB	0.85%
11	INFN - CNAF - Bologna - TIER1	INFN - Napoli - TIER2	12.06 GB	0.83%
12	Akamai-Cache	UNI-Palermo	11.92 GB	0.82%
13	Akamai-Cache	POLI-Torino	11.18 GB	0.77%

Come lo usa GARR? Net stats

Statistiche di traffico per network

Ogni rete gestita da GARR ha statistiche aggregate indipendenti dai circuiti su cui passa il traffico



Come lo usa GARR? Rilevamento DOS

---------- SUMMARY ----------
90.147.102.0/24 INFN_-_Bari_-_TIER2 573.7 M

========== 90.147.102.0/24 ==========

Src Network	Dst IP Addr:Port	Dst AS	bps	Bytes	Packets
90.147.102.0/24	162.218.53.18:80	19905	583.2 M	62.4 G	66.7 M
90.147.102.0/24	14.152.83.24:1688	58543	545.7 M	43.3 G	46.3 M
90.147.102.0/24	219.135.58.29:80	58543	574.5 M	33.5 G	35.8 M
90.147.102.0/24	14.152.82.125:81	58543	608.1 M	30.9 G	33.0 M
90.147.102.0/24	72.14.246.1:80	15169	607.0 M	26.0 G	27.8 M
90.147.102.0/24	101.71.48.190:80	4837	582.5 M	13.3 G	14.2 M
90.147.102.0/24	50.117.92.22:1688	18779	134.4 M	12.5 G	13.3 M
90.147.102.0/24	115.231.11.78:1688	4134	130.9 M	12.0 G	12.9 M

Come lo usa GARR? Rilevamento DOS

DDOS attack monitor

Last DDOS attacks report

N	target	target site	start	end	int	bytes	bps	flows	connections
1	138.41.5.42	NATF05000N - ITIS Giordani-Striano - Napoli	12:10 21/03/2016	12:50 21/03/2016	9	106,57 GB	304,28 Mbps	2653687	2653389
2	138.41.5.42	NATF05000N - ITIS Giordani-Striano - Napoli	10:10 21/03/2016	10:25 21/03/2016	4	24,32 GB	163,93 Mbps	596278	596208
3	138.41.5.42	NATF05000N - ITIS Giordani-Striano - Napoli	12:55 17/03/2016	13:10 17/03/2016	4	25,99 GB	175,34 Mbps	649666	649662
4	143.225.249.4	UNI-Napoli Federico II	21:25 16/03/2016	21:45 16/03/2016	5	262,27 GB	1,28 Gbps	184365	81119
5	138.41.5.42	NATF05000N - ITIS Giordani-Striano - Napoli	18:55 16/03/2016	19:15 16/03/2016	5	18,15 GB	120,55 Mbps	453814	453833
6	218.60.113.3	Internet	17:40 15/03/2016	18:40 15/03/2016	13	308,71 GB	587,13 Mbps	337041	334137
7	183.60.85.245	Internet	17:40 15/03/2016	18:40 15/03/2016	13	308,41 GB	574,58 Mbps	336686	333852
8	223.6.249.62	Internet	17:40 15/03/2016	18:40 15/03/2016	13	307,40 GB	587,04 Mbps	335678	332721
9	183.2.193.163	Internet	17:40 15/03/2016	18:40 15/03/2016	13	289,27 GB	534,60 Mbps	315853	313382
10	14.17.94.172	Internet	17:55 15/03/2016	18:40 15/03/2016	9	177,19 GB	487,37 Mbps	193586	192248
11	183.60.110.239	Internet	17:25 15/03/2016	17:25 15/03/2016	1	66,75 GB	2,20 Gbps	70485	70289
12	138.41.5.42	NATF05000N - ITIS Giordani-Striano - Napoli	12:10 14/03/2016	12:25 14/03/2016	4	27,27 GB	178,14 Mbps	673127	672942
13	138.41.5.39	NATF05000N - ITIS Giordani-Striano - Napoli	11:55 14/03/2016	12:00 14/03/2016	2	11,88 GB	165,41 Mbps	295879	295861
14	138.41.5.42	NATF05000N - ITIS Giordani-Striano - Napoli	11:05 14/03/2016	11:50 14/03/2016	10	75,31 GB	184,30 Mbps	1843038	1842745
15	138.41.5.33	NATF05000N - ITIS Giordani-Striano - Napoli	10:55 14/03/2016	10:55 14/03/2016	1	1,01 GB	280,87 Mbps	25357	25363
16	138.41.5.42	NATF05000N - ITIS Giordani-Striano - Napoli	10:25 14/03/2016	10:35 14/03/2016	2	11,11 GB	134,70 Mbps	270769	270647
17	138.41.5.34	NATF05000N - ITIS Giordani-Striano - Napoli	10:35 14/03/2016	10:35 14/03/2016	1	3,12 GB	140,22 Mbps	76699	76657
18	138.41.5.41	NATF05000N - ITIS Giordani-Striano - Napoli	10:30 14/03/2016	10:30 14/03/2016	1	4,01 GB	245,96 Mbps	100213	100219
19	138.41.5.39	NATF05000N - ITIS Giordani-Striano - Napoli	10:05 14/03/2016	10:25 14/03/2016	5	52,86 GB	302,47 Mbps	1321017	1320984
20	138.41.5.39	NATF05000N - ITIS Giordani-Striano - Napoli	09:00 14/03/2016	09:45 14/03/2016	9	99,98 GB	332,94 Mbps	2498673	2498605
21	138.41.5.39	NATF05000N - ITIS Giordani-Striano - Napoli	08:20 14/03/2016	08:35 14/03/2016	4	49,79 GB	338,37 Mbps	1243897	1243830
22	138.41.5.39	NATF05000N - ITIS Giordani-Striano - Napoli	12:25 11/03/2016	12:40 11/03/2016	4	25,02 GB	160,00 Mbps	623828	623805

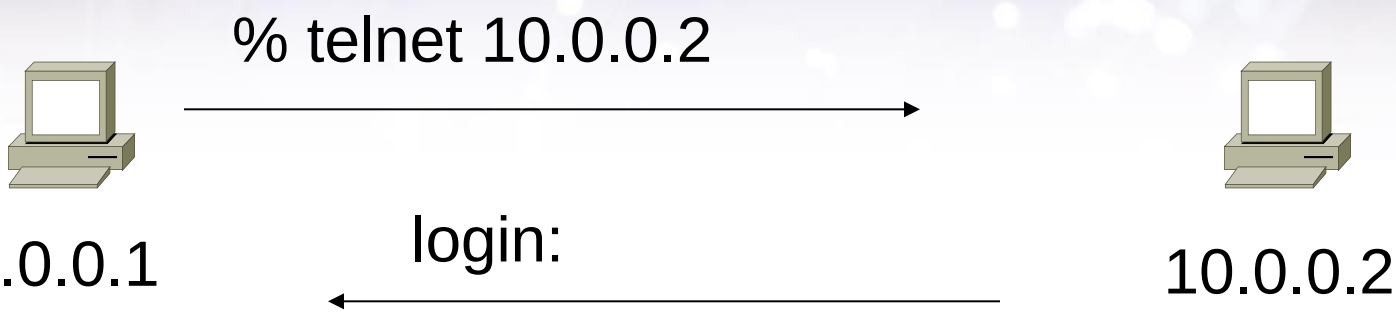
Protocolli

- Concetto di flusso
- Versioni del protocollo Netflow
  - Netflow 5
  - Netflow 9
  - IPFIX

Cos'e' un flusso Netflow?

- Per flusso si intende ogni comunicazione unidirezionale identificata da 7 campi degli header IP e UDP/TCP (valido per Netflow 5)
- Vengono raggruppati nello stesso flusso i pacchetti che hanno in comune:
  - Indirizzo IP sorgente
  - Indirizzo IP destinazione
  - porte sorgente
  - porte destinazione
  - Protocollo
  - Interfaccia di ingresso
  - ToS

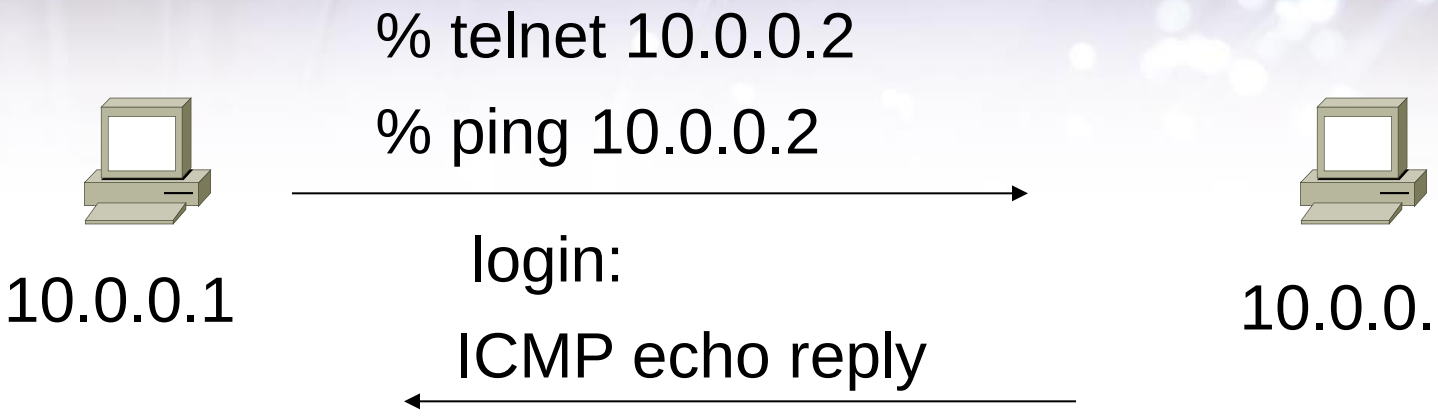
Esempi di flusso (1)



Active Flows

Flow	Source IP	Destination IP
1	10.0.0.1	10.0.0.2
2	10.0.0.2	10.0.0.1

Esempi di flusso (2)



Active Flows

Flow	Source IP	Destination IP	prot	srcPort	dstPort
1	10.0.0.1	10.0.0.2	TCP	32000	23
2	10.0.0.2	10.0.0.1	TCP	23	32000
3	10.0.0.1	10.0.0.2	ICMP	0	0
4	10.0.0.2	10.0.0.1	ICMP	0	0

Protocolli per l'esportazione dei flussi

- Netflow, inizialmente sviluppato da Cisco, e' diventato uno standard "de facto" ed implementato da gran parte dei costruttori di hardware (c/jflowd su Juniper, Cflowd su Alcatel, NetStream su Huawei).
- Versioni:
  - V5 la versione supportata da quasi tutti i vendor e ancora la piu' utilizzata
  - V7 per gli switch catalyst 5000
  - V8 possibilità di esportare flussi aggregati
  - V9 la versione piu' recente e flessibile (RFC 3954)
    - possibilità di definire template personalizzati
    - Trasporto di informazioni di livello2, IPV6, MPLS, BGP, protocol next_hop, etc
  - IPFIX (Internet Protocol Flow Information eXport) standardizzazione IETF (RFC 5101 e 5102) di NetFlow v9

Netflow versione 5

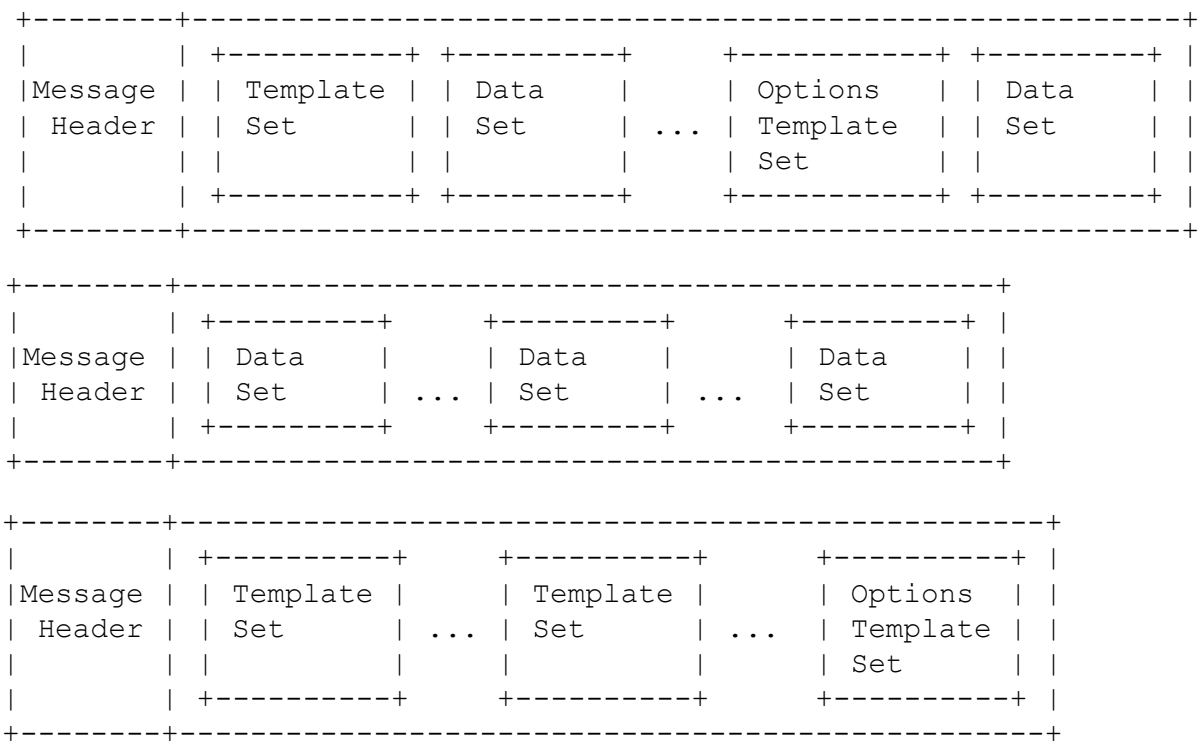
- Supporta solamente IPv4
- Formato dei record Netflow 5:
  - IP sorgente e destinazione
  - porte sorgente e destinazione
  - interfaccia d'ingresso e di uscita
  - AS number sorgente e destinazione
  - TCP flags
  - ToS (DSCP)
  - Contatori di ottetti e pacchetti

Netflow versione 9

- Supporta IPv4, IPv6 ed MPLS
- informazioni trasportate sono:
  - IP sorgente e destinazione
  - porte sorgente e destinazione
  - interfaccia d'ingresso e di uscita
  - AS number sorgente e destinazione
  - Indirizzo IP "Next-Hop"
  - BGP "Next-hop"
  - TCP flags
  - ToS (DSCP)
  - Contatori di ottetti e pacchetti
  - Direzione del flusso
  - Indirizzo MAC sorgente e destinazione in ingresso
  - Indirizzo MAC sorgente e destinazione in uscita
  - Label VLAN
  - Label MPLS

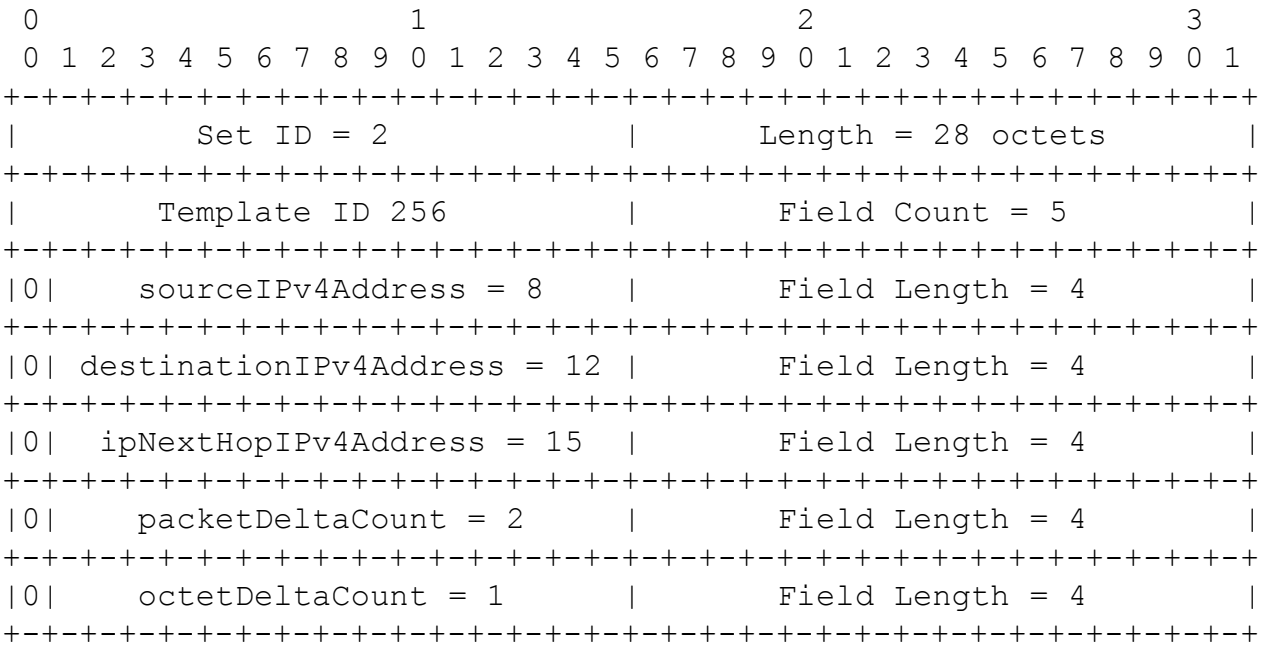
IPFIX

- Standardizzazione di Netflow v9
- RFC7011, RFC5101, RFC5153
- Meccanismo Template flessibile



IPFIX

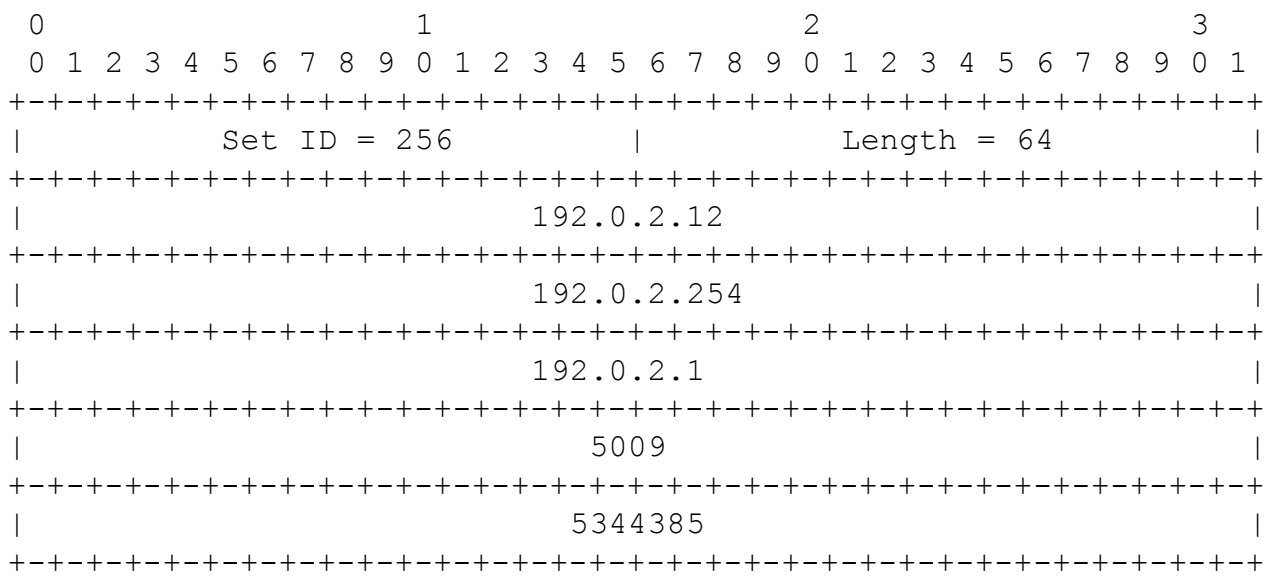
- Esempio Template



IPFIX

- Esempio Data set

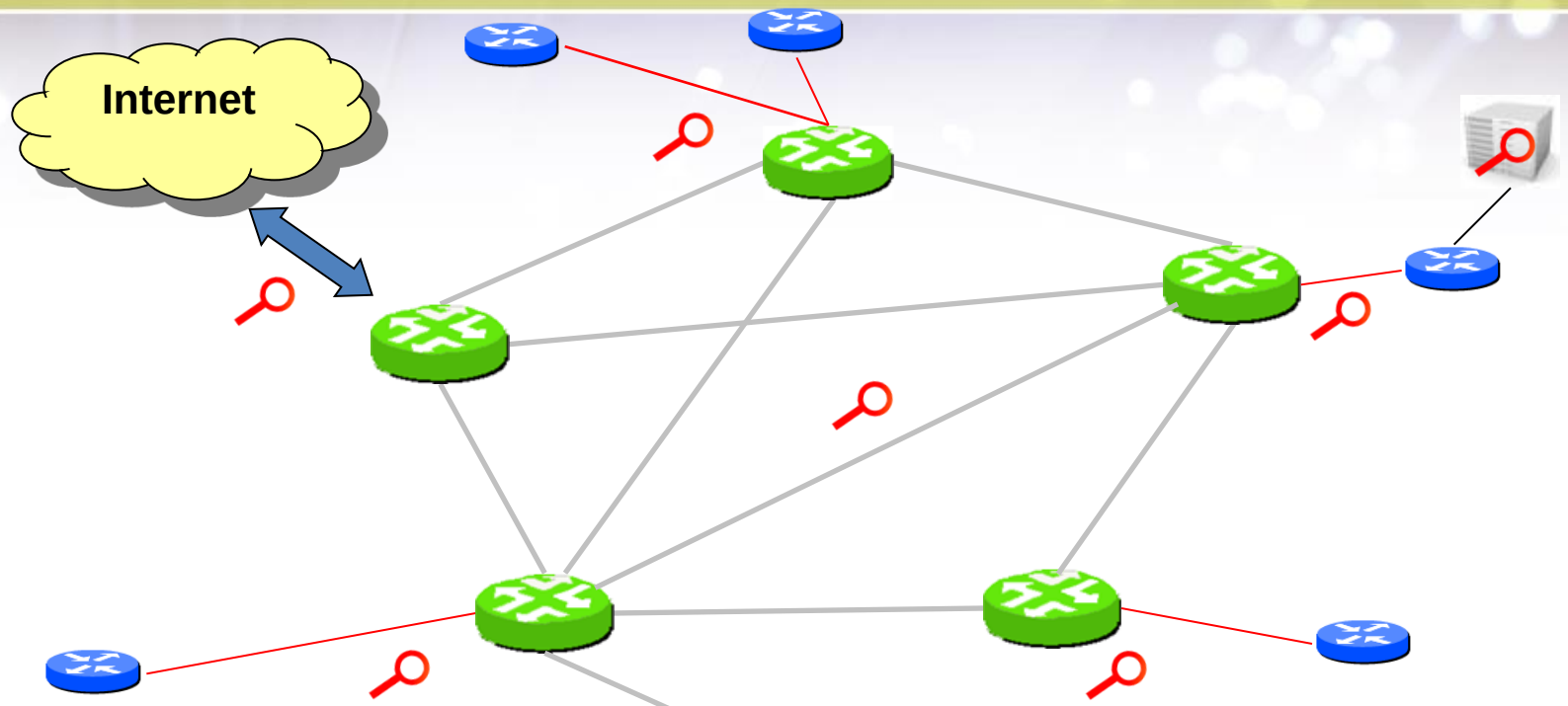
```
Src IP Addr.  | Dst IP Addr.   | Next-Hop Addr. | Packet | Octets
              |                |                | Number | Number
--------------------------------------------------------------------
192.0.2.12    | 192.0.2.254    | 192.0.2.1      | 5009   | 5344385
192.0.2.27    | 192.0.2.23     | 192.0.2.2      | 748    | 388934
192.0.2.56    | 192.0.2.65     | 192.0.2.3      | 5      | 6534
```

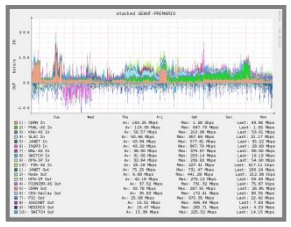


Architettura

- Esportazione dei flussi
- Collezione  ed analisi 

Architettura

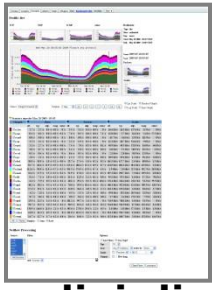




Analisi elaborata

Elaborazione

Collezione



Analisi diretta

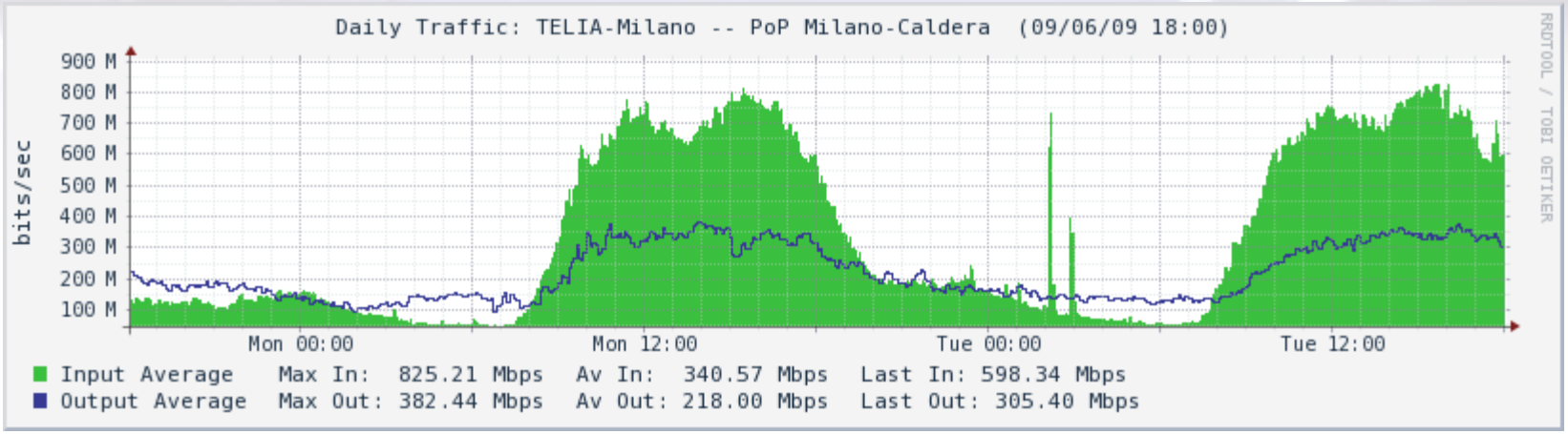
Esportazione

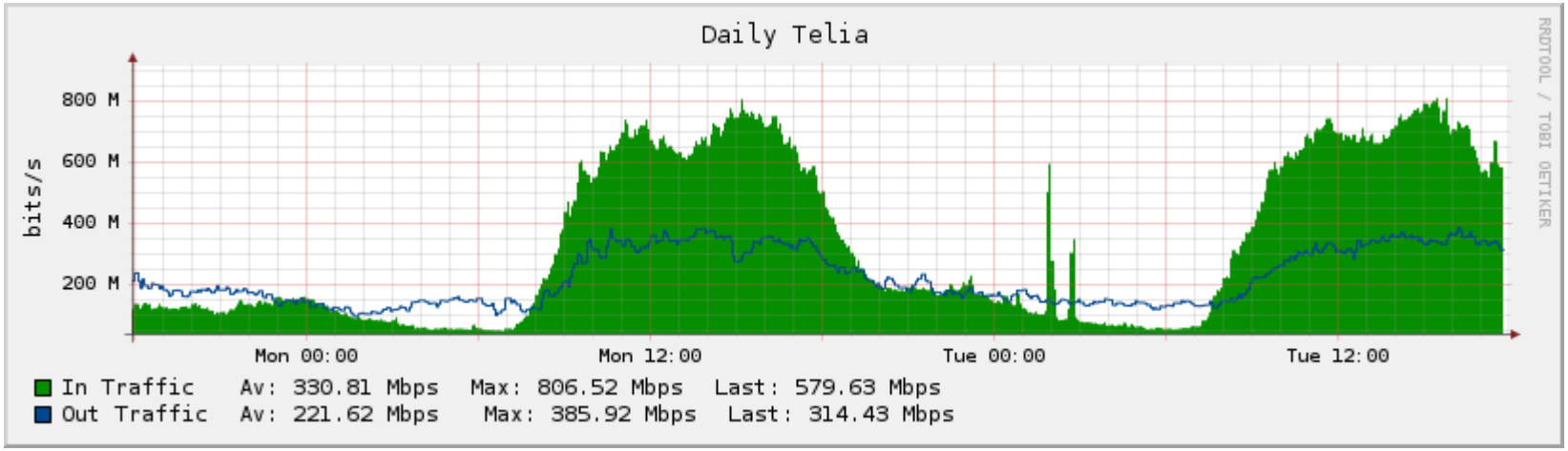
- Netflow e' stato concepito, in origine, per far esportare i flussi dagli apparati di rete, quali router e switch.
- Esistono software per server che sono in grado di emulare il comportamento dei router
- Parametri da configurare:
  - Interfacce di cui si vogliono esportare i flussi
  - Indirizzo e porta del collector
  - Versione di Netflow
  - Timeout per l'esportazione (active e inactive timeout)
  - Eventuale tasso di campionamento
  - Nel caso di Netflow v9 va definito il template dei dati da esportare

Sampling (1/2)

- La cattura dei flissi Netflow puo' risultare gravosa per il router, portando la CPU in saturazione. Per evitare problemi dovuti al sovraccaricamento del processore del router, e' stato introdotto un meccamismo di campionamento: invece di catturare tutti i pacchetti in transito, il router prende un pacchetto ogni n. Tale parametro e' configuabile a piacere.
- Quando viene usato il campionamento, il traffico visualizzato nei sistemi di analisi dei flussi e' approssimato.
- Ma per la legge dei grandi numeri i conti tornano…

Sampling (2/2)


Daily Traffic: TELIA-Milano -- PoP Milano-Caldera (09/06/09 18:00)
bits/sec
900 M
800 M
700 M
600 M
500 M
400 M
300 M
200 M
100 M
Mon 00:00
Mon 12:00
Tue 00:00
Tue 12:00
RRDTOOL / TOBI OETIKER
Input Average Max In: 825.21 Mbps Av In: 340.57 Mbps Last In: 598.34 Mbps
Output Average Max Out: 382.44 Mbps Av Out: 218.00 Mbps Last Out: 305.40 Mbps


Daily Telia
bits/s
800 M
600 M
400 M
200 M
Mon 00:00
Mon 12:00
Tue 00:00
Tue 12:00
RRDTOOL / TOBI OETIKER
In Traffic Av: 330.81 Mbps Max: 806.52 Mbps Last: 579.63 Mbps
Out Traffic Av: 221.62 Mbps Max: 385.92 Mbps Last: 314.43 Mbps

Collezione  e analisi 

- Esistono applicativi open-source e commerciali per collezionare ed analizzare i flussi esportati. Quelli open piu' conosciuti sono: flow-tools, stager, ntop, Nerd e la suite nfsen/nfdump
- La scelta, nel caso di GARR, e' ricaduta sulla suite Nfsen/Nfdump.
  - E' un progetto open-source sviluppato dalla NREN svizzera SWITCH (Peter Haag e' l'autore).
  - Tool completo
    - Supporto Netflow 9 (IPv6, MPLS)
    - Tool da linea di comando per la collezione e l'analisi dei flussi (nfcapd, nfdump)
    - altre utility per la gestione dei flussi (ri-esportazione dei flussi, cancellazione dei flussi piu' vecchi, conversione da altri formati, etc.)
    - Possibilità di anonimizzare i flussi
    - un sistema di plugin per l'estensione delle funzionalità
    - Interfaccia grafica
    - Software in continuo sviluppo (mailing lista attiva!)

Suite Nfdump/NfSen

- Installazione e configurazione
- Nfcapd
  - Collezione e salvataggio dei dati
- Nfdump
  - Analisi dei dati via shell
- Nfsen
  - Analisi dei dati tramite interfaccia web
  - Profili
  - Allarmi
  - Plugin

Installazione e configurazione

- Nfdump
  - pacchetti binari delle distribuzioni linux
    es. apt-get install nfdump
  - sorgenti
    es. ./configure –enable-nfprofile && make && make install
- Nfsen
  - Prerequisiti:
    - PHP
    - Perl
    - RRDtools
    - Nfdump con –enable-nfprofile
  - Installazione da sorgenti
    - Copiare nfsen-dist.conf in nfsen.conf
    - Modificare nfsen.conf definendo i pripri exporter in %sources e i path
    - Lanciare ./install.pl </path/nfsen.conf>

Nfcapd

- Demone che riceve i pacchetti Netflow e li scrive periodicamente (per default ogni 5 minuti) su disco sotto forma di file (dati binari indicizzati)
- Un'istanza di nfcapd per ogni router collezionato oppure un'istanza per piu' router
- Permette di lanciare un comando shell ogni volta che ha finito di scrivere un nuovo set di dati (con –x <comando>).
- *Sintassi: nfcapd –w –D –s <sampling rate> -T <v9 extension tags> –I <source_name> -p <porta> -u <user> -g <group> -B <buffer size> -S <dir-hierarchy level> –l /<path>/source_name>*
- *Esempio: nfcapd –w –D –s 1000 –T all –I router1 -p 12001 –B 200000 -S 1 –l /data/nfsen/profiles-data/live/router1*

Nfdump (1/2)

- Serve per consultare ed elaborare i dati salvati su disco sotto forma di file binari da nfcapd
- Caratteristiche:
  - Molto efficiente (dati binari indicizzati, scritto in C)
  - Supporta i formati Netflow 5,9 e IPFIX
  - Supporta sflow (sfcapd)
  - Sintassi semplice ed intuitiva (possibilità di definire filtri stile “tcpdump”)
  - Consultazione molto flessibile:
    - Analisi dei singoli flussi registrati
    - Generazione dei top talkers (bytes, flows, packets)
    - Aggregazione dei dati (temporale e di sorgenti diverse).

Nfdump (2/2)

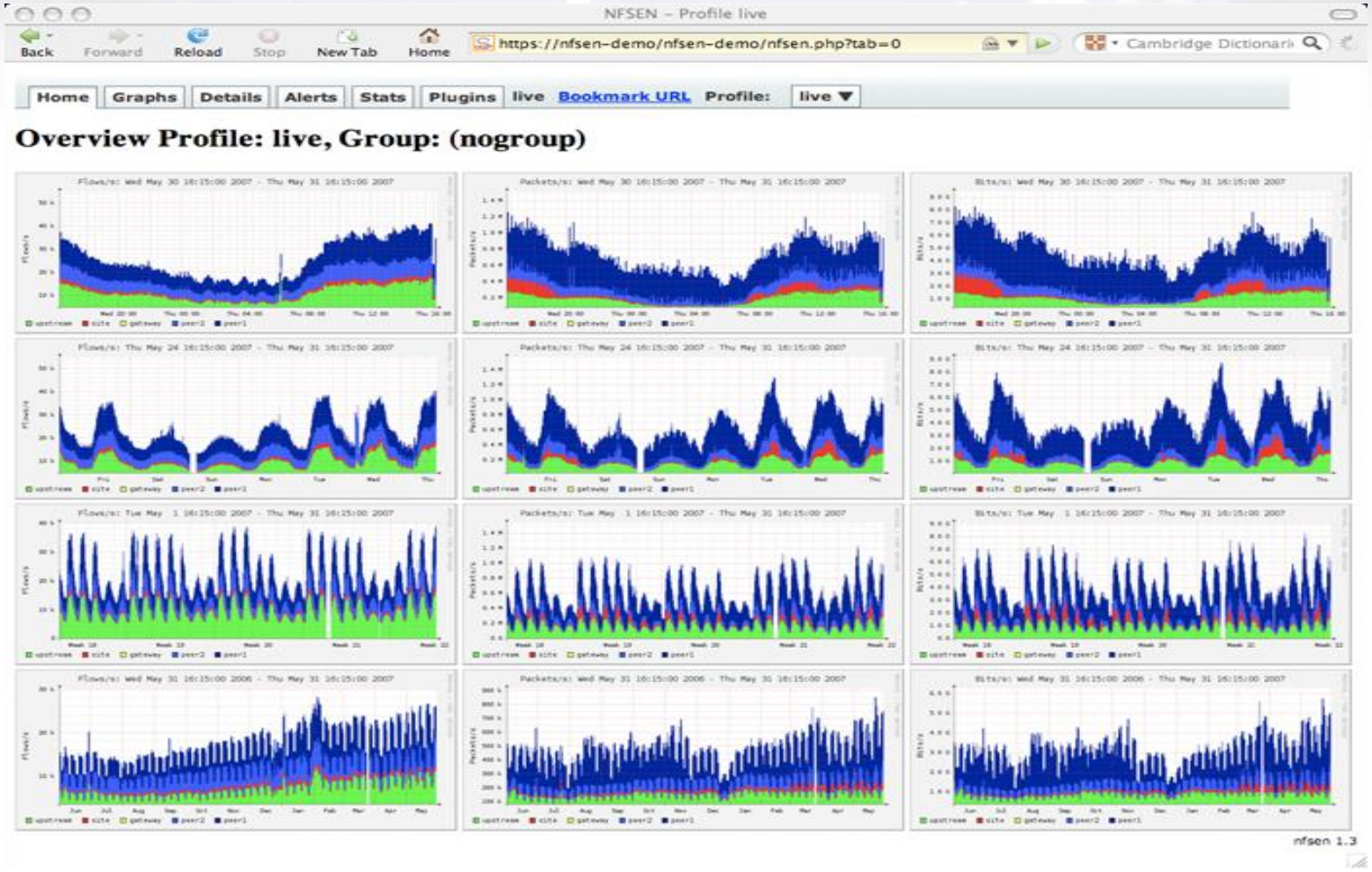
- Caratteristiche (continua …):
  - Crea statistiche su aggregati di flussi (record) secondo un insieme di criteri scelti dall'utente (src/dst IP, src/dst port, src/dst AS, protocol, ToS, interface)
  - Permette la personalizzazione del formato di output, prevede un output machine readable per lo scripting ed integrazioni con alcuni linguaggi di programmazione
  - Consente l'anonimizzazione degli indirizzi IP tramite la libreria CryptoPan
  - E' utilizzato in background da nfsen

Nfsen

- Interfaccia grafica web di nfdump
- Caratteristiche:
  - utilizza `nfdump` come back-end
  - fornisce una visione complessiva e dettagliata allo stesso tempo dello stato della rete
  - grafici specifici per profili (per host, per porta etc.)
  - analisi di un particolare lasso di tempo
  - sistema di post-processing automatico e alerting
  - flessibile con l'utilizzo dei plugin
  - utilizzo intuitivo
  - funzionalità di IP lookup
  - “si pulisce da solo”

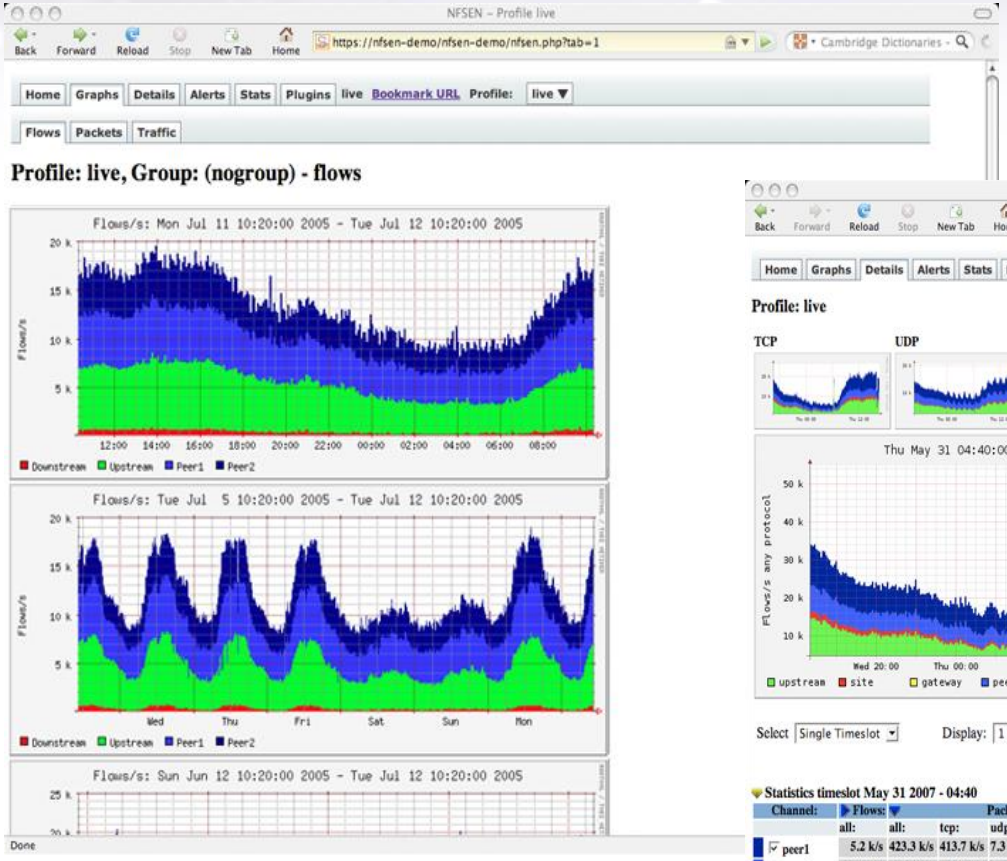
Interfaccia grafica di NfSen (1/3)

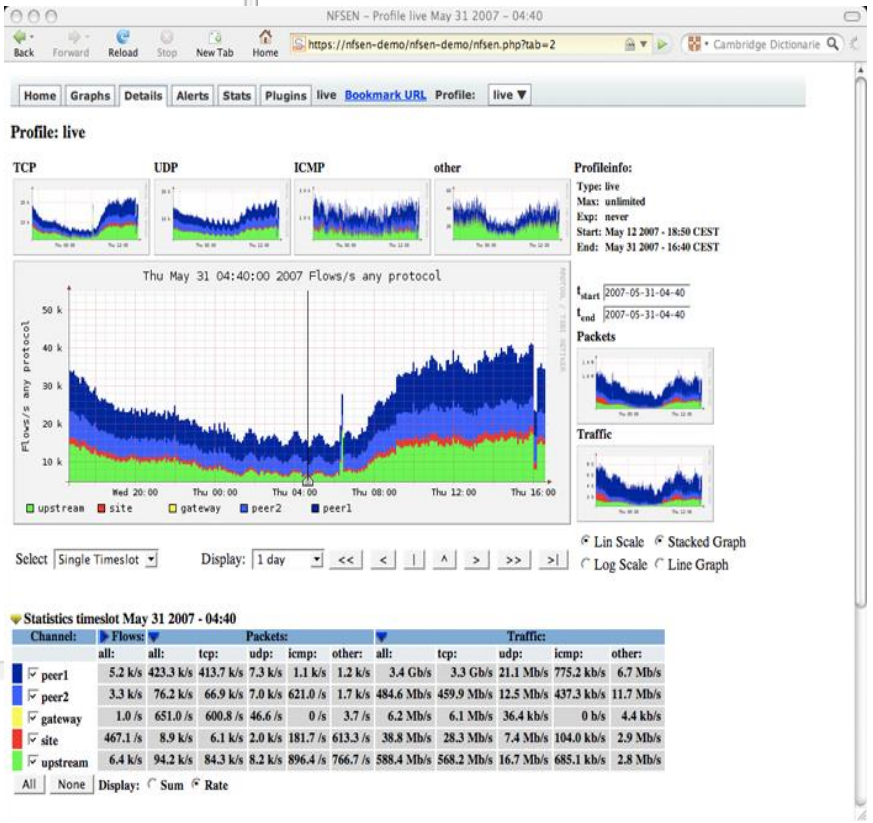
Home Tab



Interfaccia grafica di NfSen (2/3)

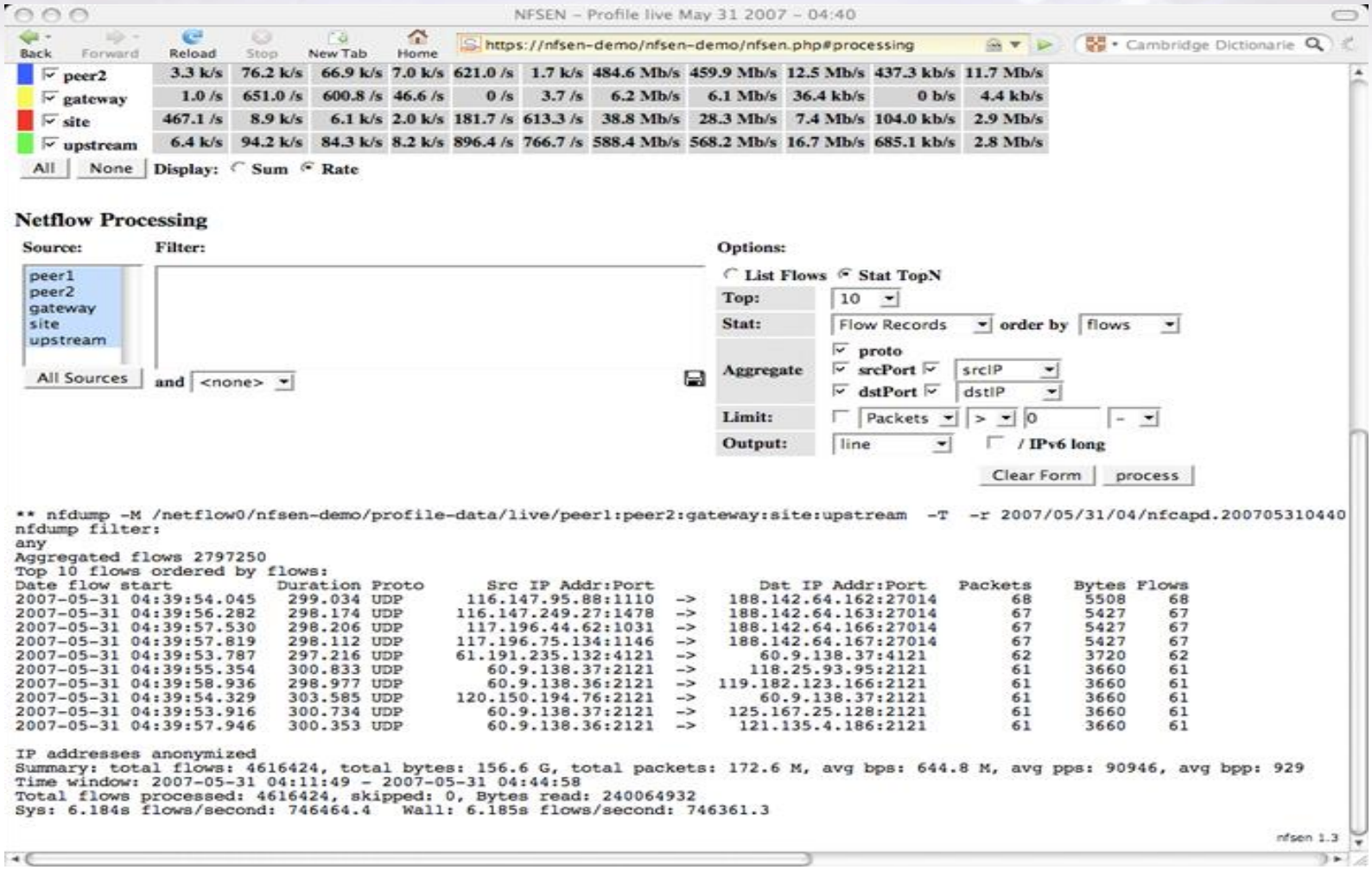
Graphs e Details tab





Interfaccia grafica di NfSen (3/3)

Dettaglio dei flussi



Profili

- Costituiscono una vista specifica di dati netflow ottenuta attraverso l'applicazione di un filtro di nfdump
- Vista GRAFICA di un filtro
- Si possono creare nel passato
- Si possono creare in modo "continuo"
- Puo' contenere un numero qualsiasi di sorgenti
- Puo' essere generato da un qualsiasi filtro

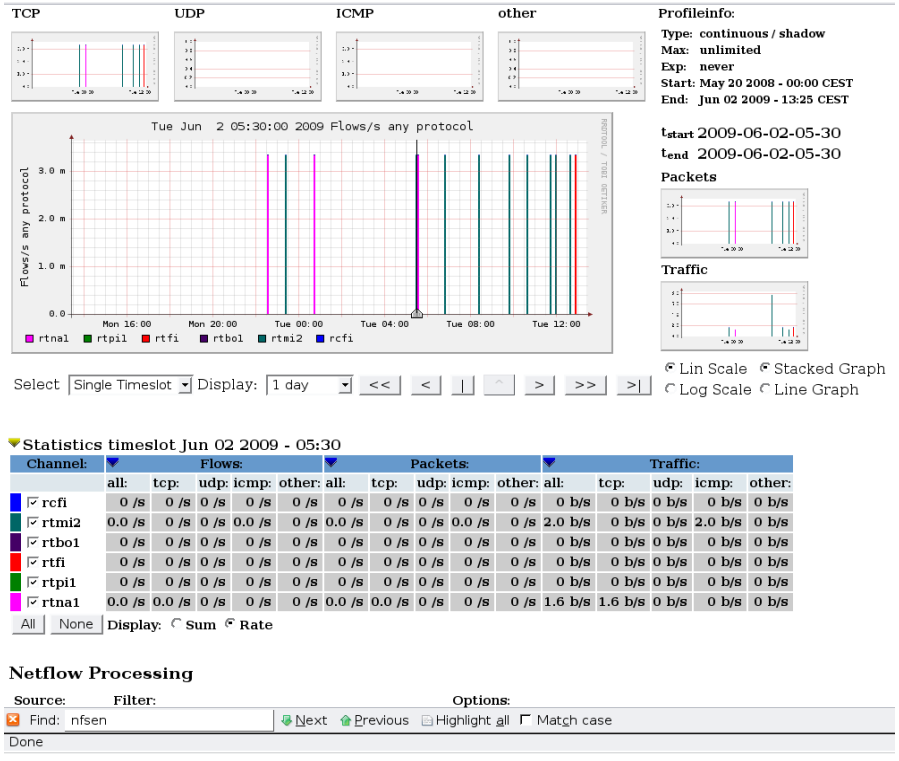
Profili: esempi

Tutti gli host che si connettono a server noti di botnet

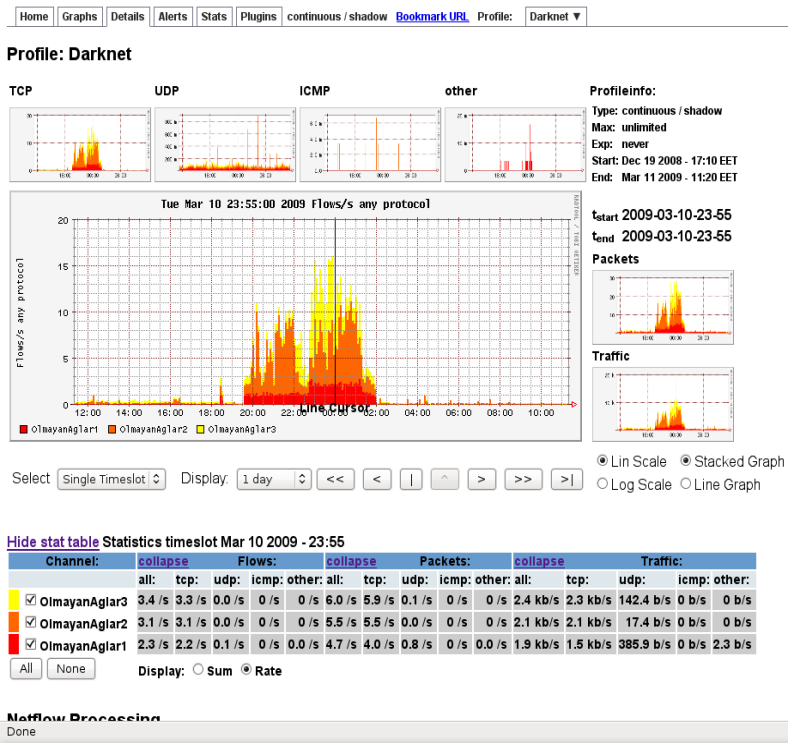
il filtro e':

- 'ip in [ip1, ip2, ..., ipN]'

dove ip1, ip2, ..., ipN sono ip di botnet

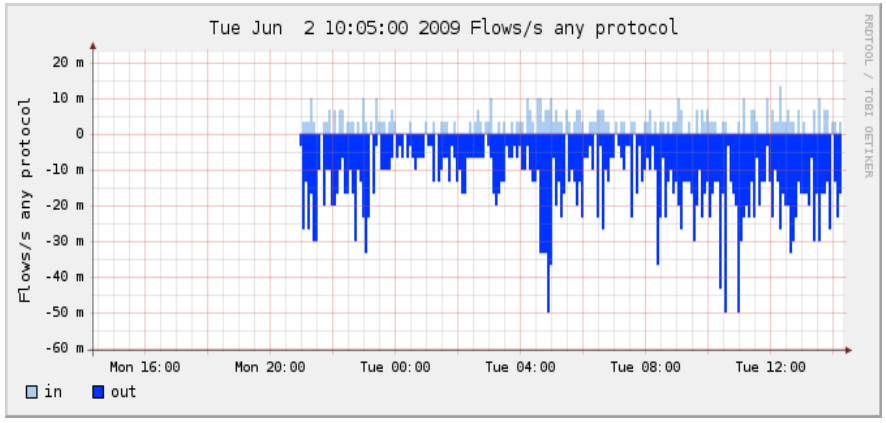


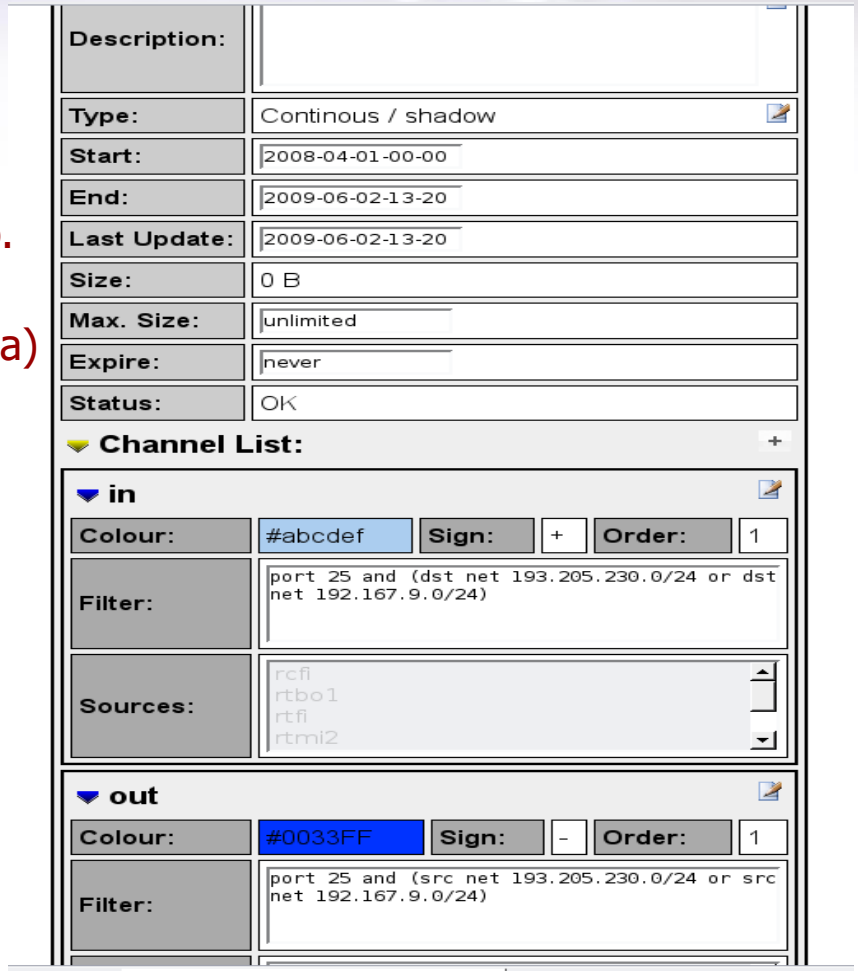
- Monitoraggio di una DarkNet
- il filtro e':
  - 'net rete.dark.net/24'



Profili: creazione

- Si possono definire canali con segno positivo e negativo per visualizzare il traffico in entrata e uscita contemporaneamente sullo stesso grafico.
- In questo caso monitoriamo server di posta suddividendo il traffico fra quello che esce (sopra) e quello che entra sulla porta 25/TCP

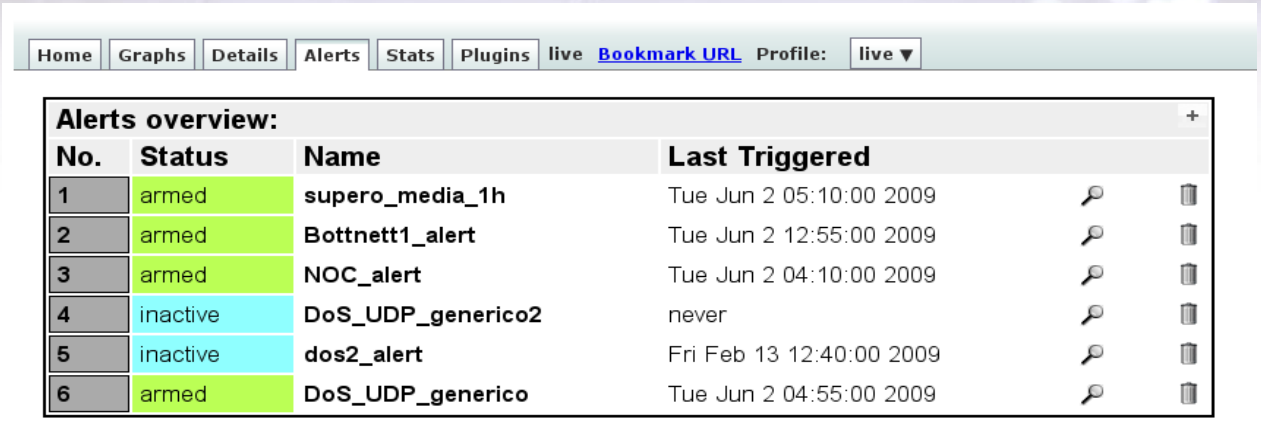




Profili: tipi

- **Continous:** e’ un profilo che, una volta creato, viene aggiornato ogni 5 minuti col nuovo traffico che soddisfa il filtro impostato
- **History:** e' un profilo che si ferma in un punto del passato e non viene piu' aggiornato
- **Real:** e’ un profilo i cui dati filtrati vengono immagazzinati su una parte diversa del disco rispetto al profilo di default
- **Shadow:** e’ un profilo i cui dati vengono filtrati, vengono generati i grafici ma non vengono salvati, il calcolo viene fatto al volo quando richiesto

Alert



- Ogni 5 minuti viene controllata la condizione di alerting impostata
- Estrema flessibilita' nelle impostazione di soglie e filtri
- Sistema automatico di "reazione" una volta che la condizione di alert e' verificata
- Sistema automatico di "notifica" una volta che la condizione di alert e' verificata

Alert: esempi di condizioni

Manda un alert quando il numero di flussi nei 5 minuti e' > 2

Manda un alert quando il rate dei flussi del router X supera i 100 flussi/secondo

Invia una mail al superamento della soglia dei 1000 pacchetti/secondo sul router Y

Esegui un programma esterno che calcola l'ip coinvolto e il suo relativo traffico, ogni volta che il numero di byte per protocollo TCP, sulla porta 80, che viene dalla sorgente X, supera il 30% della media calcolata su un periodo di 6 ore (leggermente piu' complicato)

Alert: configurazione

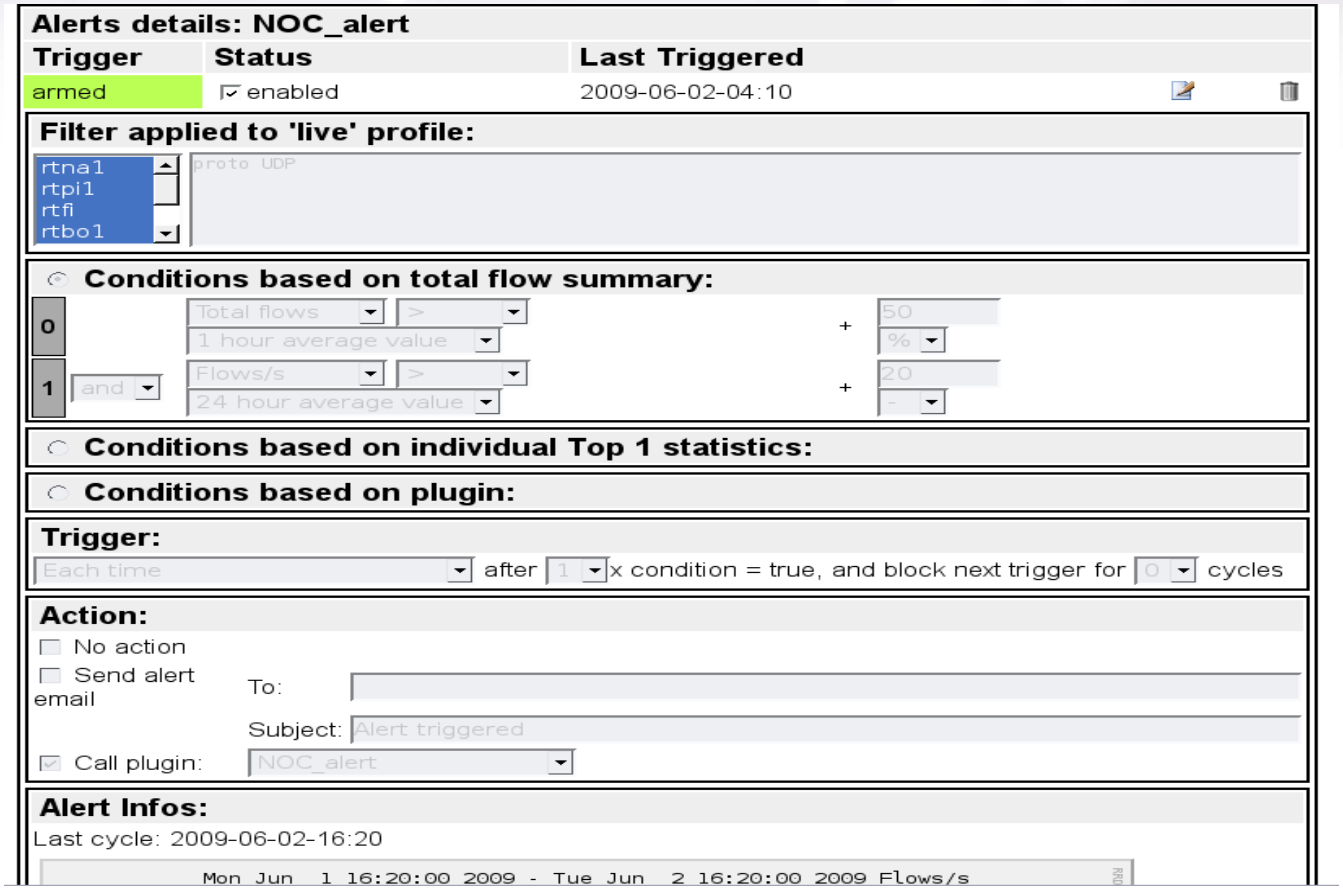
Stato

Filtro

Condizioni

Trigger

Azioni



Alert: infos

Alert Infos:

Last cycle: 2009-06-05-14:30

		Last	Avg 10m	Avg 30m	Avg 1h	Avg 6h	Avg 12h	Avg 24h
◉	**Flows**	17.1 k	17.0 k	16.7 k	16.3 k	17.1 k	11.9 k	12.1 k
		56.9 /s	56.6 /s	55.5 /s	54.3 /s	56.9 /s	39.6 /s	40.3 /s
○	**Packets**	32.2 k	32.5 k	30.6 k	31.9 k	49.3 k	42.5 k	40.3 k
		107.5 /s	108.4 /s	102.0 /s	106.5 /s	164.4 /s	141.8 /s	134.2 /s
○	**Bytes**	2.1 MB	2.1 MB	2.0 MB	2.0 MB	2.9 MB	2.6 MB	2.5 MB
		55.3 kb/s	56.2 kb/s	52.7 kb/s	52.8 kb/s	76.7 kb/s	69.4 kb/s	67.5 kb/s

Conditions:	**0**	**1**	**Final:**
State:	False	False	**False**

Plugin

Servono a:

- estendere le funzionalità di Nfsen/Nfdump
- automatizzare una serie di operazioni complesse

Possono funzionare insieme agli alert

- Generazione di una condizione di alert
- Azione a seguito di un alert

Quando usarli?

- Monitoraggio e notifica di eventi particolari sulla rete
- Tracciare botnet e mandare notifiche
- Tracciare scanning, DoS, probe non visibili dai grafici
- Analisi di traffico: porte maggiormente utilizzate o distribuzione di protocolli
- Elaborazione di statistiche avanzate

Plugin: funzionamento

- Esistono due tipi di plugin:
  - Back-end plugin:
    - Sono moduli perl che vengono “agganciati” ad Nfsen
    - Fanno cose altrimenti non possibili con la suite
    - Sono richiamati automaticamente ogni 5 minuti
  - Front-end plugin:
    - Sono moduli PHP “agganciati” ad NfSen
    - Fanno parte delle pagine web di NfSen
    - Anche questi si aggiornano ogni 5 minuti

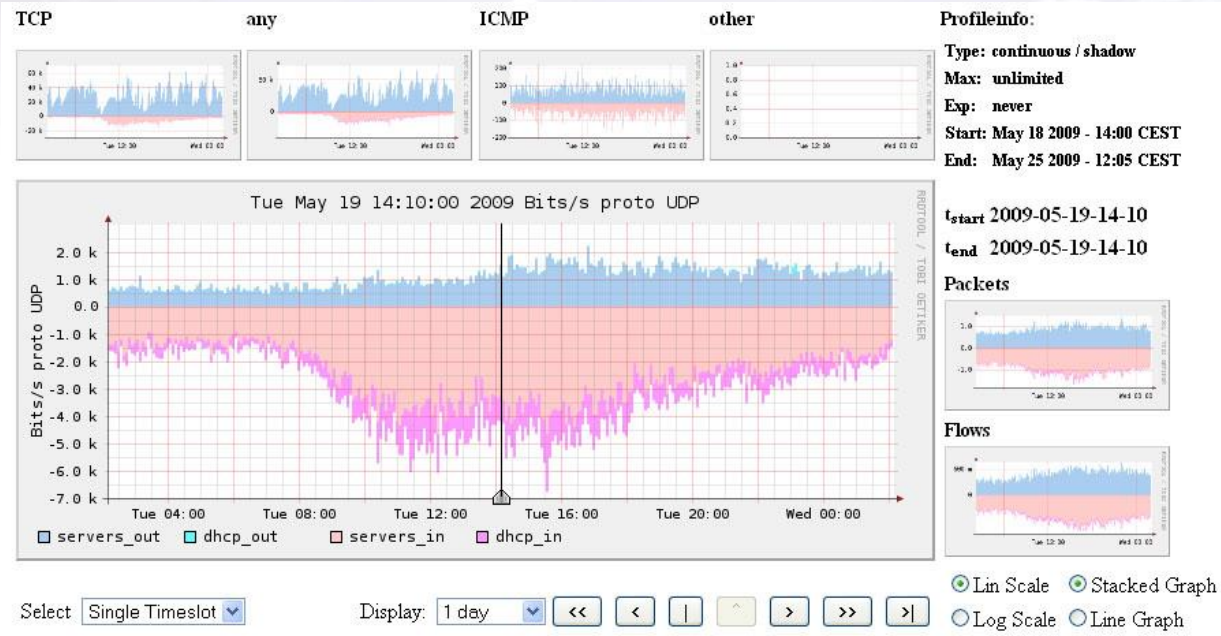
Esempi di uso di Nfsen/Nfdump

- Monitoraggio della rete
  - Analisi per subnet, per protocollo, per porta, per AS
    - Subnet
    - Servizi (Mail, DNS, WEB)
    - Protocollo
    - Porte (plugin PortTracker)
    - Numeri AS (plugin AsTracker)
  - TopTalkers
    - Aggregazione predefinita
    - Aggregazione personalizzata
- Sicurezza
  - Analisi degli incidenti di sicurezza
  - Tracciamento degli host
  - Identificazione di traffico “malevolo”

Monitoraggio della rete

- E’ possibile condurre analisi per ogni singolo campo previsto (indirizzi IP, protocollo, porte, AS, interfacce, etc)
  - Tramite lo strumento “profili” si possono configurare statistiche specifiche relative a criteri desiderati.
  - Ogni profilo, per default, fornisce le statistiche distinte per protocollo.
- Esempi:
  - Suddivisione delle rete in categorie(es. Workstation, DMZ, dhcp hosts)
  - Bogon Network, ICMP su Upstream Provider
  - Mail Server, Name Server, Web Server
  - ASes

Esempio: Traffico suddiviso per subnet

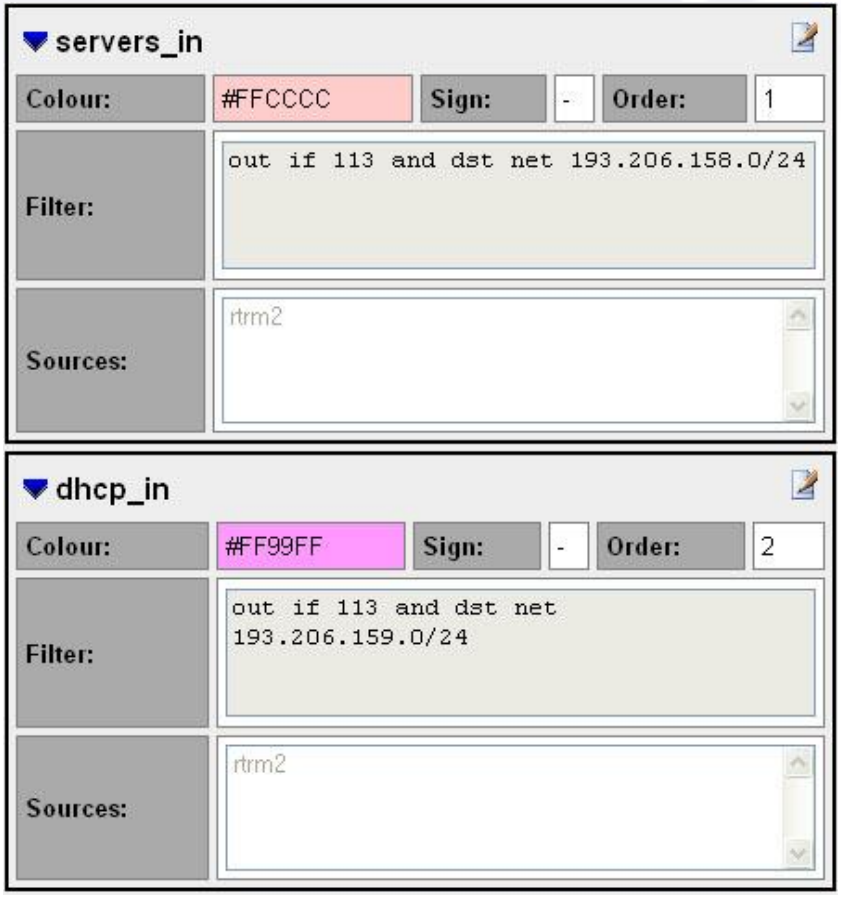


Statistics timeslot May 19 2009 - 14:10

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
dhcp_out	0.0 /s	0.0 /s	0.0 /s	0 /s	0 /s	0.0 /s	0.0 /s	0.0 /s	0 /s	0 /s	12.1 b/s	10.6 b/s	1.6 b/s	0 b/s	0 b/s
servers_out	3.7 /s	3.0 /s	0.6 /s	0.1 /s	0 /s	5.0 /s	3.8 /s	1.0 /s	0.1 /s	0 /s	30.2 kb/s	29.0 kb/s	1.1 kb/s	108.9 b/s	0 b/s
servers_in	2.9 /s	2.2 /s	0.6 /s	0.1 /s	0 /s	4.0 /s	2.7 /s	1.2 /s	0.1 /s	0 /s	13.2 kb/s	9.7 kb/s	3.4 kb/s	81.7 b/s	0 b/s
dhcp_in	0.1 /s	0.0 /s	0.0 /s	0 /s	0 /s	0.1 /s	0.0 /s	0.1 /s	0 /s	0 /s	951.5 b/s	103.1 b/s	848.4 b/s	0 b/s	0 b/s

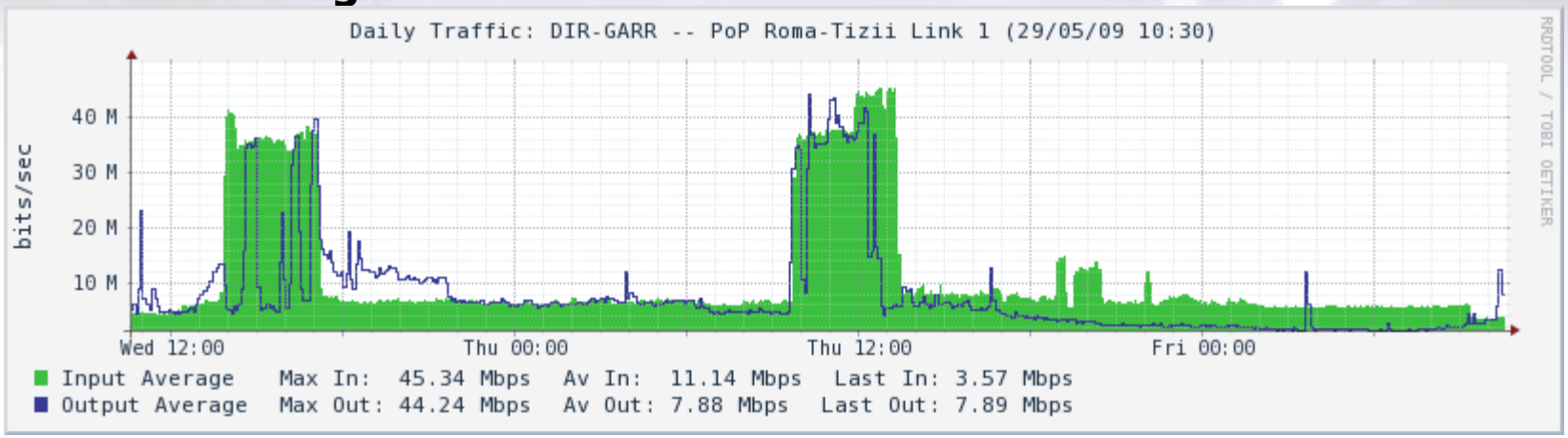
All None Display: Sum Rate

Esempio: filtri impostati

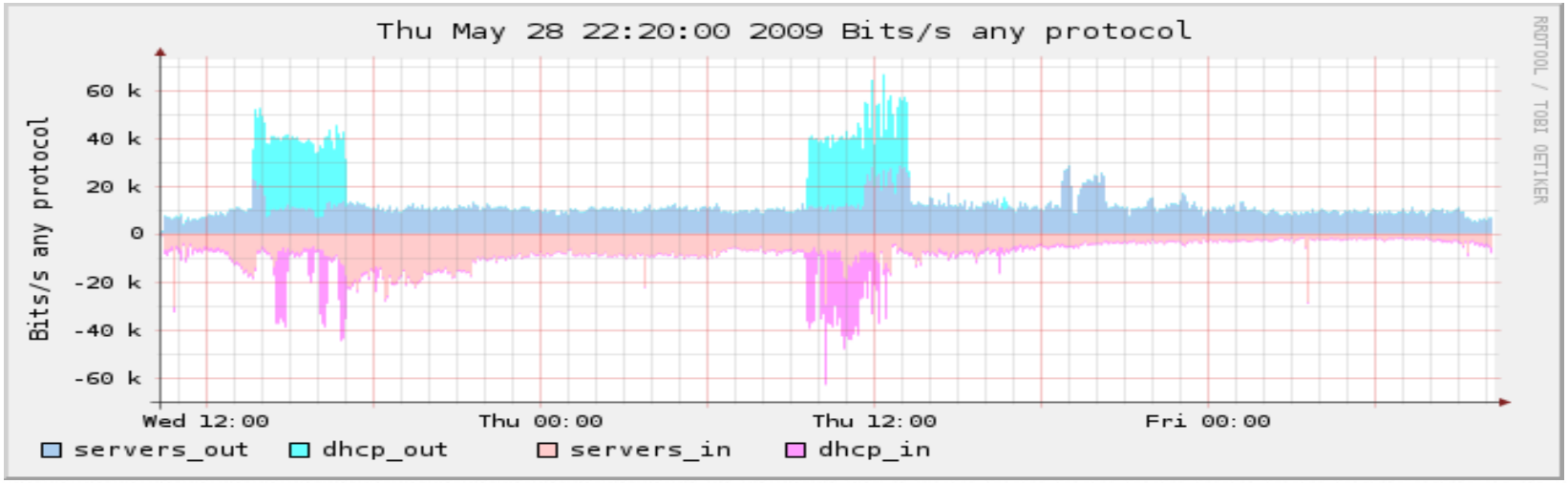


Monitoring Tradizionale vs Analisi dei flussi

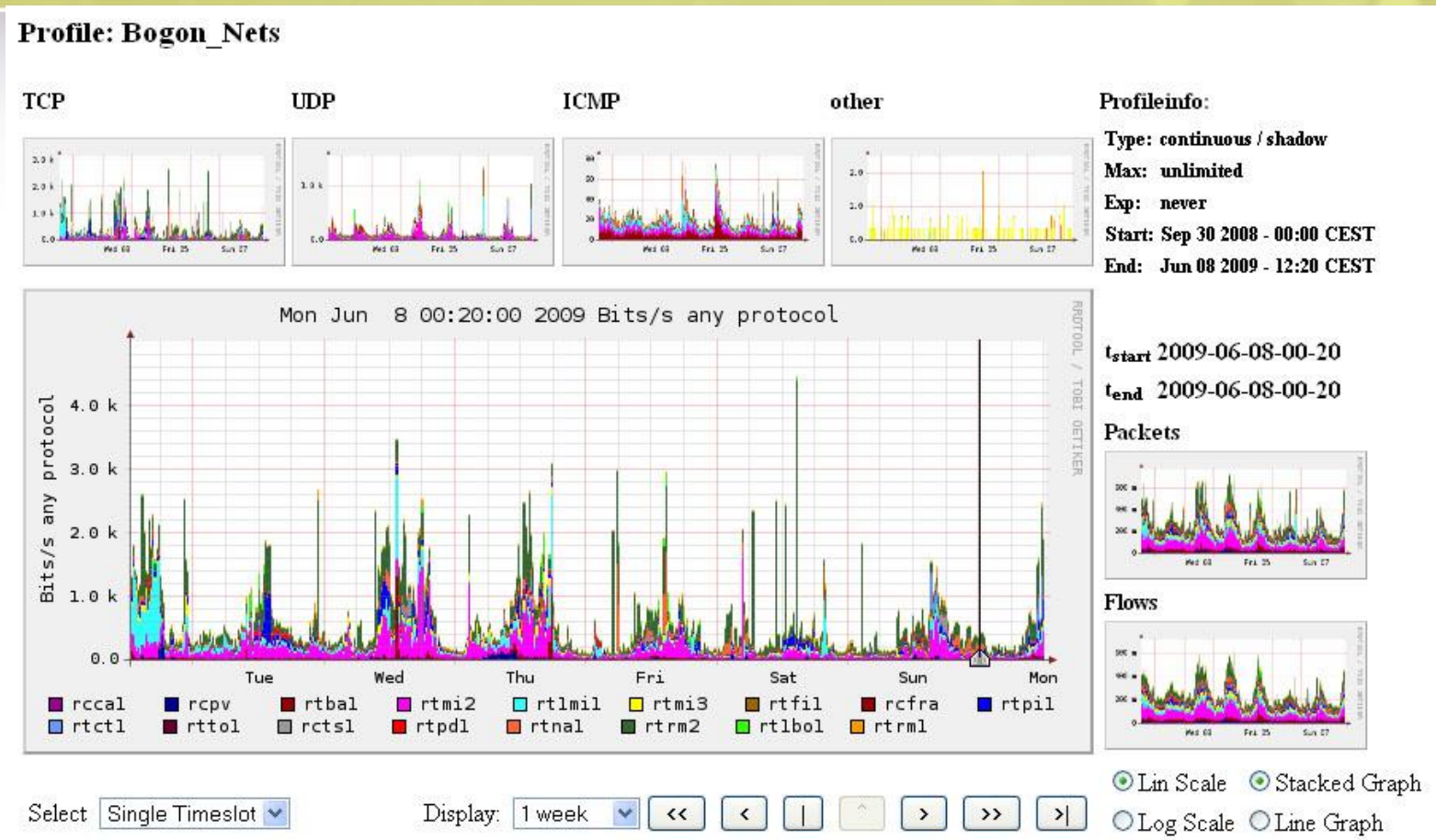
Monitoring Tradizionale



Analisi dei flussi (filtro per subnet)

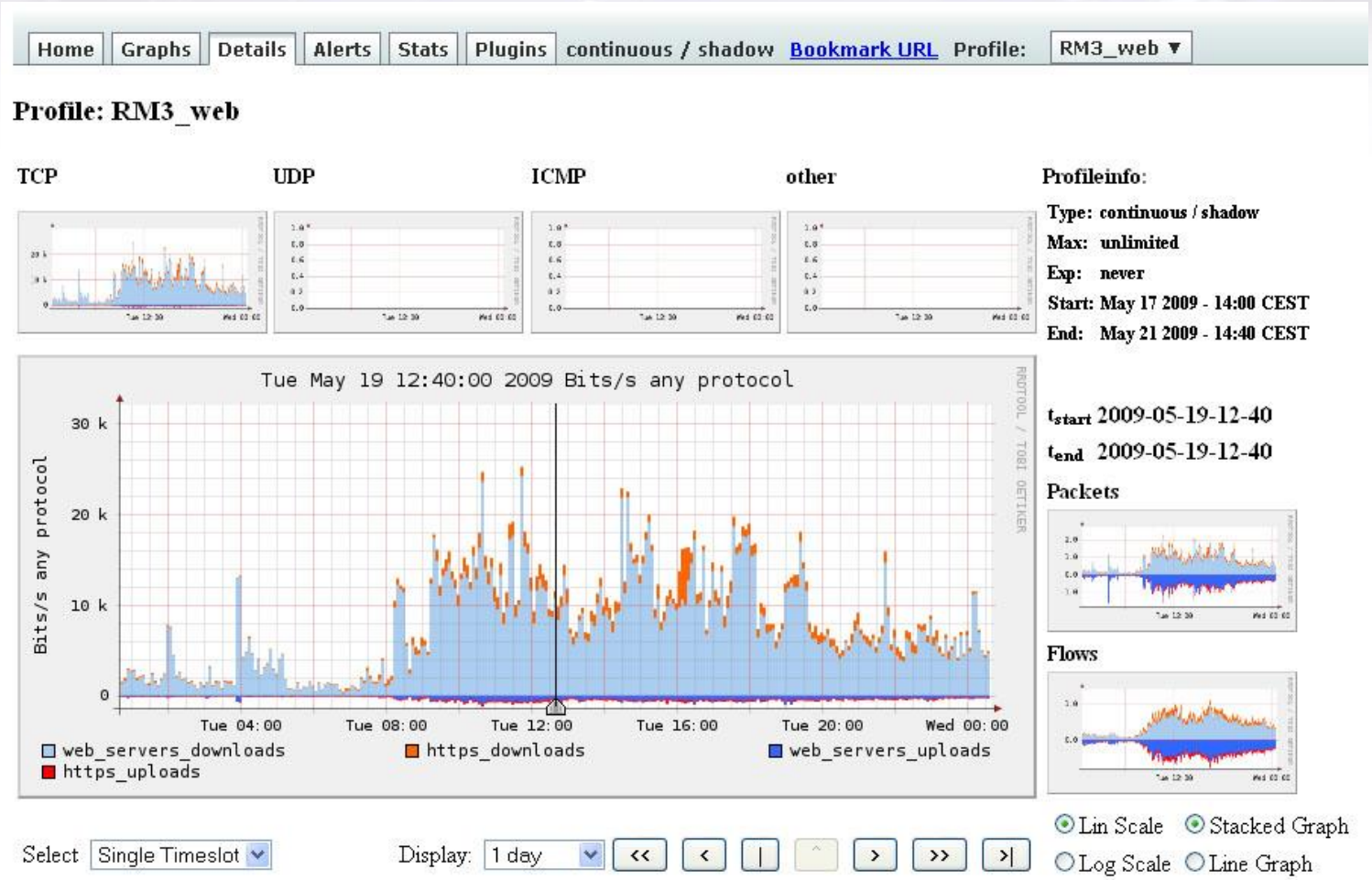


Bogon Network

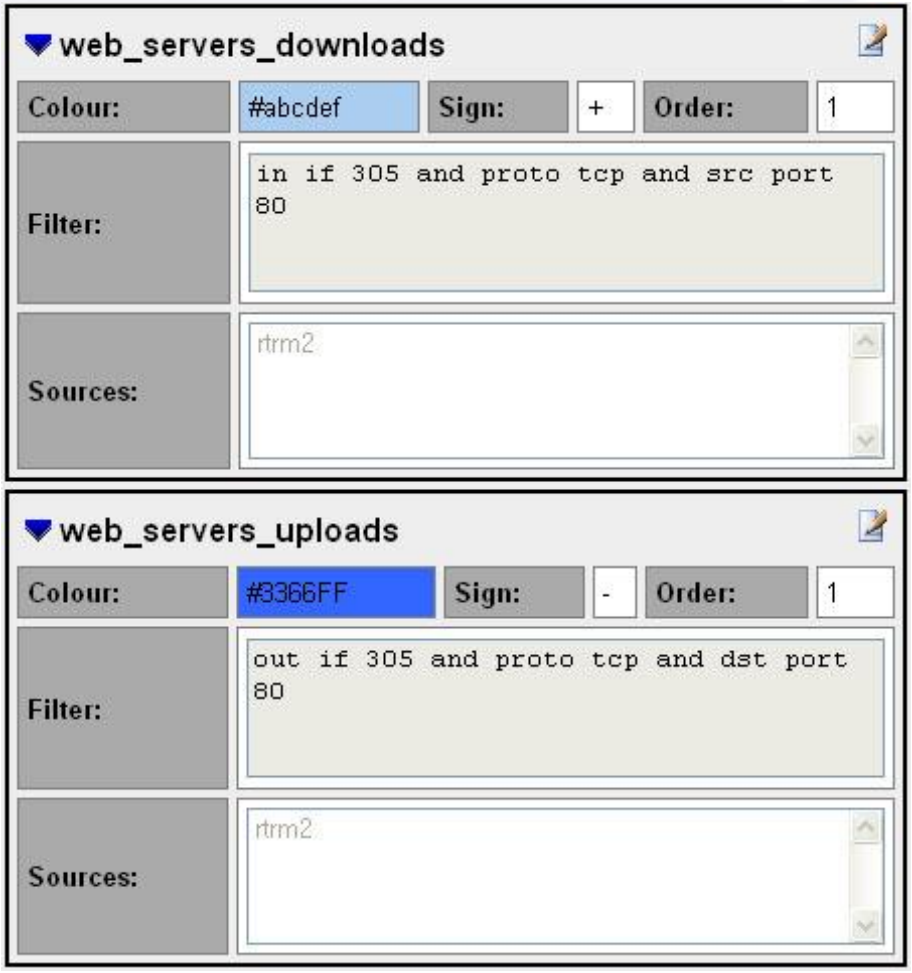


ICMP su Upstream Provider

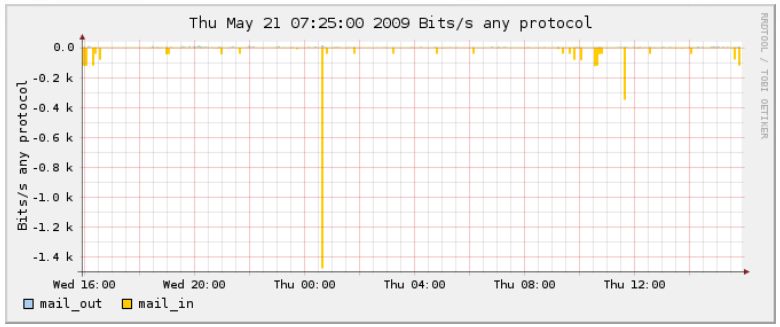
Web Server

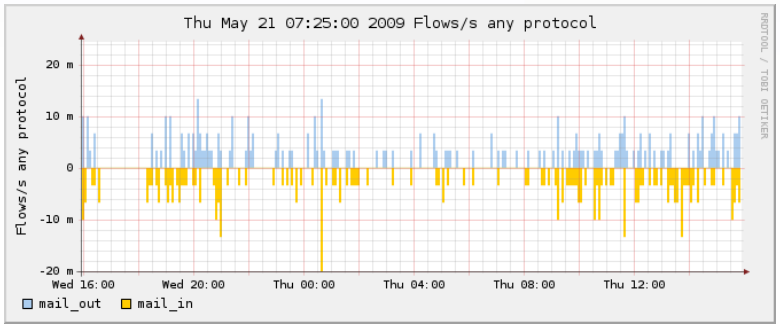

Home
Graphs
Details
Alerts
Stats
Plugins
continuous / shadow
Bookmark URL
Profile:
RM3_web
Profile: RM3_web
TCP
UDP
ICMP
other
Profileinfo:
Type: continuous / shadow
Max: unlimited
Exp: never
Start: May 17 2009 - 14:00 CEST
End: May 21 2009 - 14:40 CEST
Tue May 19 12:40:00 2009 Bits/s any protocol
Bits/s any protocol
30 k
20 k
10 k
0
Tue 04:00
Tue 08:00
Tue 12:00
Tue 16:00
Tue 20:00
Wed 00:00
web_servers_downloads
https_downloads
web_servers_uploads
https_uploads
tstart 2009-05-19-12-40
tend 2009-05-19-12-40
Packets
Flows
Select
Single Timeslot
Display:
1 day
Lin Scale
Stacked Graph
Log Scale
Line Graph

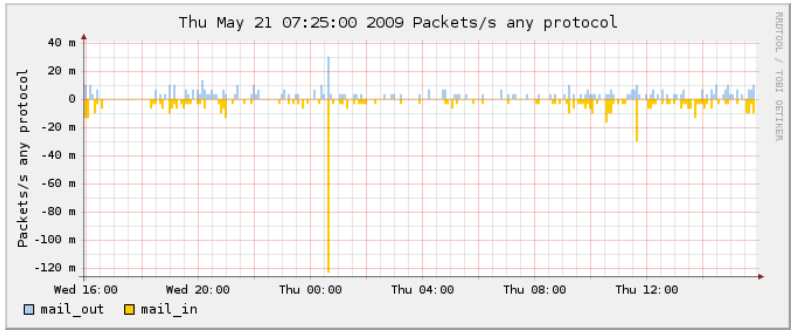
Web Server: Filtri impostati



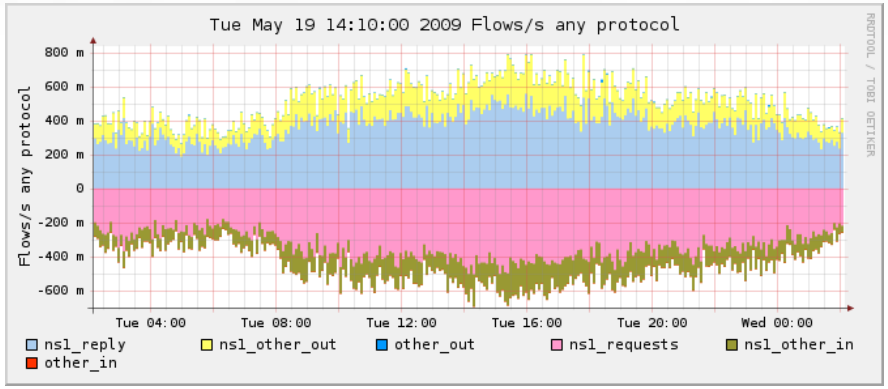
Mail Server

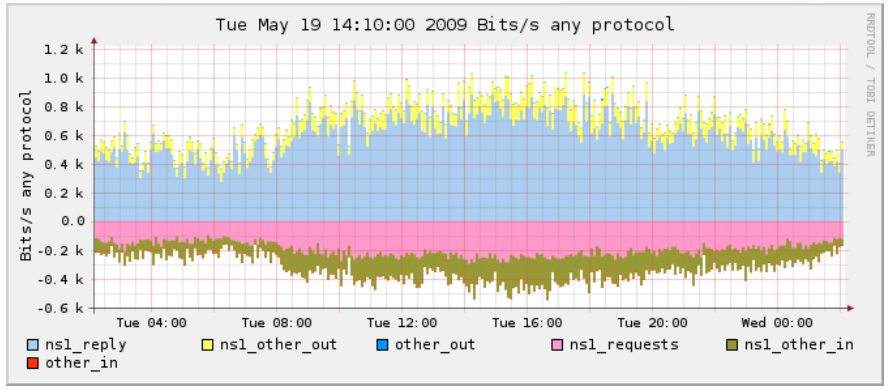

Thu May 21 07:25:00 2009 Bits/s any protocol
Bits/s any protocol
0.0
-0.2 k
-0.4 k
-0.6 k
-0.8 k
-1.0 k
-1.2 k
-1.4 k
Wed 16:00
Wed 20:00
Thu 00:00
Thu 04:00
Thu 08:00
Thu 12:00
mail_out
mail_in
RRDTOOL / TOBI OETIKER

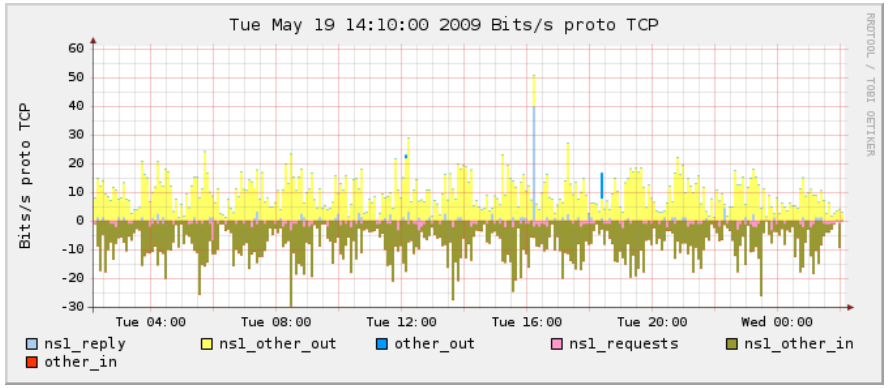

Thu May 21 07:25:00 2009 Flows/s any protocol
Flows/s any protocol
20 m
10 m
0
-10 m
-20 m
Wed 16:00
Wed 20:00
Thu 00:00
Thu 04:00
Thu 08:00
Thu 12:00
mail_out
mail_in
RRDTOOL / TOBI OETIKER

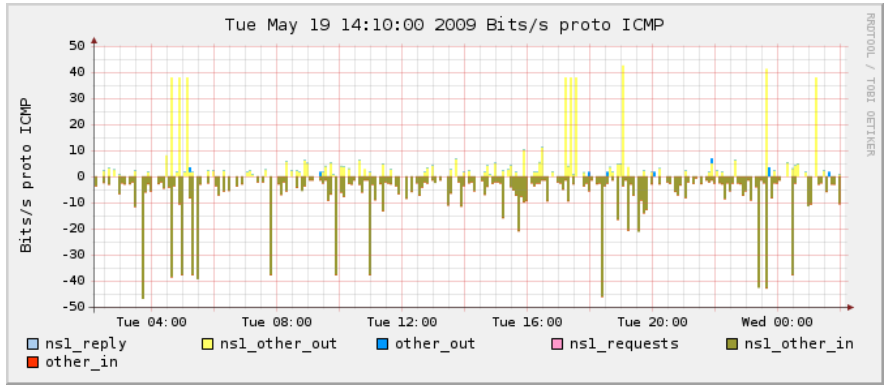

Thu May 21 07:25:00 2009 Packets/s any protocol
Packets/s any protocol
40 m
20 m
0
-20 m
-40 m
-60 m
-80 m
-100 m
-120 m
Wed 16:00
Wed 20:00
Thu 00:00
Thu 04:00
Thu 08:00
Thu 12:00
mail_out
mail_in
RRDTOOL / TOBI OETIKER

Name Server

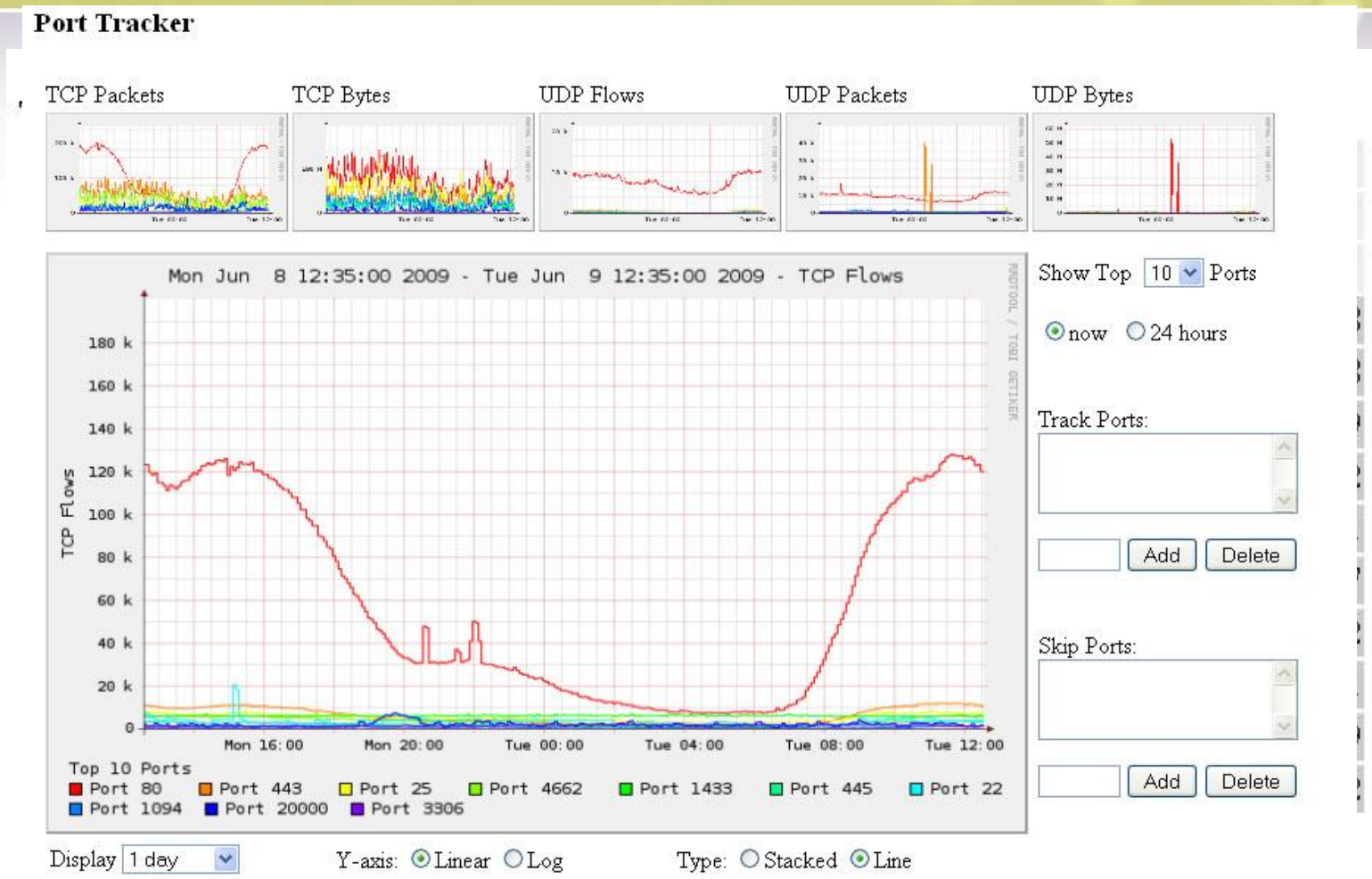

Tue May 19 14:10:00 2009 Flows/s any protocol
Flows/s any protocol
800 m
600 m
400 m
200 m
0
-200 m
-400 m
-600 m
Tue 04:00
Tue 08:00
Tue 12:00
Tue 16:00
Tue 20:00
Wed 00:00
nsl_reply
nsl_other_out
other_out
nsl_requests
nsl_other_in
other_in
RRDTOOL / TOBI OETIKER


Tue May 19 14:10:00 2009 Bits/s any protocol
Bits/s any protocol
1.2 k
1.0 k
0.8 k
0.6 k
0.4 k
0.2 k
0.0
-0.2 k
-0.4 k
-0.6 k
Tue 04:00
Tue 08:00
Tue 12:00
Tue 16:00
Tue 20:00
Wed 00:00
nsl_reply
nsl_other_out
other_out
nsl_requests
nsl_other_in
other_in
RRDTOOL / TOBI OETIKER

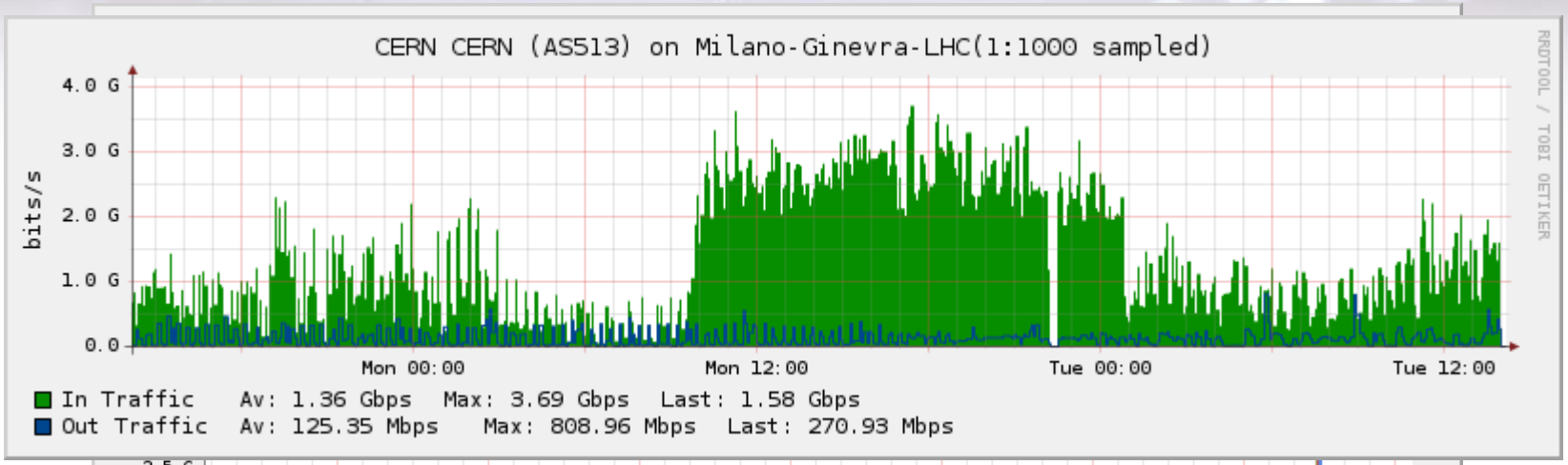

Tue May 19 14:10:00 2009 Bits/s proto TCP
Bits/s proto TCP
60
50
40
30
20
10
0
-10
-20
-30
Tue 04:00
Tue 08:00
Tue 12:00
Tue 16:00
Tue 20:00
Wed 00:00
nsl_reply
nsl_other_out
other_out
nsl_requests
nsl_other_in
other_in
RRDTOOL / TOBI OETIKER

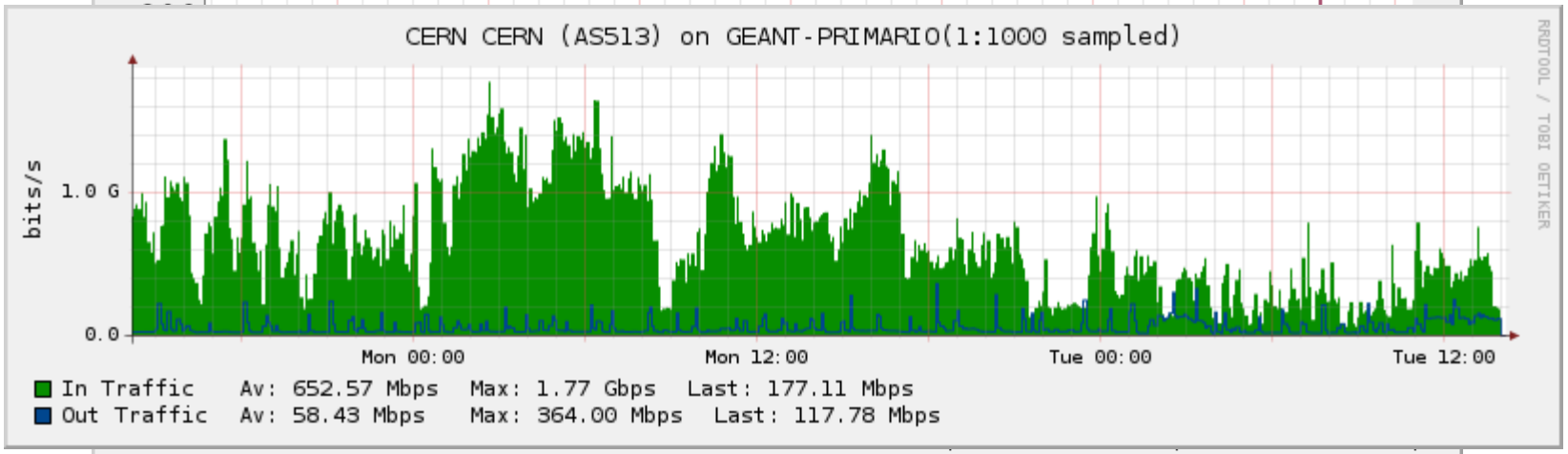

Tue May 19 14:10:00 2009 Bits/s proto ICMP
Bits/s proto ICMP
50
40
30
20
10
0
-10
-20
-30
-40
-50
Tue 04:00
Tue 08:00
Tue 12:00
Tue 16:00
Tue 20:00
Wed 00:00
nsl_reply
nsl_other_out
other_out
nsl_requests
nsl_other_in
other_in
RRDTOOL / TOBI OETIKER

Porte (plugin PortTracker)



Numeri AS (plugin AsTracker)

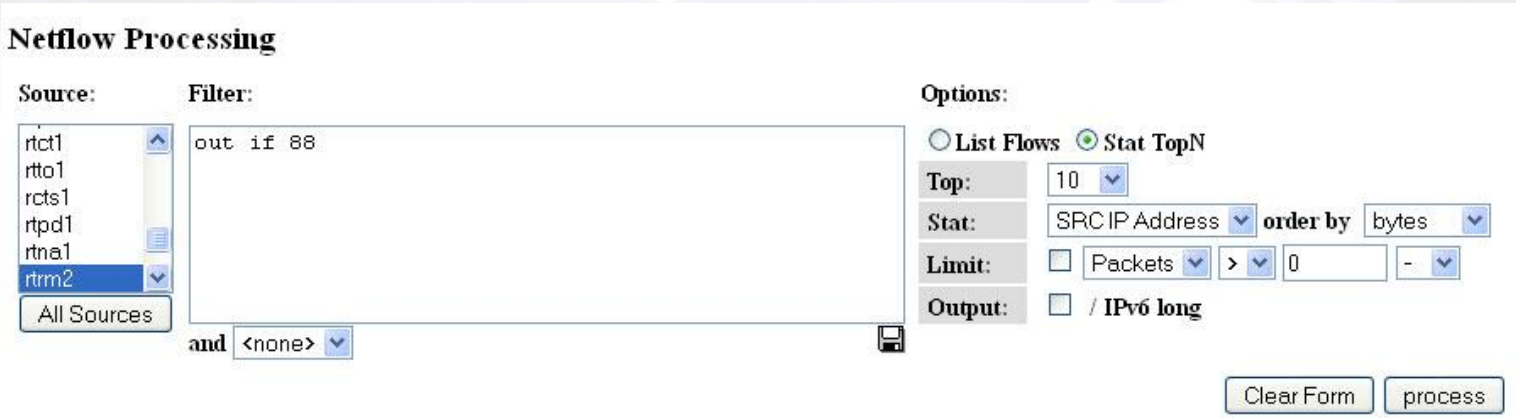




7)- ULTRALIGHT Out	Av:	58.38 Mbps	Max:	560.50 Mbps	Last: 44.85 kbps
8)- IN2P3 Out	Av:	37.21 Mbps	Max:	297.78 Mbps	Last: 2.94 Mbps
9)- BNL-AS Out	Av:	22.48 Mbps	Max:	486.40 Mbps	Last: 6.08 Mbps
10)- TRIUMF Out	Av:	21.19 Mbps	Max:	342.27 Mbps	Last: 4.77 Mbps

TopTalkers

IP sorgenti che hanno spedito piu' bytes in uscita sull'interfaccia 88 di rtrm2:



** nfdump -M /data/nfsen/profiles-data/live/rtrm2 -T -r 2009/06/09/nfcapd.200906090150 -n 10 -s srcip/bytes
Nfdump filter:
out if 88
Top 10 Src IP Addr ordered by bytes:

Date first seen	Duration	Proto	Src IP Addr	Flows	Packets	Bytes	pps	bps	bpp
2009-06-09 01:59:33.076	299.668	any	194.206.113.164	783	7790	10.7 M	25	300382	1444
2009-06-09 01:59:33.075	299.669	any	168.170.108.199	196	1010	1.4 M	3	38555	1429
2009-06-09 02:00:00.276	272.203	any	128.81.67.96	45	860	931808	3	27385	1083
2009-06-09 01:59:33.263	299.480	any	168.170.80.52	277	684	916303	2	24477	1339
2009-06-09 01:59:33.073	299.401	any	183.233.148.108	274	409	503907	1	13464	1232
2009-06-09 01:59:33.297	299.443	any	194.205.41.37	37	199	291483	0	7787	1464
2009-06-09 01:59:33.596	296.011	any	183.233.112.25	107	188	241836	0	6535	1286
2009-06-09 01:59:35.302	296.923	any	168.170.220.175	115	184	234215	0	6310	1272
2009-06-09 01:59:35.260	297.489	any	194.205.152.107	28	155	220376	0	5926	1421
2009-06-09 01:59:37.731	293.831	any	178.50.109.75	62	156	214522	0	5840	1375

Summary: total flows: 13583, total bytes: 24.3 M, total packets: 27850, avg bps: 680244, avg pps: 92, avg bpp: 914
Time window: 2009-06-09 01:59:32 - 2009-06-09 02:04:32
Total flows processed: 52740, Records skipped: 0, Bytes read: 2742528
Sys: 0.016s flows/second: 3296250.0 Wall: 0.012s flows/second: 4091543.8

TopTalkers

IP che hanno avuto il maggior troughout:

nfdev:~# ***nfdump -r /data/nfsen/profiles-data/live/rtrm2/2009/05/20/nfcapd.200905201000 -s ip/bps***

Top 10 IP Addr ordered by bps:

Date first seen	Duration	Proto	IP Addr	Flows	Packets	Bytes	pps	bps	bpp
2009-05-20 10:00:30.610	0.001	any	**150.51.86.103**	2	4	4540	3999	**34.6 M**	1135
2009-05-20 09:59:09.513	0.001	any	75.250.7.176	1	2	3000	1999	22.9 M	1500
2009-05-20 10:02:29.722	0.001	any	246.172.20.59	2	2	1540	1999	11.7 M	770
2009-05-20 10:03:29.710	0.001	any	226.82.105.197	2	2	1540	1999	11.7 M	770
2009-05-20 10:03:00.206	0.001	any	140.67.231.196	2	2	1460	1999	11.1 M	730
2009-05-20 10:03:00.206	0.001	any	139.119.70.252	2	2	1460	1999	11.1 M	730
2009-05-20 09:59:08.572	0.001	any	86.241.106.137	2	2	1322	1999	10.1 M	661
2009-05-20 10:03:19.627	0.003	any	225.136.245.127	3	3	3052	999	7.8 M	1017
2009-05-20 10:01:52.910	0.003	any	86.234.231.165	1	2	2984	666	7.6 M	1492
2009-05-20 10:01:52.910	0.003	any	224.190.13.154	1	2	2984	666	7.6 M	1492

Summary: total flows: 161250, total bytes: 185.8 M, total packets: 265150, avg bps: 4.1 M, avg pps: 736, avg bpp: 734
Time window: 2009-05-20 09:58:46 - 2009-05-20 10:04:46
Total flows processed: 161250, Records skipped: 0, Bytes read: 8385120
Sys: 0.108s flows/second: 1492972.6 Wall: 0.099s flows/second: 1620733.3

TopTalkers

IP che hanno scambiato piu' bytes:

nfdev:~$ ***nfdump -r /data/nfsen/profiles-data/live/rtrm2/2009/05/20/nfcapd.200905201000 -s ip/bytes***

Top 10 IP Addr ordered by bytes:

Date first seen	Duration	Proto	IP Addr	Flows	Packets	Bytes	pps	bps	bpp
2009-05-20 09:58:46.982	359.855	any	**225.207.115.198**	5200	16856	**15.2 M**	46	354798	946
2009-05-20 09:58:47.116	359.780	any	225.207.115.194	3845	12558	11.4 M	34	266840	955
2009-05-20 09:58:47.795	359.039	any	225.207.119.162	1784	3661	3.0 M	10	69643	853
2009-05-20 09:58:48.694	357.934	any	146.236.52.35	125	2464	2.5 M	6	59696	1083
2009-05-20 09:58:47.147	359.749	any	225.204.174.91	1514	2756	2.1 M	7	48689	794
2009-05-20 09:58:46.984	299.885	any	225.204.240.255	122	1392	2.0 M	4	55092	1483
2009-05-20 09:58:47.540	359.356	any	139.3.140.89	297	2007	1.9 M	5	44553	997
2009-05-20 09:58:47.444	359.261	any	224.20.182.157	1478	2433	1.7 M	6	40415	745
2009-05-20 09:58:46.984	299.885	any	159.127.154.129	51	1198	1.7 M	3	47938	1500
2009-05-20 10:02:02.549	17.876	any	225.18.67.245	16	1449	1.4 M	81	657509	1013

Summary: total flows: 161250, total bytes: 185.8 M, total packets: 265150, avg bps: 4.1 M, avg pps: 736, avg bpp: 734
Time window: 2009-05-20 09:58:46 - 2009-05-20 10:04:46
Total flows processed: 161250, Records skipped: 0, Bytes read: 8385120
Sys: 0.112s flows/second: 1439655.0 Wall: 0.109s flows/second: 1478828.7

TopTalkers

IP piu' informati…:

nfsen:~# ***nfdump -r /data/nfsen/profiles-data/live/rtrm2/2009/06/01/nfcapd.200906011520 -o 'fmt: %ts %td %da %byt %fl' "src host www.ansa.it"***

Resolving www.ansa.it ...

IPv4 address: 194.244.5.206 (194.244.5.206)

Date flow start	Duration	Dst IP Addr	Bytes	Flows
2009-06-01 15:19:46.354	0.000	**192.222.119.198**	**1500**	1
2009-06-01 15:19:47.490	0.000	**192.222.119.198**	**1500**	1
2009-06-01 15:19:49.490	0.000	**192.222.119.198**	**40**	1
2009-06-01 15:19:58.479	0.000	**194.206.33.67**	**1500**	1
2009-06-01 15:21:22.588	0.000	**194.206.5.154**	**347**	1
2009-06-01 15:21:42.761	0.000	**168.170.192.19**	**40**	1
2009-06-01 15:21:32.637	0.000	**168.170.195.141**	**40**	1
2009-06-01 15:21:02.716	0.000	**168.170.115.252**	**48**	1
2009-06-01 15:22:24.463	0.000	**195.80.138.242**	**48**	1
2009-06-01 15:22:58.452	0.000	**168.170.192.62**	**1500**	1

Summary: total flows: 10, total bytes: 6563, total packets: 10, avg bps: 273, avg pps: 0, avg bpp: 656

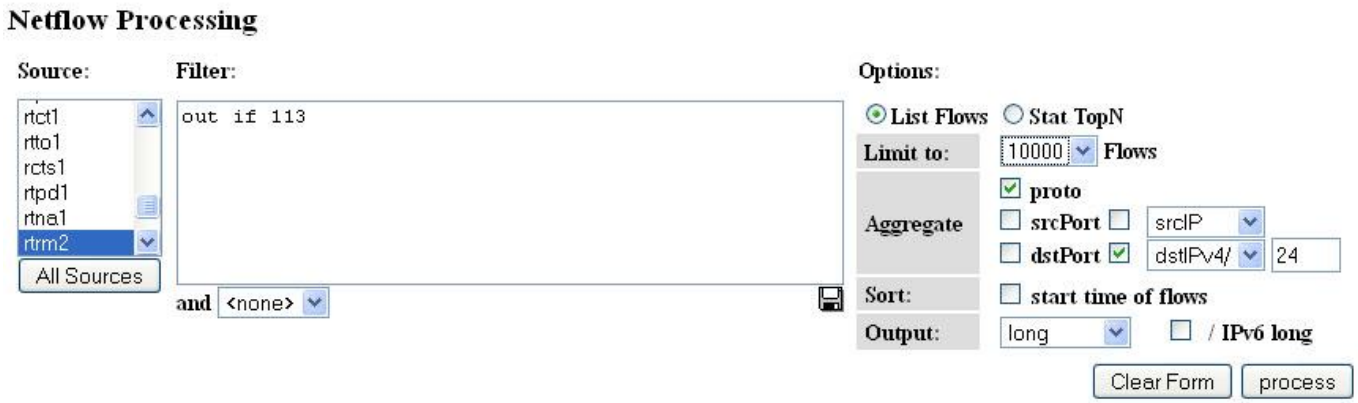
Time window: 2009-06-01 15:18:57 - 2009-06-01 15:24:57

Total flows processed: 131043, Records skipped: 0, Bytes read: 6814344

Sys: 0.028s flows/second: 4679940.0 Wall: 0.019s flows/second: 6680073.4

TopTalkers con aggregazione presonalizzata

Statistiche aggregate per netmask /24: e protocollo in uscita sulla interfaccia 113 del router rtrm2 (Direzione GARR):




```
** nfdump -M /data/nfsen/profiles-data/live/rtrm2  -T  -r 2009/06/09/nfcapd.200906090150 -a  -A proto,dstip4/24 -o long -c 10000
nfdump filter:
out if 113
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Flags Tos  Packets    Bytes Flows
2009-06-09 01:59:40.297   291.930 UDP            0.0.0.0:0     ->    193.206.158.0:0     ......   0      263    64401   111
2009-06-09 01:59:59.298   270.818 UDP            0.0.0.0:0     ->    193.206.159.0:0     ......   0        8    11552     7
2009-06-09 01:59:34.298   294.930 ICMP           0.0.0.0:0     ->    193.206.158.0:0.0   ......   0       14     1400    13
2009-06-09 01:59:33.287   293.520 TCP            0.0.0.0:0     ->    193.206.158.0:0     .AP.SF   0      139    30099   115
2009-06-09 02:01:09.888     0.321 TCP            0.0.0.0:0     ->    193.206.159.0:0     .A...F   0        2       80     2
Summary: total flows: 248, total bytes: 107532, total packets: 426, avg bps: 2877, avg pps: 1, avg bpp: 252
Time window: 2009-06-09 01:59:32 - 2009-06-09 02:04:32
Total flows processed: 52740, Records skipped: 0, Bytes read: 2742528
Sys: 0.008s flows/second: 6592500.0  Wall: 0.008s flows/second: 6464027.5
```

TopTalkers con aggregazione personalizzata

Sintassi (nfdump): “-s record/<misura> -A <campo/i da aggregare>”

Nota: alcune aggregazioni non sono supportate da nfsen

Top 10 AS sorgenti in ingresso sull’intefaccia avente interfaccia di ingresso con ifindex 88:

nfdev:~$ ***nfdump -r /data/nfsen/profiles-data/live/rtrm2/2009/05/20/nfcapd.200905201000 -s record/bytes -A srcAS -o 'fmt: %sas %byt' "in if 88"***

Aggregated flows 1477

Top 10 flows ordered by bytes:

Src AS	Bytes
15169	9.3 M
3356	5.6 M
22822	3.3 M
32934	1.6 M
6453	1.3 M
30058	934121
40824	900070
20473	823638
3320	624968
12322	622658

Summary: total flows: 30776, total bytes: 42.1 M, total packets: 50866, avg bps: 982085, avg pps: 141, avg bpp: 868

Time window: 2009-05-20 09:58:46 - 2009-05-20 10:04:46

Total flows processed: 161250, Records skipped: 0, Bytes read: 8385120

Sys: 0.036s flows/second: 4479042.2 Wall: 0.033s flows/second: 4796965.6

TopTalkers con aggregazione personalizzata

Le 15 coppie di subnet /24 che fanno piu' traffico:

nfdev:~$ ***nfdump -r /data/nfsen/profiles-data/live/rtrm2/2009/05/20/nfcapd.200905201400 -n 15 -A srcip4/24,dstip4/24 -s record/bytes***
Aggregated flows 97223
Top 15 flows ordered by bytes:

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2009-05-20 14:00:47.661	147.406	0	**181.236.167.0**:0	->	**190.145.223. 0**:0	1886	2.7 M	12
2009-05-20 14:00:47.661	115.573	0	**181.236.167.0**:0	->	**190.145.215.0**:0	1796	2.6 M	12
2009-05-20 13:59:55.152	61.697	0	**194.29.173.0**:0	->	**181.236.167.0**:0	1001	1.4 M	18
2009-05-20 14:02:46.055	123.094	0	**195.155.83.0**:0	->	**185.97.168.0**:0	692	1038000	9
2009-05-20 13:59:49.975	299.796	0	**198.72.64.0**:0	->	**169.113.129.0**:0	591	839092	63
2009-05-20 13:58:53.163	55.841	0	**181.236.165.0**:0	->	**188.121.158.0**:0	502	750432	21
2009-05-20 13:58:50.670	296.337	0	**168.170.152.0**:0	->	**73.131.20.0**:0	505	716592	12
2009-05-20 13:58:52.243	297.526	0	**194.206.113.0**:0	->	**192.225.109.0**:0	371	549080	10
2009-05-20 13:59:40.489	248.515	0	**194.206.113.0**:0	->	**170.122.12.0**:0	363	544500	7
2009-05-20 14:01:17.925	127.824	0	**95.64.160.0**:0	->	**188.80.192.0**:0	360	540000	6
2009-05-20 13:59:52.428	296.694	0	**194.201.138.0**:0	->	**194.205.140.0**:0	362	539781	59
2009-05-20 13:58:50.328	297.970	0	**194.206.113.0**:0	->	**79.40.54.0**:0	337	502804	8
2009-05-20 13:58:51.130	298.494	0	**194.206.113.0**:0	->	**81.201.82.0**:0	322	483000	19
2009-05-20 13:58:53.064	296.526	0	**194.206.113.0**:0	->	**216.138.183.0**:0	331	482598	10
2009-05-20 13:59:13.108	276.661	0	**194.206.113.0**:0	->	**95.186.140.0**:0	328	471493	17

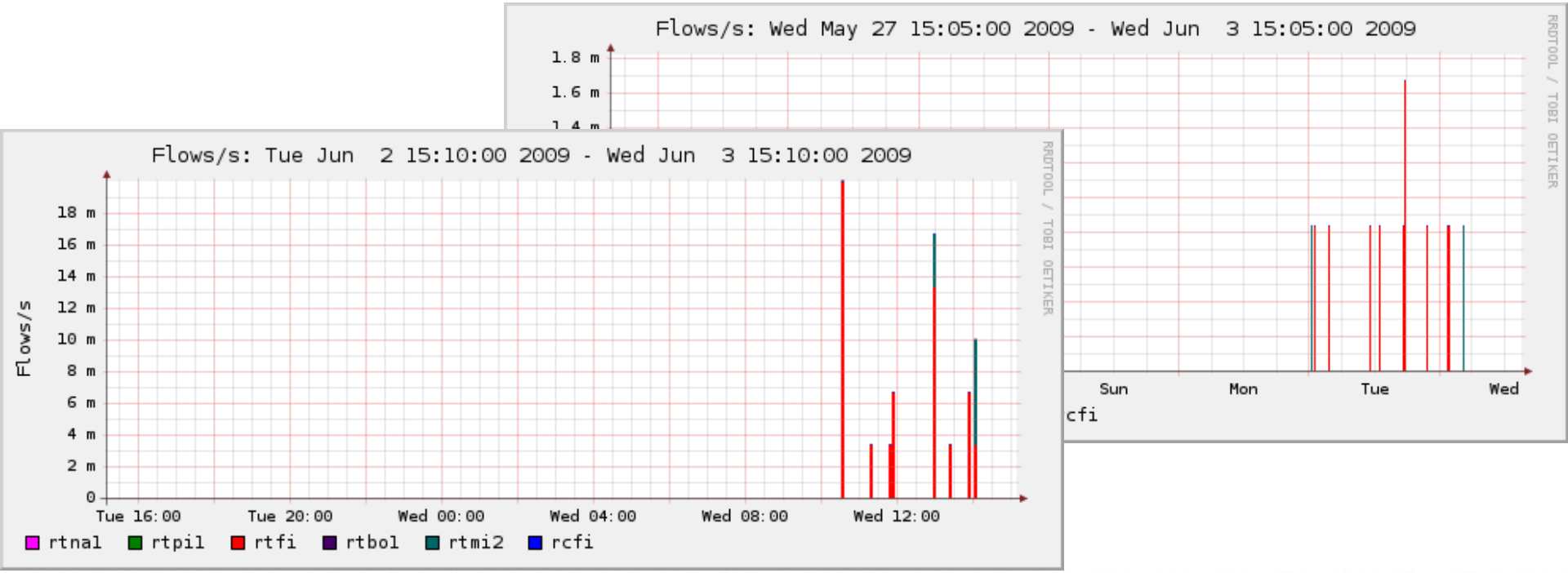
Summary: total flows: 185341, total bytes: 217.8 M, total packets: 308936, avg bps: 4.8 M, avg pps: 858, avg bpp: 739
Time window: 2009-05-20 13:58:49 - 2009-05-20 14:04:49
Total flows processed: 185341, Records skipped: 0, Bytes read: 9637876
Sys: 0.116s flows/second: 1597684.6 Wall: 0.145s flows/second: 1270860.3

Analisi incidenti di sicurezza

- Segnalazione esterna di macchina che fa traffico anomalo
- Controllo del traffico sul router a quel timeslot
- Tracciamento di ip spoofati in caso di DDoS
- Come procedere in…..
  - Caso di PHISHING
    - controllo delle macchine che gli si sono collegate
  - Caso di Probe/Scan
    - controllo di cosa fa la macchina nel tempo precedente al timeslot
  - Caso di SPAM
    - controllo delle connesstioni sulla TCP/25
  - Caso di DoS
    - controllo dei picchi e dei flussi entranti/uscenti dalla macchina e dal router nelle vicinanze di quel timeslot

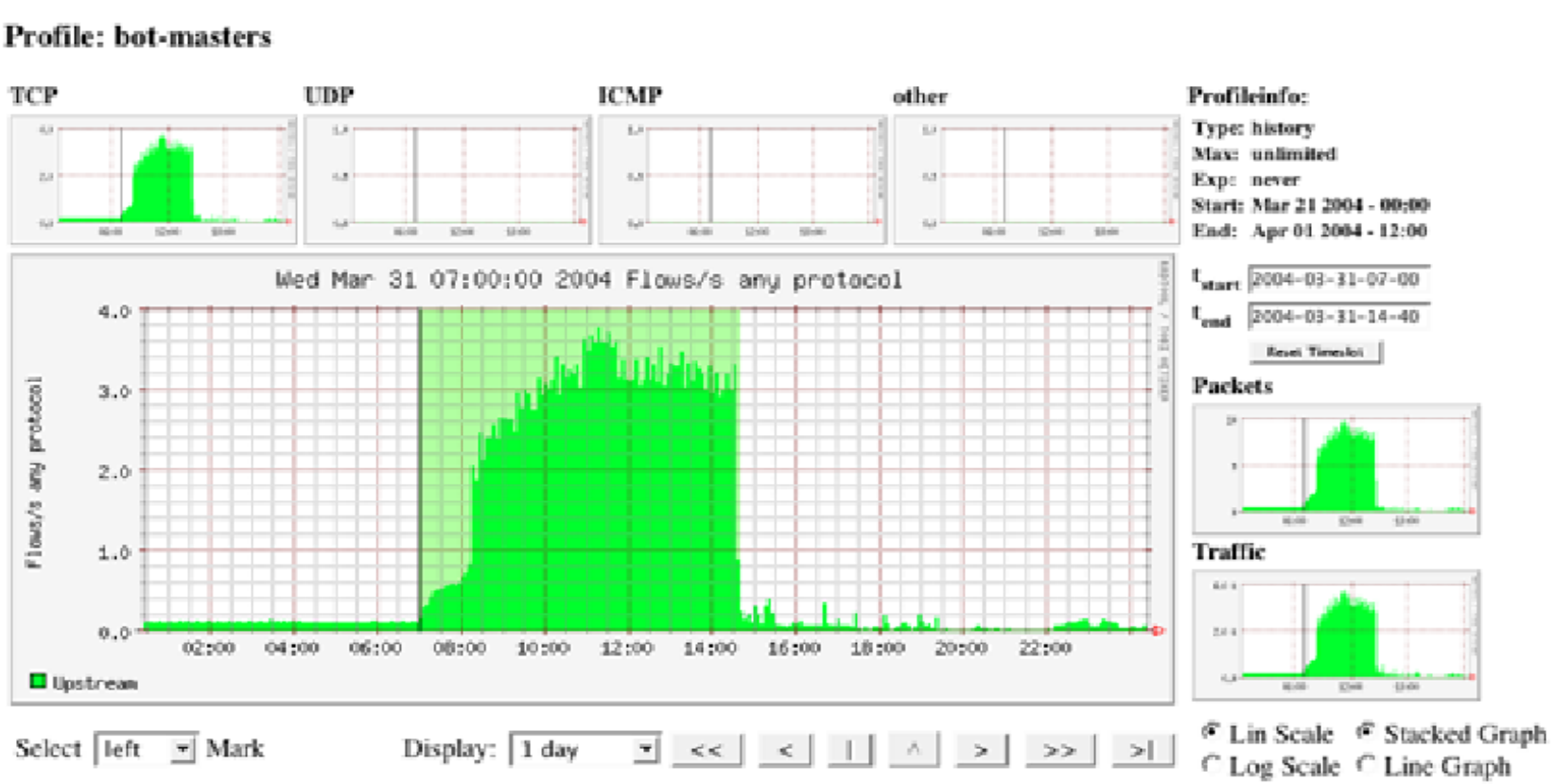
Tracciamento degli Host (1/2)

- Segnalazione di un host che fa traffico malevolo
- Profilatura dell'host a partire da qualche giorno o settimana prima della segnalazione tramite shadow profile
- Controllo continuo del traffico della macchina



Tracciamento degli Host (2/2)

- Profilatura di un host compromesso



Identificazione di traffico “malevolo”

Esempio (Presunti IP sorgenti di scanning e porte bersaglio):

nfdev:~$ ***nfdump -r /data/nfsen/profiles-data/live/router1/2009/05/20/nfcapd.200905201400 –A srcip,dstport -s record/packets "not proto icmp and bytes < 100 and bpp < 100 and packets < 5 and not port 80 and not port 53 and not port 110 and not port 123 and not port 22"***

Aggregated flows 30404
Top 10 flows ordered by packets:

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2009-05-20 13:58:56.362	289.563	0	**87.177.37.47**:0	->	0.0.0.0:**1080**	185	7614	182
2009-05-20 13:58:50.298	296.047	0	**195.155.76.158**:0	->	0.0.0.0:**443**	66	2912	66
2009-05-20 13:59:52.617	282.893	0	**168.170.104.98**:0	->	0.0.0.0:**445**	54	2584	54
2009-05-20 13:58:53.117	295.026	0	**212.238.91.31**:0	->	0.0.0.0:**445**	47	2256	45
2009-05-20 13:58:51.228	292.875	0	**168.170.128.34**:0	->	0.0.0.0:**445**	45	2160	45
2009-05-20 13:58:51.678	292.002	0	**168.173.164.192**:0	->	0.0.0.0:**445**	43	1995	43
2009-05-20 13:58:52.974	289.299	0	**169.113.129.189**:0	->	0.0.0.0:**445**	42	2016	42
2009-05-20 13:59:51.397	295.530	0	**168.170.170.9**:0	->	0.0.0.0:**445**	42	2016	42
2009-05-20 13:58:51.872	296.238	0	**168.170.186.180**:0	->	0.0.0.0:**445**	38	1824	38
2009-05-20 13:58:50.895	287.792	0	**168.170.118.100**:0	->	0.0.0.0:**445**	36	1720	35

Summary: total flows: 41946, total bytes: 2.1 M, total packets: 45408, avg bps: 47839, avg pps: 126, avg bpp: 47
Time window: 2009-05-20 13:58:49 - 2009-05-20 14:04:49
Total flows processed: 185341, Records skipped: 0, Bytes read: 9637876
Sys: 0.128s flows/second: 1447897.4 Wall: 0.682s flows/second: 271443.8

Identificazione di traffico “malevolo”

Esempio synflood generato da GARR:

Traffico TCP con il solo flag SYN settato con #pacchetti > 12Mpkts e volume di traffico generato > 2GBytes

nino@nf:~# nfdump -M /data/nfsen/profiles-data/live/rrm2:rmi2:rx1mi1:rx2mi1 –R 2016/04/12/nfcapd.201604120700:2016/04/12/nfcapd.201604120800 -s record/packets -A srcnet,srcmask -l **12000000** -L **2G** -n 10 -o 'fmt:%sn %bps' **"((flags S and not flags AFRPU**))and (src as 137 or (src as > 64511 and src as < 65535) or as 24869 or as 8978 or as 35110 or as 42165 or as 16004 or as 47630 or as 2597 or as 50112 or as 51708 or as 50507 or as 29609 or as 197440 or as 49976 or as 31638 or as 199342 or as 2596)«

Byte limit: > 2000000000 bytes

Packet limit: > 12000000 packets

Src Network	bps	Bytes
151.97.0.0/16	**58.1 M**	**28.3G**

Identificazione di traffico “malevolo”

… continua: Chi sono i target dell’attacco?

nino@nf:~# NET="**151.97.0.0/16**"; nfdump -M /data/nfsen/profiles-data/live/rrm2:rmi1:rmi2:rbo1:rx1mi2 -R nfcapd.201604120700:nfcapd.201604120800 -s record/packets -A srcnet,srcmask,dstas,dstip,dstport -n 8 -o 'fmt:%sn %dap %das %bps %byt %pkt' -q "((**flags S and not flags AFRPU**)) and src net **${NET}**"

151.97.0.0/16	**180.163.189.253:3602**	**4812**	**10.6 M**	**624.5 M**	**13.0 M**
151.97.0.0/16	180.163.189.253:3600	4812	10.2 M	595.2 M	12.4 M
151.97.0.0/16	180.163.189.253:3601	4812	10.2 M	594.8 M	12.4 M
151.97.0.0/16	218.244.157.237:5507	37963	4.7 M	1.6 G	12.0 M
151.97.0.0/16	112.74.65.100:3724	37963	5.7 M	1.6 G	11.9 M
151.97.0.0/16	112.83.192.34:30625	4837	3.2 M	1.1 G	11.5 M
151.97.0.0/16	101.200.169.114:5009	37963	39.6 M	409.3 M	8.5 M
151.97.0.0/16	61.153.111.110:7006	4134	3.7 M	1.0 G	8.0 M

nino@nf:~# whois -h whois.cymru.com as4812
AS Name
CHINANET-SH-AP China Telecom (Group), CN

Identificazione di traffico “malevolo”

Top5 talkers per # flussi:

nino@nf:~# nfdump -M /data/nfsen/profiles-data/live/**rrm2:rmi2:rx1mi1:rx1mi2** -r nfcapd.201604122315 **-s ip/flows -n 5**
Top 5 IP Addr ordered by flows:

Date first seen	Duration	Proto	IP Addr	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
2016-04-12 23:09:20.770	585.280	any	**147.162.157.191**	11744(3.4)	26.4 M(1.2)	35.3 G(1.4)	45041	482.8 M	1339
2016-04-12 19:30:00.250	13796.640	any	90.147.160.69	6418(1.9)	42.2 M(1.9)	43.7 G(1.7)	3058	25.4 M	1036
2016-04-12 23:13:58.430	360.520	any	212.189.205.65	5800(1.7)	75.9 M(3.4)	92.1 G(3.6)	210501	2.0 G	1213
2016-04-12 23:13:59.370	358.550	any	212.189.129.249	4309(1.3)	4.5 M(0.2)	3.4 G(0.1)	12556	75.2 M	748
2016-04-12 22:52:10.230	1665.510	any	31.13.86.4	3951(1.1)	6.6 M(0.3)	5.3 G(0.2)	3933	25.5 M	810

Summary: total flows: 344198, total bytes: 2.5 T, total packets: 2.2 G, avg bps: 10.5 M, avg pps: 1170, avg bpp: 1126
Time window: 2016-03-21 17:59:25 - 2016-04-12 23:19:58
Total flows processed: 344198, Blocks skipped: 0, Bytes read: 35081160
Sys: 0.256s flows/second: 1344444.7 Wall: 10.589s flows/second: 32504.1

Calcolo le sorgenti differenti:
nino@nf:~# nfdump -M /data/nfsen/profiles-data/live/rrm2:rmi2:rx1mi1:rx1mi2 -n 5000000 -r nfcapd.201604122315
-s record/flows -q -A srcip -N -o 'fmt:%sa %fl %pkt %byt'
"dst ip **147.162.157.191** and (proto UDP or (proto TCP and (flags S or flags R)) or proto ICMP)" |**wc -l**

= 3737

Identificazione di traffico “malevolo”

Tipologia di traffico di attacco:

nino@nf:~# nfdump -M /data/nfsen/profiles-data/live/rrm2:rmi2:rx1mi1:rx1mi2 -n 50 -r nfcapd.201604122315
"**dst ip 147.162.157.191 and (proto UDP or (proto TCP and (flags S or flags R)) or proto ICMP)**"

Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2016-04-12 23:14:00.420	0.000	UDP	111.63.22.42:13652	->	147.162.157.191:80	1000	1.5 M	1
2016-04-12 23:14:00.290	0.000	**UDP**	**103.53.198.237:53**	->	**147.162.157.191:4444**	1000	1.5 M	1
2016-04-12 23:14:00.280	0.000	**UDP**	**211.55.92.30:58774**	**->**	**147.162.157.191:80**	1000	1.5 M	1
2016-04-12 23:14:00.270	0.000	UDP	**97.105.14.101:53**	->	147.162.157.191:4444	1000	1.5 M	1
2016-04-12 23:14:00.250	0.000	UDP	85.23.206.27:58449	->	147.162.157.191:80	1000	1.5 M	1
2016-04-12 23:14:00.250	0.000	UDP	96.36.11.210:53	->	147.162.157.191:4444	1000	1.5 M	1
2016-04-12 23:14:00.250	0.000	UDP	**95.68.241.194:53**	->	147.162.157.191:4444	1000	1.5 M	1
2016-04-12 23:14:00.250	0.000	UDP	**95.171.199.168:53**	->	147.162.157.191:4444	1000	1.5 M	1
2016-04-12 23:14:00.230	0.000	UDP	103.193.0.39:53	->	147.162.157.191:4444	1000	1.5 M	1
2016-04-12 23:14:00.210	0.000	UDP	**27.131.12.2:53**	->	147.162.157.191:58323	1000	65000	1
2016-04-12 23:14:00.190	0.000	UDP	85.23.206.27:58438	->	147.162.157.191:80	1000	1.5 M	1
2016-04-12 23:14:00.170	0.000	UDP	114.159.95.56:53	->	147.162.157.191:4444	1000	1.5 M	1

Multidimensionale: open-resolver + altri attachi

Identificazione di traffico “malevolo”

GARR NOC DDoS attack monitor

DDOS attack monitor

Last DDOS attacks report

N	target	target site	start	end	int	bytes	bps	flows	connections
1	147.162.157.191	UNI-Padova	00:10 13/04/2016	00:15 13/04/2016	2	90,66 GB	912,23 Mbps	37817	15650
2	147.162.157.191	UNI-Padova	22:05 12/04/2016	22:05 12/04/2016	1	20,12 GB	447,96 Mbps	14590	9994
3	193.206.131.122	RMIS084008 - IIS Caffè - Roma	16:25 11/04/2016	16:30 11/04/2016	2	7,35 GB	120,27 Mbps	141953	141874
4	138.41.5.42	NATF05000N - ITIS Giordani-Striano - Napoli	11:20 11/04/2016	11:40 11/04/2016	5	30,03 GB	158,30 Mbps	742392	742159
5	192.107.70.102	ENEA - Portici CRESCO (NA)	20:55 10/04/2016	20:55 10/04/2016	1	23,89 GB	1,61 Gbps	14185	11884

Identificazione di traffico “malevolo”

SSH scan

nfdev:~$ ***nfdump -r /data/nfsen/profiles-data/live/router1/2009/05/20/nfcapd.200905201400 –A srcip -s record/packets "proto TCP and dport 22 and flags S and not flags AFRPU"***

2009-06-04 16:59:54.057 **xxx.80.208.239**:35823 -> yyy.200.199.203:22 ....S. 1 60 1
2009-06-04 16:59:39.123 **xxx.80.208.23**9:44577 -> yyy.200.195.226:22 ....S. 1 60 1
2009-06-04 17:01:54.084 **xxx.80.208.239**:53769 -> yyy.200.237.133:22 ....S. 1 60 1
2009-06-04 17:01:31.024 **xxx.80.208.239**:60829 -> yyy.200.232.39:22 ....S. 1 60 1
2009-06-04 16:59:53.279 **xxx.80.208.239**:53731 -> yyy.200.199.108:22 ....S. 1 60 1
2009-06-04 17:00:28.348 **xxx.80.208.239**:34654 -> yyy.200.211.104:22 ....S. 1 60 1
2009-06-04 16:59:31.080 **xxx.80.208.239**:54641 -> yyy.200.194.28:22 ....S. 1 60 1
2009-06-04 16:59:18.316 **xxx.80.208.239**:34426 -> yyy.200.189.162:22 ....S. 1 60 1
2009-06-04 17:00:34.093 **xxx.80.208.239**:51640 -> yyy.200.212.76:22 ....S. 1 60 1
2009-06-04 16:58:54.459 **xxx.80.208.239**:58954 -> yyy.200.182.14:22 ....S. 1 60 1
2009-06-04 16:59:35.459 **xxx.80.208.239**:58471 -> yyy.200.195.5:22 ....S. 1 60 1
2009-06-04 17:01:01.080 **xxx.80.208.239**:52688 -> yyy.200.222.197:22 ....S. 1 60 1

Summary: total flows: 105, total bytes: 6300, total packets: 105, avg bps: 214, avg pps: 0, avg bpp: 60
Time window: 2009-06-04 16:58:17 - 2009-06-04 17:05:07
Total flows processed: 565374, Records skipped: 0, Bytes read: 29400036
Sys: 0.068s flows/second: 8313834.5 Wall: 0.064s flows/second: 8823628.6

Netflow sulla LAN/NAT

- switch (Sflow)
  - Open vSwitch
- server (nprobe)
  - monitoring NAT, firewall, server

Sflow: caratteristiche

- Il protocollo Sflow, oltre a supportare i protocolli IP/ICMP/UDP/TCP, supporta anche:
  - Packet headers
  - Ethernet/802.3
  - IP/ICMP/UDP/TCP
  - IPX Appletalk
- Nel layer 2 supporta le interfaccia di ingresso e uscita ma anche:
  - Priorita' 802.1p Ingresso/Uscita
  - VLAN 802.1Q Ingresso/Uscita
- Configurabile via SNMP
- Piattaforme HW: 3com, Alcatel-Lucent, Extreme networks, Force10 networks, HP, Juniper (EX series),

Switch (Sflow): Configurazione

- Netflow su cisco (solo su serie 4500/6500)

```
Router(config-if)# mls flow ip destination-source
Router(config-if)# mls nde src_address 10.1.1.37 version 8
Router(config-if)# interface vlan1
Router(config-if)# ip route-cache flow
Router(config-if)# interface fastethernet 3/2
Router(config-if)# ip address 10.200.8.2 255.255.255.0
Router(config-if)# ip route-cache flow
Router(config-if)# ip flow-export source vlan1
Router(config-if)# ip flow-export version 5
Router(config)# ip flow-export destination 10.1.1.99 9999
```

- Sflow su Juniper switch

```
[edit protocols sflow]
user@switch#    set collector <ip-address>
                set collector udp-port <port-number>
                set interfaces interface-name
                set polling-interval seconds
                set sample-rate number
```

Open vSwitch (sflow)

ovs-vsctl -- --id=@sflow create sflow agent=${AGENT_IP} target=\"${COLLECTOR_IP}:${COLLECTOR_PORT}\" header=${HEADER_BYTES} sampling=${SAMPLING_N} polling=${POLLING_SECS} -- set bridge ${BRIDGE}

- AGENT_IP = interfaccia verso il collettore
- COLLECTOR_IP/PORT = indirizzo/porta collettore
- HEADER_BYTES = bytes di header
- SAMPLING_N = sampling rate
- POLLING_SECS = intervallo di campionatura
- BRIDGE = nome bridge

Open vSwitch (netflow)

ovs-vsctl -- set bridge ovsbr1 netflow=@nf -- --id=@nf create NetFlow targets=\"${COLLECTOR_IP}:${COLLECTOR_PORT}\" \ active-timeout=${TIMEOUT}

- COLLECTOR_IP/PORT=indirizzo/porta collettore netflow
- TIMEOUT= timeout flussi

Server/Linux Firewall

- **Scopo:**
  - Esportazione dei flussi su sistemi linux (es. firewall/NAT)
  - Controllo del traffico interno al NAT o di singola macchine

- **Come:**
  - Utilizzando un'applicazione che crea pacchetti NetFlow analizzando i pacchetti entranti e uscenti dalle interfacce in modalita' promiscua

Server/Linux Firewall

- **Cosa:**
  - nProbe
  - flowprobe
  - Ipt-netflow (NetFlow iptables module)
  - Fprobe-ulog

- **Architettura:**

La macchina linux con il probe installato agisce come un router, esportando i pacchetti NetFlow verso il collector (nel nostro caso sempre `nfcapd`)

Abbiamo scelto e testato **nProbe** per le caratteristiche di performances, stabilita' e affidabilita'

E' opensource per gli enti accademici e di ricerca

Installazione nProbe e collector 1/2

- Sulla macchina linux che fa NAT
  - Download nProbe
  - tar -zxvf nprobe-XXX.tgz
  - ./autogen.sh && make && make install
  - Comandi d'esportazione:
    - **nprobe -G -i eth0 -n localhost:10000**
    - **nprobe -G -i eth1 -n localhost:10001**

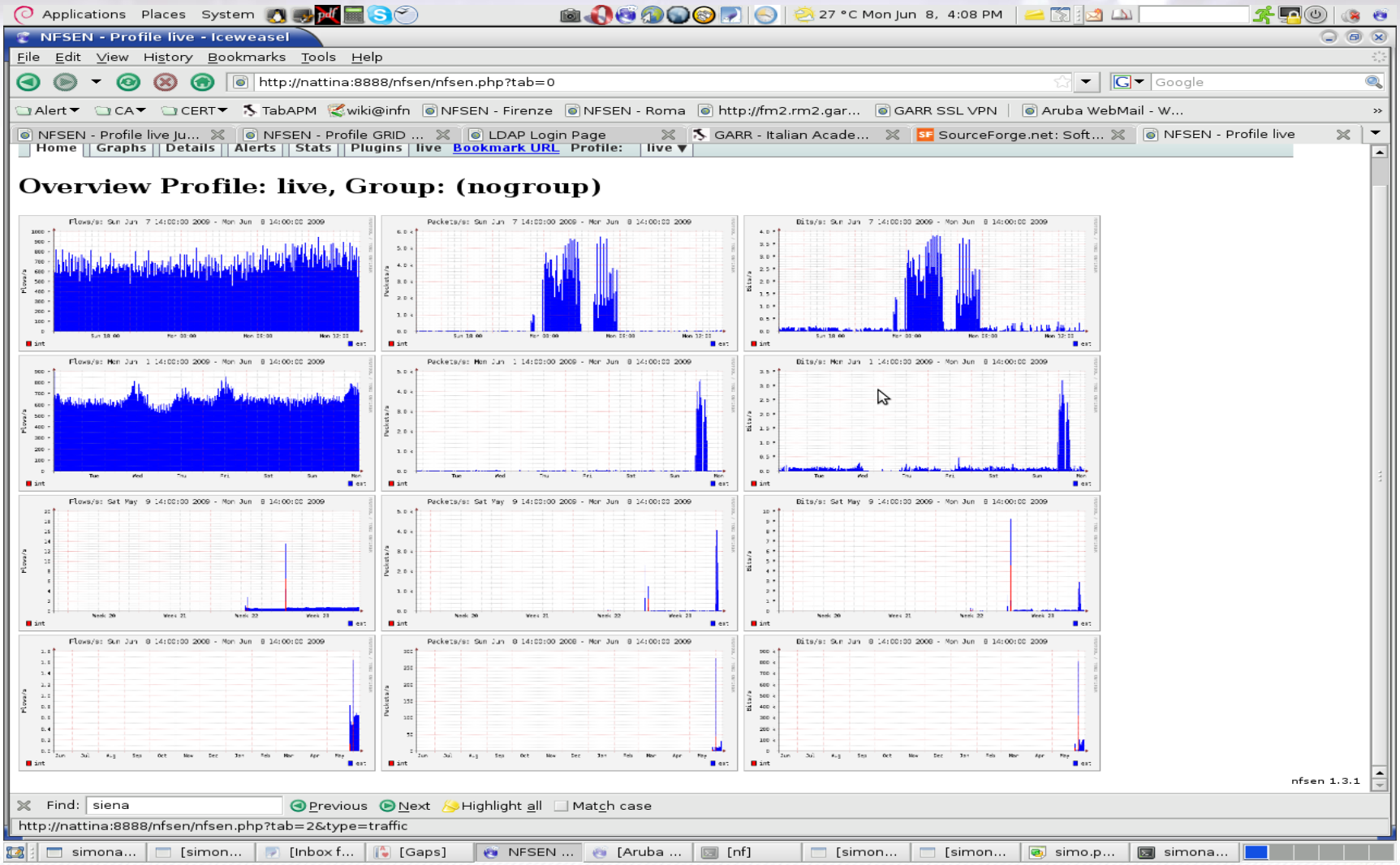
Installazione nProbe e collector 2/2

- Installazione Nfsen/nfdump
- Configurazione Nfsen
  - Aggiungere a ./etc/nfsen.conf le righe relative alle due interfacce del NAT

```
%sources = (
    'ext'    => { 'port'    => '10000', 'col' => '#0000ff', 'type' => netflow' },
    'int'        => { 'port'    => '10001', 'col' => '#ff0000' },
);
```

./install.pl ./etc/nfsen.conf

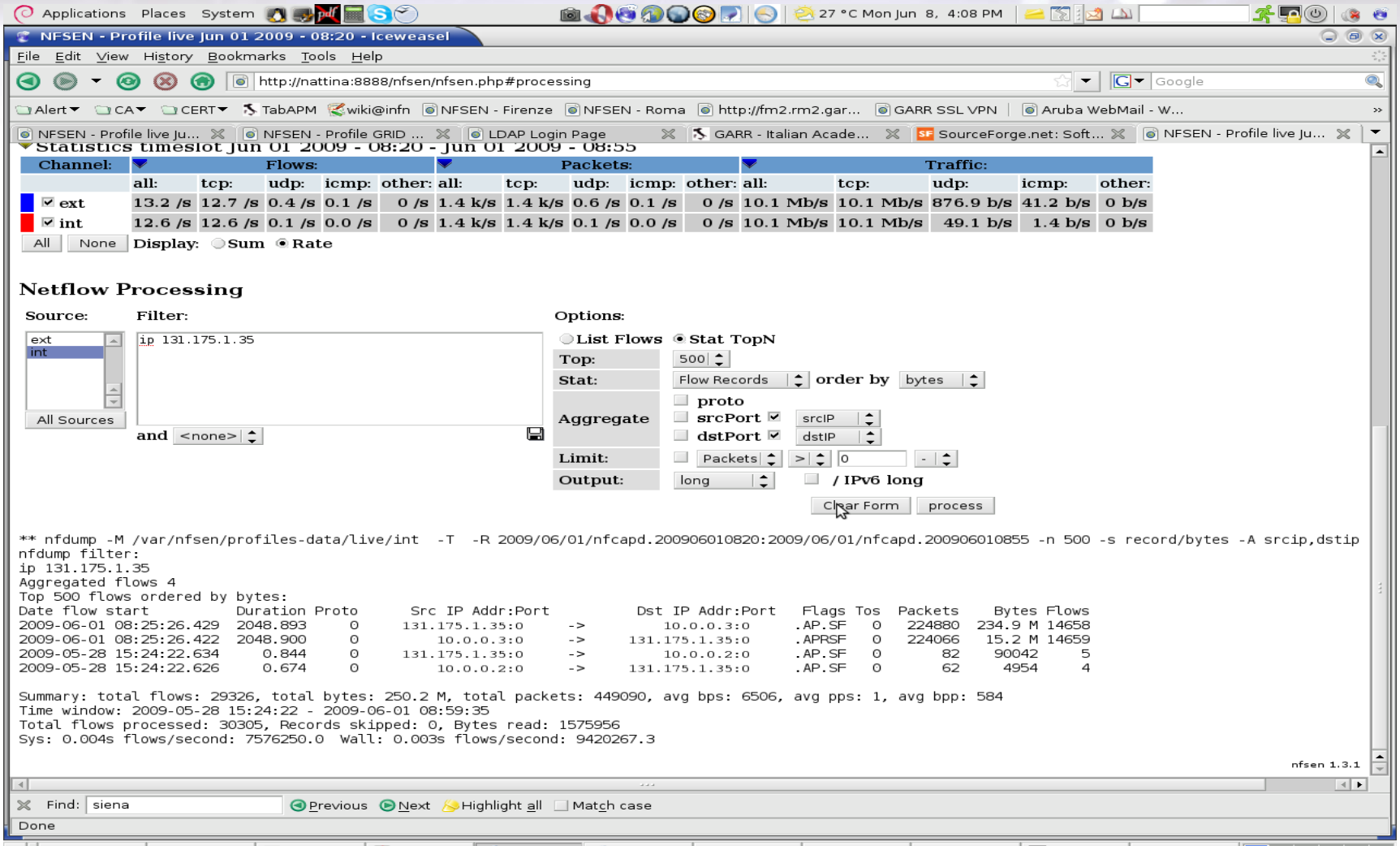
Risultato


Applications Places System
27 °C Mon Jun 8, 4:08 PM
NFSEN - Profile live - Iceweasel
File Edit View History Bookmarks Tools Help
http://nattina:8888/nfsen/nfsen.php?tab=0
Google
Alert CA CERT TabAPM wiki@infn NFSEN - Firenze NFSEN - Roma http://fm2.rm2.gar... GARR SSL VPN Aruba WebMail - W...
NFSEN - Profile live Ju... NFSEN - Profile GRID ... LDAP Login Page GARR - Italian Acade... SourceForge.net: Soft... NFSEN - Profile live
Home Graphs Details Alerts Stats Plugins live Bookmark URL Profile: live
Overview Profile: live, Group: (nogroup)
nfsen 1.3.1
Find: siena Previous Next Highlight all Match case
http://nattina:8888/nfsen/nfsen.php?tab=2&type=traffic
simona... [simon... [Inbox f... [Gaps] NFSEN ... [Aruba ... [nf] [simon... [simon... simo.p... simona...

Dettagli


NFSEN - Profile live Jun 01 2009 - 08:20 - Iceweasel
http://nattina:8888/nfsen/nfsen.php#processing
Home Graphs Details Alerts Stats Plugins live Bookmark URL Profile: live
Profile: live
TCP
UDP
ICMP
other
Profileinfo:
Type: live
Max: unlimited
Exp: never
Start: May 28 2009 - 09:17 UTC
End: Jun 08 2009 - 12:55 UTC
Mon Jun 1 08:20:00 2009 Bits/s any protocol
Bits/s any protocol
ext
int
t start 2009-06-01-08-20
t end 2009-06-01-08-55
Packets
Flows
Select Time Window Display: 12 Hours
Lin Scale Stacked Graph
Log Scale Line Graph
Statistics timeslot Jun 01 2009 - 08:20 - Jun 01 2009 - 08:55
Channel: Flows: Packets: Traffic:
ext 13.2 /s 12.7 /s 0.4 /s 0.1 /s 0 /s 1.4 k/s 1.4 k/s 0.6 /s 0.1 /s 0 /s 10.1 Mb/s 10.1 Mb/s 876.9 b/s 41.2 b/s 0 b/s
int 12.6 /s 12.6 /s 0.1 /s 0.0 /s 0 /s 1.4 k/s 1.4 k/s 0.1 /s 0.0 /s 0 /s 10.1 Mb/s 10.1 Mb/s 49.1 b/s 1.4 b/s 0 b/s
All None Display: Sum Rate
Find: siena Previous Next Highlight all Match case
Done

Processing


NFSEN - Profile live Jun 01 2009 - 08:20 - Iceweasel
http://nattina:8888/nfsen/nfsen.php#processing
Statistics timeslot Jun 01 2009 - 08:20 - Jun 01 2009 - 08:55
Channel: Flows: Packets: Traffic:
all: tcp: udp: icmp: other: all: tcp: udp: icmp: other: all: tcp: udp: icmp: other:
ext 13.2 /s 12.7 /s 0.4 /s 0.1 /s 0 /s 1.4 k/s 1.4 k/s 0.6 /s 0.1 /s 0 /s 10.1 Mb/s 10.1 Mb/s 876.9 b/s 41.2 b/s 0 b/s
int 12.6 /s 12.6 /s 0.1 /s 0.0 /s 0 /s 1.4 k/s 1.4 k/s 0.1 /s 0.0 /s 0 /s 10.1 Mb/s 10.1 Mb/s 49.1 b/s 1.4 b/s 0 b/s
All None Display: Sum Rate
Netflow Processing
Source: Filter: Options:
ext int
All Sources
ip 131.175.1.35
and <none>
List Flows Stat TopN
Top: 500
Stat: Flow Records order by bytes
Aggregate proto srcPort srcIP dstPort dstIP
Limit: Packets > 0
Output: long / IPv6 long
Clear Form process
** nfdump -M /var/nfsen/profiles-data/live/int -T -R 2009/06/01/nfcapd.200906010820:2009/06/01/nfcapd.200906010855 -n 500 -s record/bytes -A srcip,dstip
nfdump filter:
ip 131.175.1.35
Aggregated flows 4
Top 500 flows ordered by bytes:
Date flow start Duration Proto Src IP Addr:Port Dst IP Addr:Port Flags Tos Packets Bytes Flows
2009-06-01 08:25:26.429 2048.893 0 131.175.1.35:0 -> 10.0.0.3:0 .AP.SF 0 224880 234.9 M 14658
2009-06-01 08:25:26.422 2048.900 0 10.0.0.3:0 -> 131.175.1.35:0 .APRSF 0 224066 15.2 M 14659
2009-05-28 15:24:22.634 0.844 0 131.175.1.35:0 -> 10.0.0.2:0 .AP.SF 0 82 90042 5
2009-05-28 15:24:22.626 0.674 0 10.0.0.2:0 -> 131.175.1.35:0 .AP.SF 0 62 4954 4
Summary: total flows: 29326, total bytes: 250.2 M, total packets: 449090, avg bps: 6506, avg pps: 1, avg bpp: 584
Time window: 2009-05-28 15:24:22 - 2009-06-01 08:59:35
Total flows processed: 30305, Records skipped: 0, Bytes read: 1575956
Sys: 0.004s flows/second: 7576250.0 Wall: 0.003s flows/second: 9420267.3
nfsen 1.3.1
Find: siena Previous Next Highlight all Match case
Done

Estendere le capacita' della suite

- scripting + nfdump
  - -o pipe
  - -o csv
- nfsen plugins

Nfdump –o pipe

- Nfdump prevede un output machine readable tramite l'opzione: *-o pipe*
- Il formato di output e' riportato nella tabella, ogni campo e' separato da un "pipe"(|).
- Gli indirizzi IP sono rappresentati da numeri interi.
- L'uso di filtri e dell'aggregazione non modifica il formato di output, ma solo il riempimento dei campi.

Address family	PF_INET or PF_INET6
Time first seen UNIX time seconds	
msec first seen Mili seconds first seen	
Time last seen UNIX time seconds	
msec last seen Mili seconds first seen	
Protocol	Protocol
Src address	Src address as 4 consecutive 32bit numbers
Src port	Src port
Dst address	Dst address as 4 consecutive 32bit numbers.
Dst port	Dst port
Src AS	Src AS number
Dst AS	Dst AS number
Input IF	Input Interface
Output IF	Output Interface
TCP Flags	000001 FIN. 000010 SYN 000100 RESET 001000 PUSH 010000 ACK 100000 URGENT
Tos	Type of Service
Packets	Packets
Bytes	Bytes

Nfdump –o pipe

- Esempio di output:

2|1242719921|778|1242719921|778|6|0|0|0|3235805120|52616|0|0|0|1134240473|1863|24869|8075|114|88|24|0|1|45

- In cui: 3235805120 Corrisponde a: 192.222.119.192
- 24869 e' AS sorgente e 8075 quello destinazione
- 114 e' l'snmp ifindex di ingresso e 88 l'snmp ifindex di uscita
- 1 e' il pacchetto che contiene 45 bytes

Nfdump –o csv

- Su prima riga nome campi
- Tutti i campi del flusso (lista flussi), alcuni campi specifici per query aggregate
- IP in notazione decimale (IPv6 esadecimale), Date formato YYYY-MM-DD hh:mm:ss, volume di traffico in bytes

Come scrivere nuovi plugin

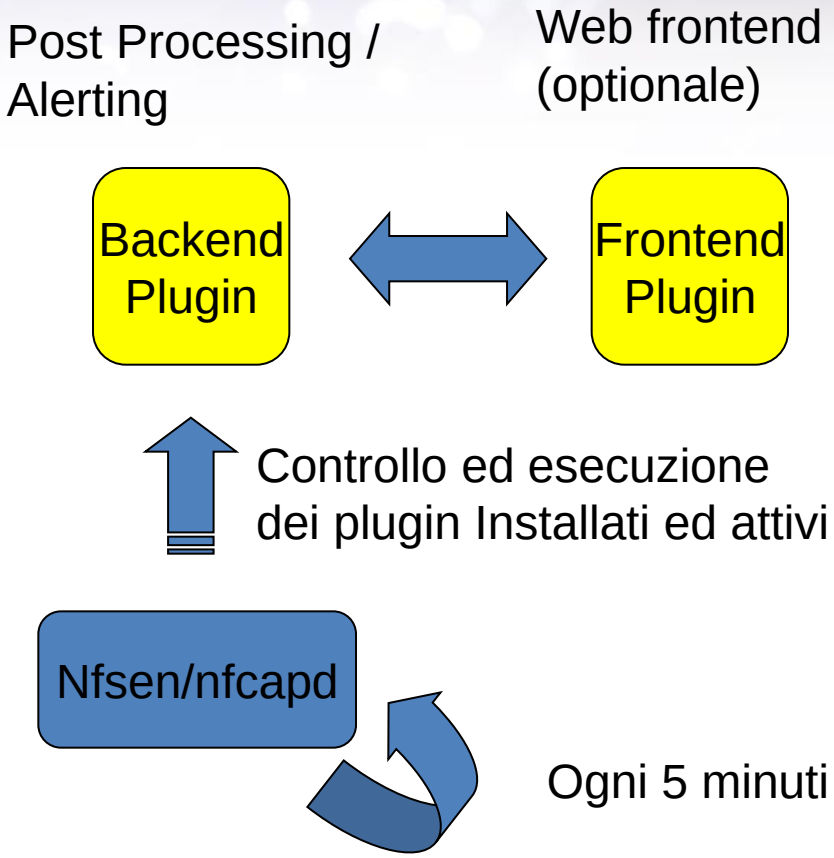
- Nfsen plugins:

Ogni 5 minuti, quando vengono scritti i flussi su disco e sono riempite le strutture RRD, nfsen lancia i plugin installati.

Sono composti da tue parti:

1. Backend, scritti in linguaggio perl, hanno lo scopo di elaborare i dati
2. Frontend, scritti in linguaggio php, fanno da interfaccia al backend

- I file di un plugin devono avere lo stesso nome:
  - Backend: <nome_plugin>.pm
  - Frontend: <nome_plugin>.php



Appendici

- Esempi di configurazione esportazione sui router Juniper e Cisco:
  - JunOS v5
  - JunOS v9
  - Cisco v5
  - Cisco v9
  - Cisco FNF

Esempi di configurazione:JunOS (v5)

- Definizione del filtro:

  set firewall family inet filter NETFLOW-SAMPLE term default then sample
  set firewall family inet filter NETFLOW-SAMPLE term default then accept

- Configurazione interfacce:

  set interfaces fe-0/1/0 unit 0 family inet filter input NETFLOW-SAMPLE
  set interfaces fe-0/1/0 unit 0 family inet filter output NETFLOW-SAMPLE

- Configurazione collezionatore

  set forwarding-options sampling input family inte rate 1000
  set forwarding-options sampling output cflowd 172.16.0.1 port 20000
  set forwarding-options sampling output cflowd version 5
  set forwarding-options sampling output cflowd autonomous-system-type [peer|origin]

Esempi di configurazione:JunOS (v9)

- Configurazione interfacce:
  - *set interfaces fe-0/1/0 unit 0 family inet filter input NETFLOW-SAMPLE*
  - *set interfaces fe-0/1/0 unit 0 family inet filter output NETFLOW-SAMPLE*
- Configurazione esportazione e sampling:
  - *set forwarding-options sampling input family inet rate 1*
  - *set forwarding-options sampling output cflowd 172.16.0.1 port 20000*
  - *set forwarding-options sampling output cflowd 172.16.0.1 version9 template prova-template*
  - *set forwarding-options sampling output interface sp-0/2/0 source-address 10.0.0.1*
- Configurazione del filtro:
  - *set firewall family inet filter NETFLOW-SAMPLE term default then sample*
  - *set firewall family inet filter NETFLOW-SAMPLE term default then accept*

Esempi di configurazione:Cisco (v5)

- Configurazione interfacce

  interface FastEthernet0/0

  ip route cache flow

- Esportazione dei flussi

  ip flow-export

  ip flow-export version 5

  ip flow-export destination 172.16.0.1 20000

  ip flow-cache timeout active 5

  ip flow-cache timeout inactive 1000

Esempi di configurazione:Cisco(v9)

Configurazione Sampling:

```
flow-sampler-map sampling1-1000
 mode random one-out-of 1000
```

Configurazione interfacce:

```
interface X/X/X
  flow-sampler sampling1-1000
```

Configurazione collettore:

```
ip flow-capture fragment-offset
ip flow-capture packet-length
ip flow-capture vlan-id
ip flow-capture icmp
ip flow-capture mac-addresses
ip flow-export version 9 origin-as bgp-nexthop
ip flow-export destination 172.16.0.1 20000
```

Esempi di configurazione:Cisco (FNF)

- Definizione template:

```
flow record template_prova
match ipv4 source address
match ipv4 source mask
match ipv4 destination address
match ipv4 destination mask
match transport source-port
match transport destination-port
match transport tcp source-port
match transport tcp destination-port
match interface input
match interface output
collect datalink mac source address input
collect routing next-hop address ipv4 bgp
collect ipv4 section payload size 100
```

Esempi di configurazione:Cisco(FNF)

- Definizione del monitor:

flow monitor prova_monitor

record ***template_prova***

exporter ***prova_exporter***

cache timeout active 30

statistics packet protocol

statistics packet size

- Definizione exporter

flow exporter prova_exporter

destination 172.16.0.1

transport udp 20000

Esempi di configurazione:Cisco(FNF)

- Configurazione Interfacce

interface FastEthernet0/0

ip address X.X.X.X X.X.X.X

*ip flow monitor **prova_monitor** sampler **prova_SAMPLER** input*

*ip flow monitor **prova_monitor** sampler **prova_SAMPLER** output*

- Configurazione Sampler

sampler prova_SAMPLER

mode deterministic 1 out-of 1000

exit

Hands-on

Agenda

- Architettura laboratori/VMs
- Analisi incidente
- Usare la VM nella vostra rete di produzione come collettore sflow pronto all'uso

Introduzione alle attivita'

- Scopo:
  - illustrare i componenti del sistema di analisi dei flussi per la LAN (sflow) da utilizzare per reagire in caso di incidenti di sicurezza.
- Come:
  - Laboratori
  - VM in produzione

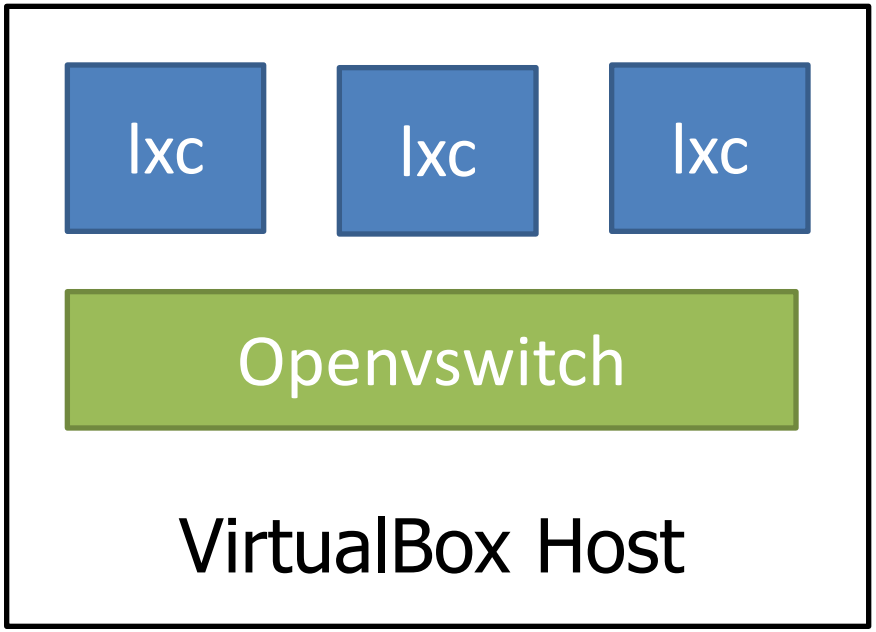
Introduzione alle attivita'

- Tool utilizzati:
  - Nfdump (sflowd, nfdump)
  - Openvswitch
  - Linux Container
  - Iproute2 (ip)
  - arp

Architettura laboratorio

Descrizione Laboratorio

- Virtual Machine (VirtualBox)
- Linux container
- Openvswitch



Utenza

- Virtual Machine (VirtualBox)
  - User: user
  - Pass: GarrGarr
  - Root password (su): GarrGarr
- Linux container
  - Sulla virtual machine chiavi per utenza root dei container

File, Script e comandi

Direcrtory sflow_lab/

- **attacks/**: script di esempo di attacco
- **data**: file statistiche dei flussi
- **nfdump_example_query.sh**: esempi di interrogazione con nfdump
- **run_me.sh**: script per far partire il testbed velocemente
- **set_ovs_sflow.sh**: script per l'esportazione dei flussi sul OvS
- **sfcapd.sh**: script di avvio del collettore dei flussi sflow
- **show_ovs_arp_table_command.sh**: comando per arp table di OvS
- **tools**: directory con vari script utili
- **vm_creation.sh**: script per la creazione di altri linux container

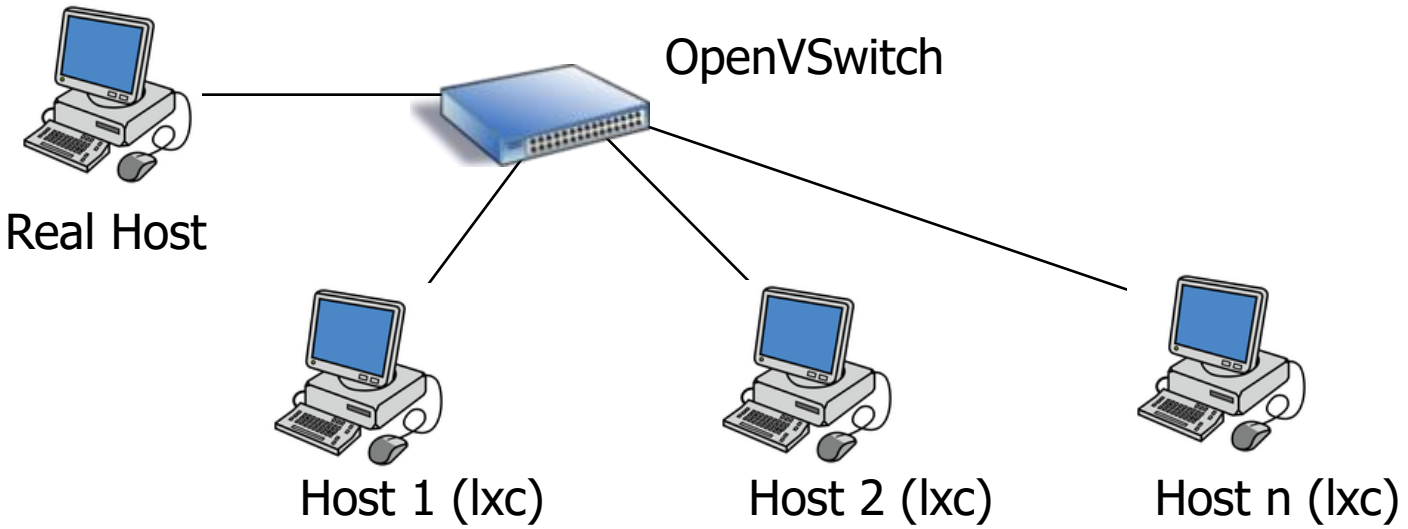
File, Script e comandi

- **ovs-vsctl show:** mostra i bridge e le sue porte
- **Ip addr show:** mostra le interfaccie di rete con la loro conf
- **ssh <utente>@<IP>:** per accedere agli host (containers)
- **nfdump -r <data path>/nfcapd.<timeslot> -s ip/flows:** top10 IP per # di flussi
- **Tcpdump**
- **ovs-appctl fdb/show br0:** tabella MAC address
- **ovs-vsctl --format csv --columns ofport,ifindex,name list Interface:** corrispondenza indice porte, ifindex e nome delle interfacce
- **ovs-vsctl list sflow:** visualizza l'exporter configurato su openvswitch

Laboratorio

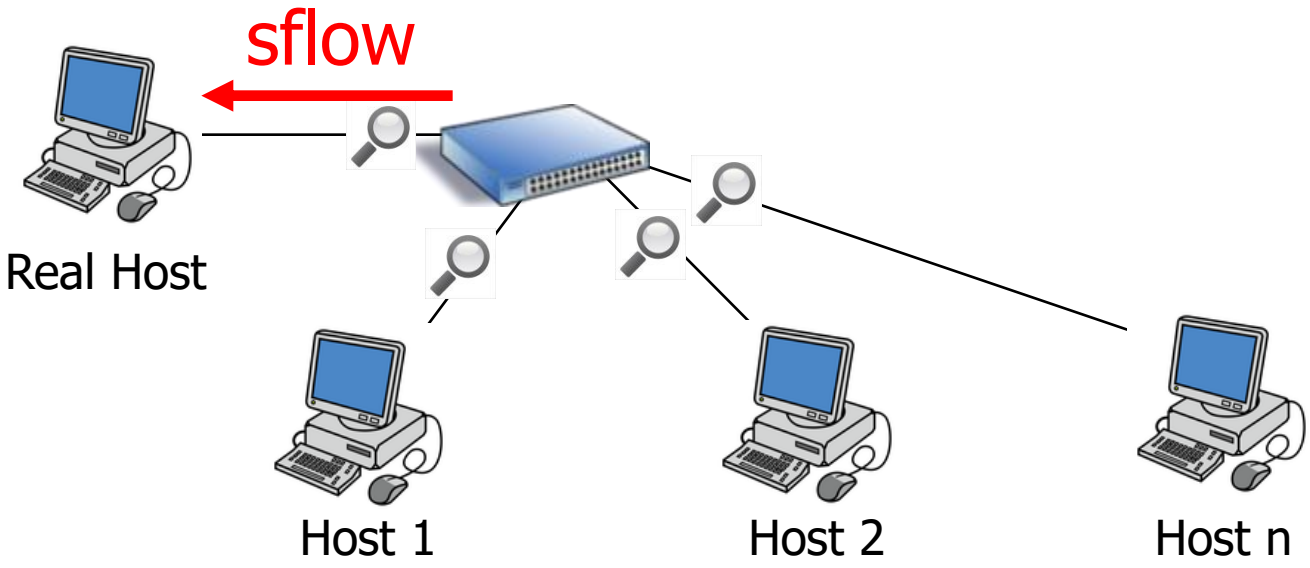
Topologia di rete laboratorio

- Switched LAN



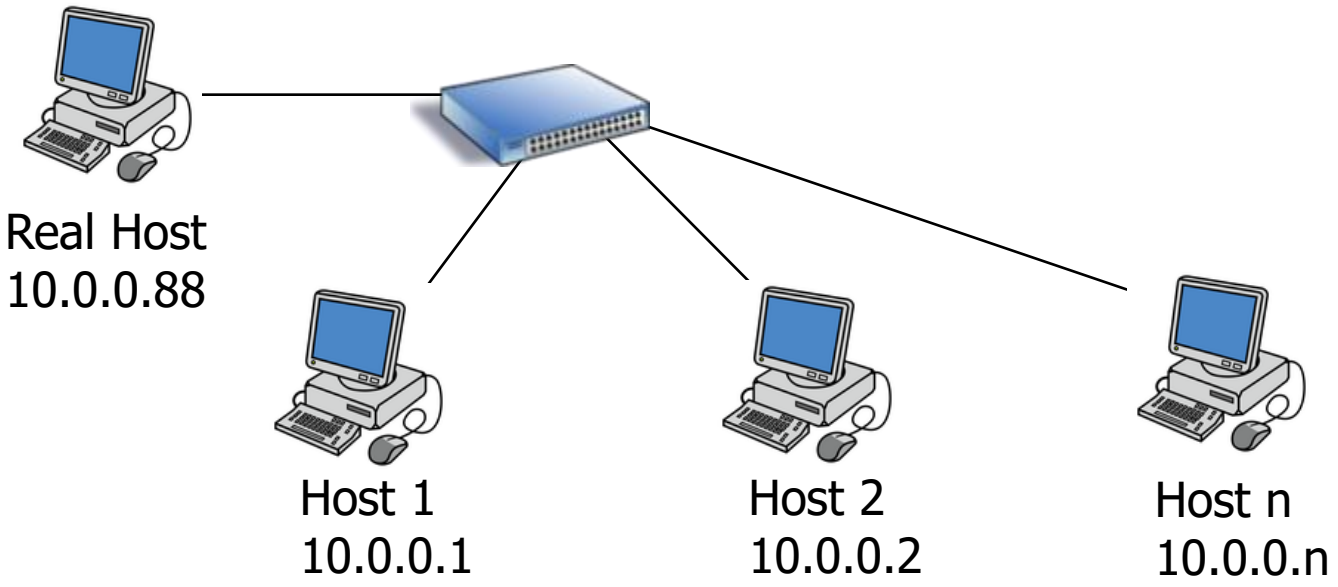
Laboratorio

- Test sflow
  - Real host = collettore dei flussi (sfcapd)
  - Hosts = Linux container in rete



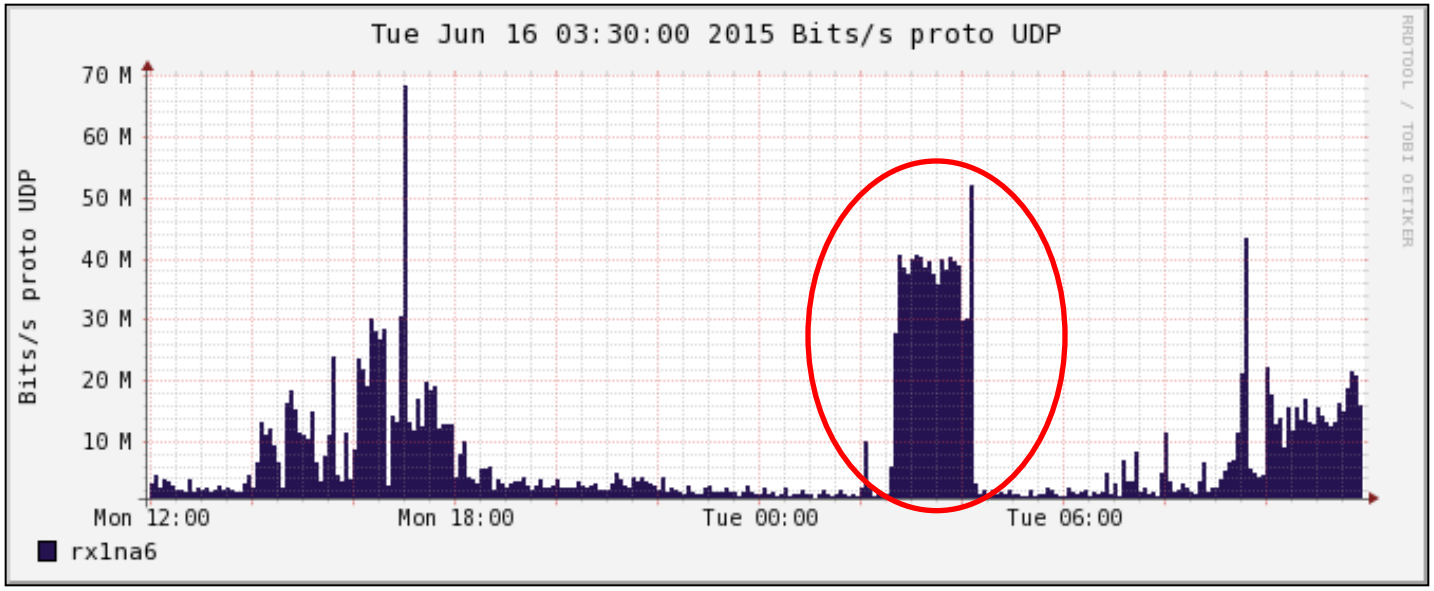
Laboratorio

- Indirizzamento IP



Analisi incidente

- Si rileva un’anomalia nella rete
  - Traffico «burst»
  - Rete satura
  - Email del Garr CERT



Analisi incidente

LAB# **nfdump -r 2016/04/15/nfcapd.201604151712 -s ip/flows**

Top 10 IP Addr ordered by flows:

Date first seen	Duration	Proto	IP Addr	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
2016-04-15 17:13:45.993	**209.999**	**any**	**10.0.0.1**	**994(100.0)**	**63616(100.0)**	**3.7 M(100.0)**	**302**	**140561**	**58**
2016-04-15 17:14:06.775	146.923	any	10.0.0.182	10(1.0)	640(1.0)	37120(1.0)	4	2021	58
2016-04-15 17:14:31.991	161.610	any	10.0.0.252	10(1.0)	640(1.0)	37120(1.0)	3	1837	58
2016-04-15 17:13:45.993	202.000	any	10.0.0.88	9(0.9)	576(0.9)	33408(0.9)	2	1323	58
2016-04-15 17:13:46.992	103.947	any	10.0.0.114	9(0.9)	576(0.9)	33408(0.9)	5	2571	58
2016-04-15 17:13:46.992	177.989	any	10.0.0.239	9(0.9)	576(0.9)	33408(0.9)	3	1501	58
2016-04-15 17:14:21.988	174.004	any	10.0.0.66	8(0.8)	512(0.8)	29696(0.8)	2	1365	58
2016-04-15 17:14:14.993	166.895	any	10.0.0.72	8(0.8)	512(0.8)	29696(0.8)	3	1423	58
2016-04-15 17:13:52.993	166.999	any	10.0.0.2	8(0.8)	512(0.8)	29696(0.8)	3	1422	58
2016-04-15 17:13:57.992	165.814	any	10.0.0.173	8(0.8)	512(0.8)	29696(0.8)	3	1432	58

Summary: total flows: 994, total bytes: 3689728, total packets: 63616, avg bps: 140561, avg pps: 302, avg bpp: 58

Time window: 2016-04-15 17:12:16 - 2016-04-15 17:17:15

Total flows processed: 3840, Blocks skipped: 0, Bytes read: 414852

Sys: 0.000s flows/second: 0.0 Wall: 0.000s flows/second: 7084870.8

Analisi incidente

- Indagine:
  - Analisi dei flussi in transito sullo switch
  - Analizziamo il traffico con nfdump alla ricerca del traffico malevolo
  - Visualizziamo i mac address!!
  - Aggregazione dei flussi
  - Statistiche
  - ARP cache
  - Ifindex, porte

Opzioni di nfdump

Opzioni di nfdump:

Formato di output:

- -o ‘fmt: … %ismc %odmc …’

Aggregazione:

- -a –A insrcmac,srcip,dstip

Dati statistici:

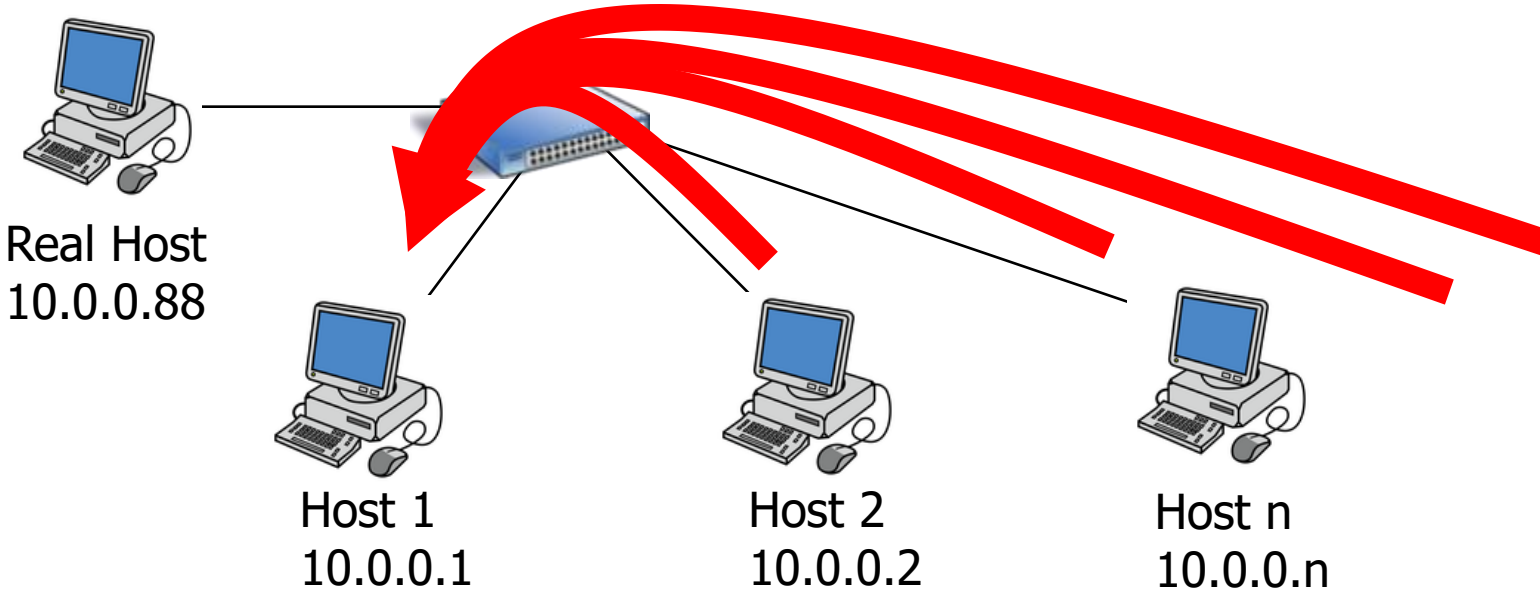
- -s ip/flows = IP top flows
- -s record/packets = record (aggregati con opzione –A) top packets
- -s record/bytes = record (aggregati con opzione –A) top bytes

Esempio:

nfdump –r <data path>/nfcapd.<nf-timeslot> -o ‘fmt: %ts %pr %ismc %odmc %sap %dap %sas %das %in %out %byt %bps’ –a –A insrcmac,srcip,dstip –s record/packets

Esempio incidente 1

- Apparentemente il traffico proviene da tutti indirizzi della LAN /24
- E' corrotta tutta la LAN o si tratta di traffico «Spoofato»?



Esempio incidente 1

LAB# nfdump -r data/2016/04/15/nfcapd.201604151243 -o 'fmt:%ismc %odmc %in %out %sap %dap %byt'

In src MAC Addr	Out dst MAC Addr	Input	Output	**Src IP Addr**:Port	Dst IP Addr:Port	Bytes
be:32:45:b9:0b:5d	56:9c:3c:77:7e:54	10	6	**10.0.0.240**:45055	10.0.0.1:80	3712
be:32:45:b9:0b:5d	56:9c:3c:77:7e:54	10	6	**10.0.0.162**:13344	10.0.0.1:80	3712
be:32:45:b9:0b:5d	56:9c:3c:77:7e:54	10	6	**10.0.0.89**:62848	10.0.0.1:80	3712
be:32:45:b9:0b:5d	56:9c:3c:77:7e:54	10	6	**10.0.0.137**:25307	10.0.0.1:80	3712
be:32:45:b9:0b:5d	56:9c:3c:77:7e:54	10	6	**10.0.0.70**:14419	10.0.0.1:80	3712
be:32:45:b9:0b:5d	56:9c:3c:77:7e:54	10	6	**10.0.0.164**:49085	10.0.0.1:80	3712
be:32:45:b9:0b:5d	56:9c:3c:77:7e:54	10	6	**10.0.0.54**:1025	10.0.0.1:80	3712
be:32:45:b9:0b:5d	56:9c:3c:77:7e:54	10	6	**10.0.0.81**:60817	10.0.0.1:80	3712
be:32:45:b9:0b:5d	56:9c:3c:77:7e:54	10	6	**10.0.0.19**:58914	10.0.0.1:80	3712
be:32:45:b9:0b:5d	56:9c:3c:77:7e:54	10	6	**10.0.0.111**:54273	10.0.0.1:80	3712
be:32:45:b9:0b:5d	56:9c:3c:77:7e:54	10	6	**10.0.0.170**:17226	10.0.0.1:80	3712

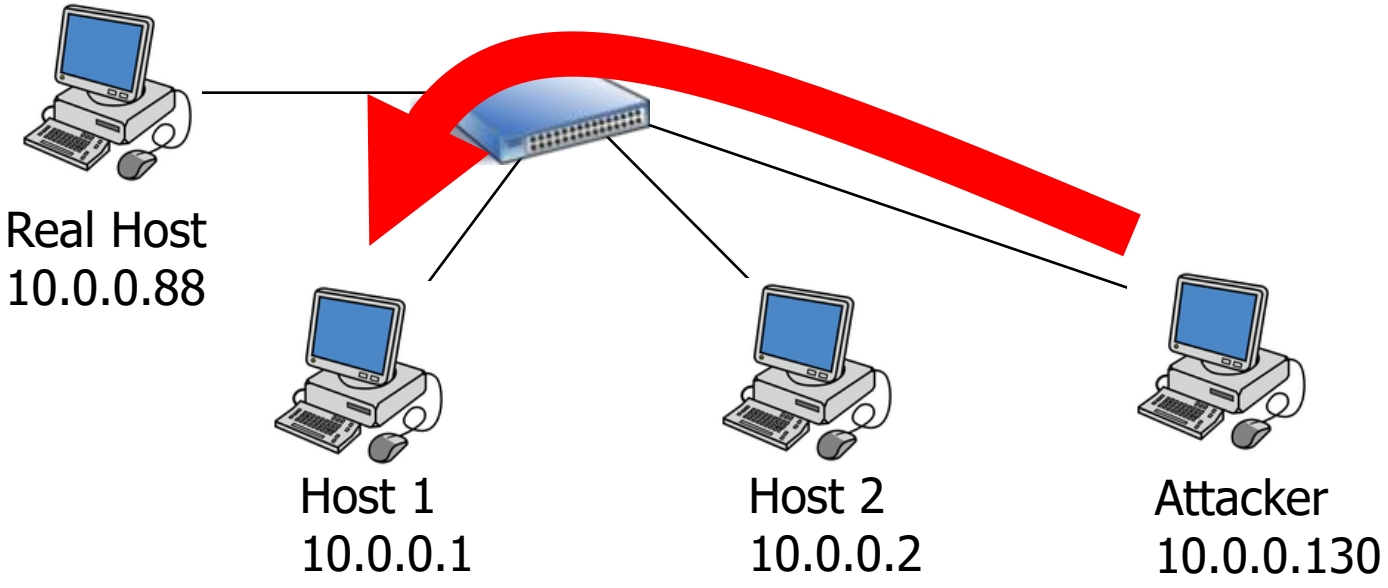
Summary: total flows: 1797, total bytes: 6670464, total packets: 115008, avg bps: 178474, avg pps: 384, avg bpp: 58
Time window: 2016-04-15 12:43:47 - 2016-04-15 12:48:46
Total flows processed: 1797, Blocks skipped: 0, Bytes read: 194208
Sys: 0.016s flows/second: 112312.5 Wall: 0.038s flows/second: 46478.5

LAB# **arp -a | grep be:32:45:b9:0b:5d**

host130 (**10.0.0.130**) at **be:32:45:b9:0b:5d** [ether] on br0

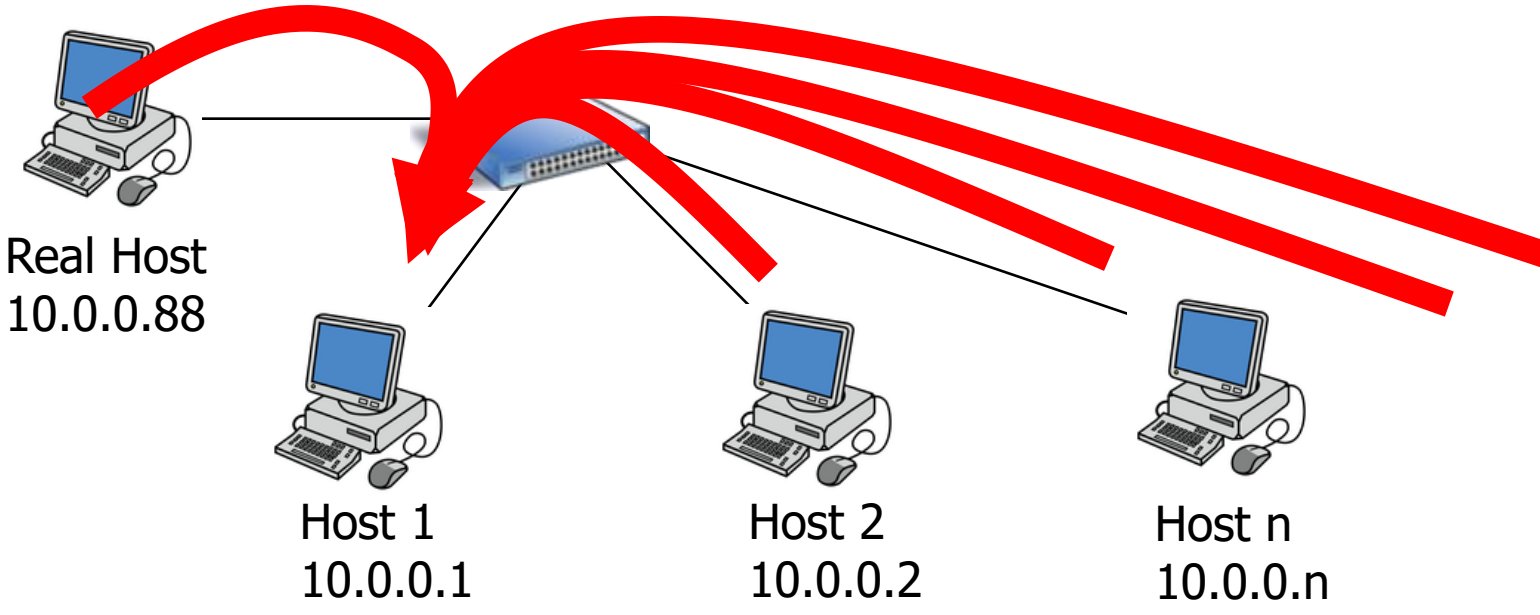
Analisi incidente

- Traffico reale



Esempio incidente 2

- Apparentemente il traffico proviene da indirizzi diversi (tutta Internet)



Esempio incidente 2

- Apparentemente il traffico proviene da indirizzi diversi (tutta Internet)

```
LAB# nfdump -r data/2016/04/15/nfcapd.201604151527 -o 'fmt:%ismc %odmc %in %out %sap %dap %byt'
  In src MAC Addr  Out dst MAC Addr  Input Output      Src IP Addr:Port       Dst IP Addr:Port     Bytes
c2:8f:81:5b:8f:38 aa:4d:c1:fe:94:52     10      6   120.32.138.210:11064        10.0.0.1:22        3712
c2:8f:81:5b:8f:38 aa:4d:c1:fe:94:52     10      6    57.23.96.159:15975         10.0.0.1:22        3712
c2:8f:81:5b:8f:38 aa:4d:c1:fe:94:52     10      6    10.77.167.145:30783        10.0.0.1:22        3712
c2:8f:81:5b:8f:38 aa:4d:c1:fe:94:52     10      6    33.93.127.110:64757        10.0.0.1:22        3712
c2:8f:81:5b:8f:38 aa:4d:c1:fe:94:52     10      6    183.249.163.25:30008       10.0.0.1:22        3712
aa:4d:c1:fe:94:52 e2:37:95:a7:aa:4e      6      4       10.0.0.1:22        62.244.13.69:39349     3968
c2:8f:81:5b:8f:38 aa:4d:c1:fe:94:52     10      6   241.121.82.188:31924        10.0.0.1:22        3712
c2:8f:81:5b:8f:38 aa:4d:c1:fe:94:52     10      6    216.18.79.215:8781         10.0.0.1:22        3712
c2:8f:81:5b:8f:38 aa:4d:c1:fe:94:52     10      6   55.217.185.149:34341        10.0.0.1:22        3712
c2:8f:81:5b:8f:38 aa:4d:c1:fe:94:52     10      6   108.52.144.37:43454         10.0.0.1:22        3712
Summary: total flows: 3333, total bytes: 13232448, total packets: 213312, avg bps: 357632, avg pps: 720, avg bpp: 62
Time window: 2016-04-15 15:27:19 - 2016-04-15 15:32:15
Total flows processed: 3333, Blocks skipped: 0, Bytes read: 360120
Sys: 0.024s flows/second: 138875.0   Wall: 0.183s flows/second: 18115.3

LAB# ovs-appctl fdb/show br0
 port  VLAN  MAC                Age
LOCAL     0  e2:37:95:a7:aa:4e   23
    1     0  aa:4d:c1:fe:94:52    0
    3     0  c2:8f:81:5b:8f:38    0
```

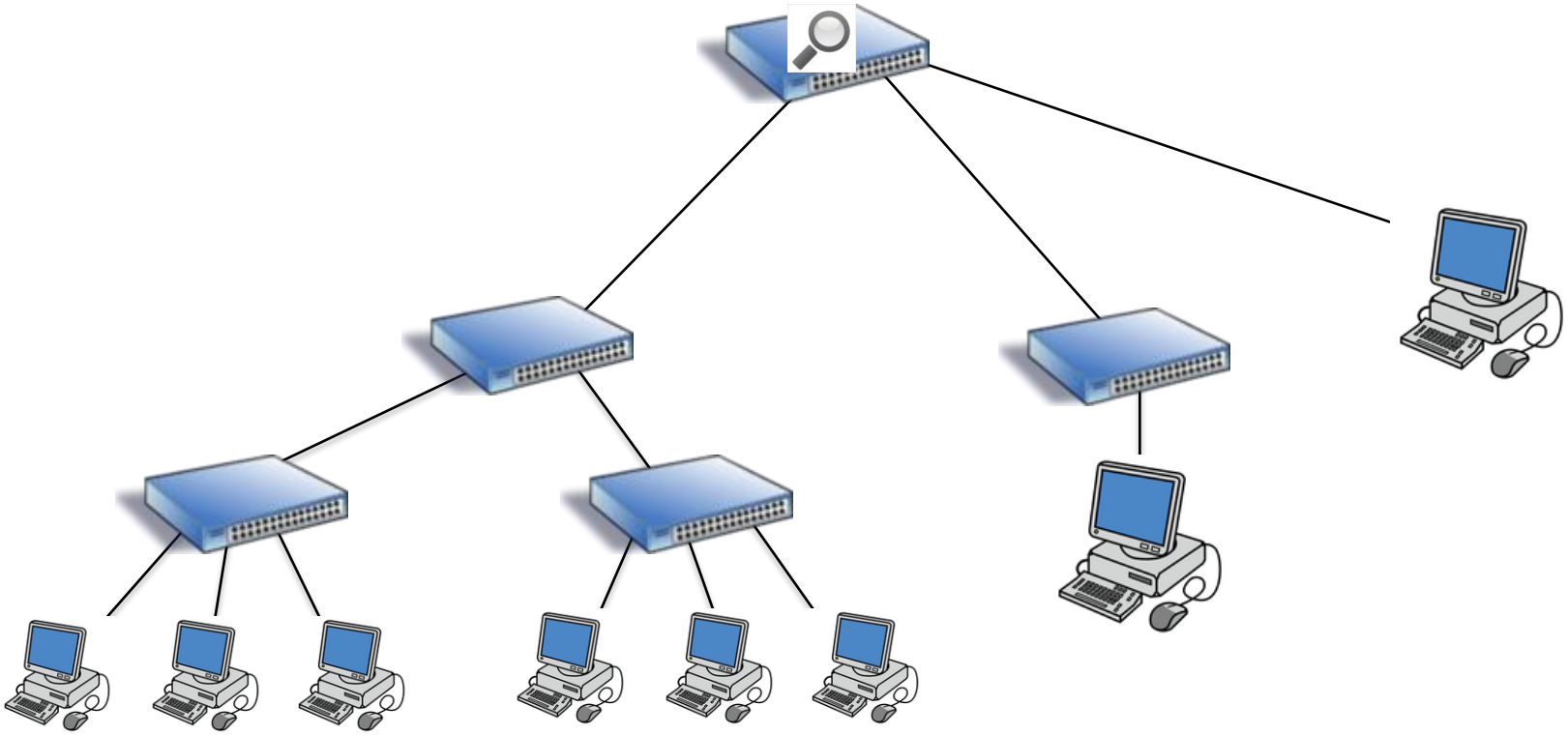
Esempio incidente 2

LAB# ovs-vsctl --format csv --columns ofport,ifindex,name list Interface

ofport,ifindex,name
3,10,spoofer
1,6,"""host1"""
65534,4,"""br0"""
2,8,"""host2"""

Esempio incidente 3

Basta il MAC address per identificare l'attaccante?



Esempio incidente 3

MAC spoofing

LAB# nfdump -r data/2016/04/15/nfcapd.201604151632 -o 'fmt:%ismc %odmc %in %out %sap %dap %byt'

In src MAC Addr	Out dst MAC Addr	**Input**	Output	Src IP Addr:Port	Dst IP Addr:Port	Bytes
8e:fb:30:04:49:b8	aa:4d:c1:fe:94:52	**10**	6	9.90.236.76:60679	10.0.0.1:22	3712
d8:ed:b6:e2:e0:c1	aa:4d:c1:fe:94:52	**10**	6	59.118.176.167:44839	10.0.0.1:22	3712
a5:c6:b1:0d:e1:33	aa:4d:c1:fe:94:52	**10**	6	184.166.232.31:65275	10.0.0.1:22	3712
a5:b2:81:2f:39:a2	aa:4d:c1:fe:94:52	**10**	6	251.252.102.169:26870	10.0.0.1:22	3712
6b:7a:83:42:0a:79	aa:4d:c1:fe:94:52	**10**	6	173.247.113.173:38301	10.0.0.1:22	3712
31:1a:cb:ab:55:b8	aa:4d:c1:fe:94:52	**10**	6	142.47.59.62:29877	10.0.0.1:22	3712
0f:23:ac:6a:88:da	aa:4d:c1:fe:94:52	**10**	6	108.194.65.156:36536	10.0.0.1:22	3712
71:28:f6:7c:fe:9f	aa:4d:c1:fe:94:52	**10**	6	118.92.169.138:61940	10.0.0.1:22	3712
63:f7:39:21:31:ca	aa:4d:c1:fe:94:52	**10**	6	167.103.82.15:44050	10.0.0.1:22	3712
80:2d:b0:bb:de:5a	aa:4d:c1:fe:94:52	**10**	6	184.111.11.16:9636	10.0.0.1:22	3712
e6:5a:d1:46:ae:a3	aa:4d:c1:fe:94:52	**10**	6	18.1.163.163:25422	10.0.0.1:22	3712
58:b0:e3:89:d2:ab	aa:4d:c1:fe:94:52	10	6	139.23.157.82:4887	10.0.0.1:22	3712
eb:56:90:8d:f9:ed	aa:4d:c1:fe:94:52	**10**	6	214.5.143.218:3839	10.0.0.1:22	3712
74:6e:a5:16:52:19	aa:4d:c1:fe:94:52	10	6	27.207.107.146:6176	10.0.0.1:22	3712
f0:b4:76:c9:2f:16	aa:4d:c1:fe:94:52	10	6	181.55.33.28:51957	10.0.0.1:22	3712
7e:46:5e:50:a3:75	aa:4d:c1:fe:94:52	10	6	241.10.108.26:52715	10.0.0.1:22	3712
2e:aa:bd:b2:7a:cc	aa:4d:c1:fe:94:52	10	6	5.1.226.27:16401	10.0.0.1:22	3712

Summary: total flows: 1745, total bytes: 6477440, total packets: 111680, avg bps: 172879, avg pps: 372, avg bpp: 58
Time window: 2016-04-15 16:32:16 - 2016-04-15 16:37:15
Total flows processed: 14084, Blocks skipped: 0, Bytes read: 1521216
Sys: 0.016s flows/second: 880250.0 Wall: 0.077s flows/second: 182660.0

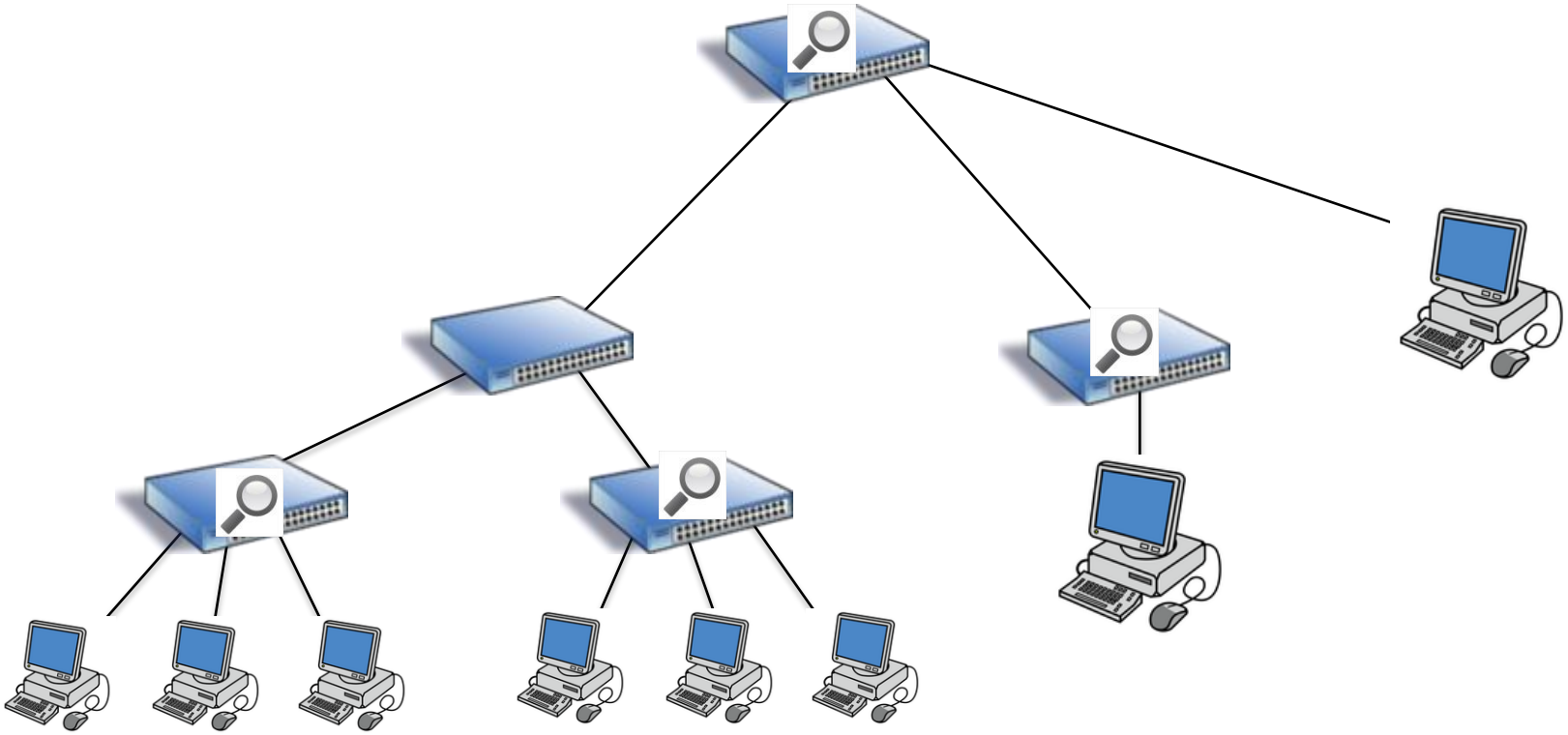
Esempio incidente 3

LAB# ovs-vsctl --format csv --columns ofport,ifindex,name list Interface

ofport,ifindex,name
3,10,spoofer
1,6,"""host1"""
65534,4,"""br0"""
2,8,"""host2"""

Esempio incidente 3

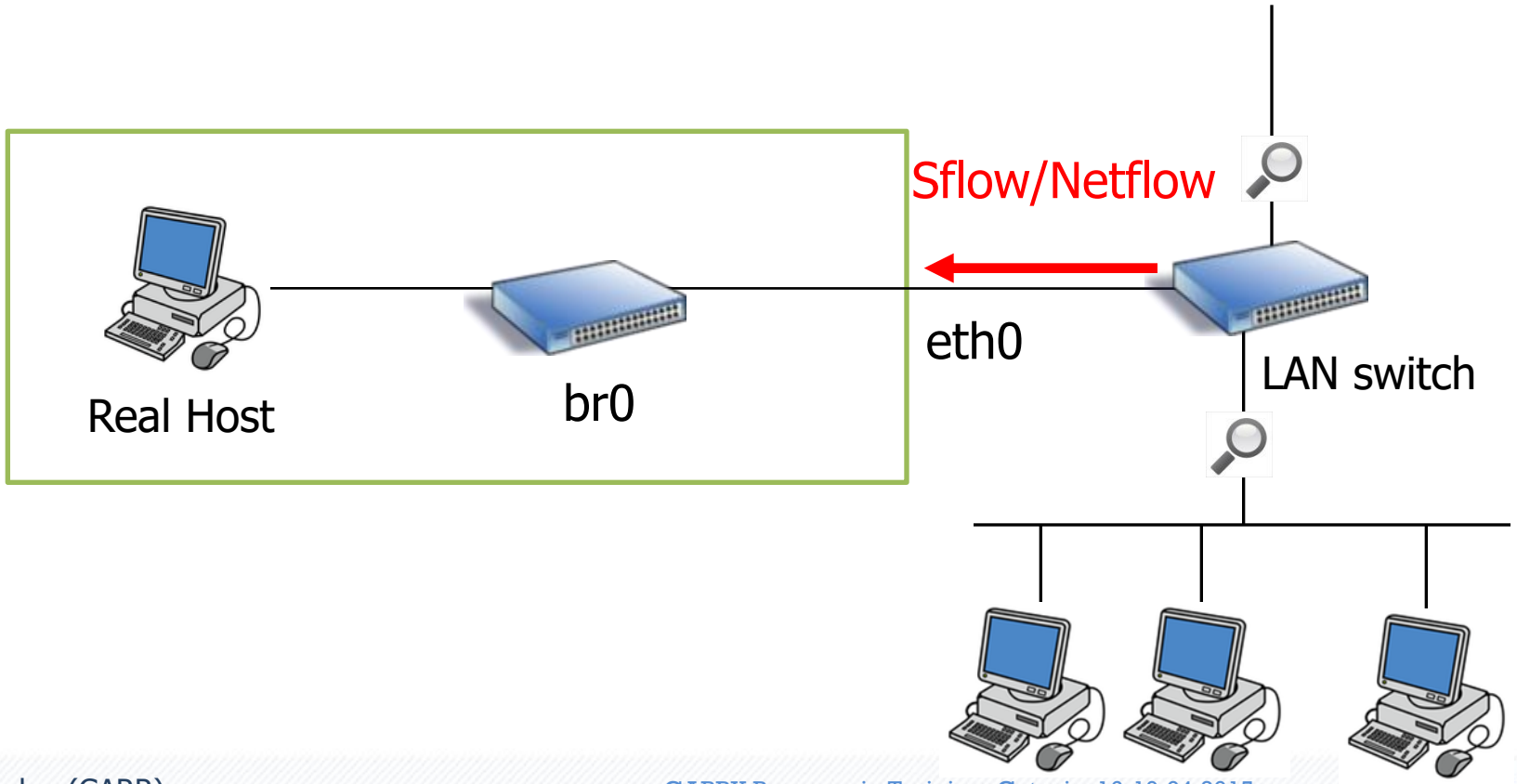
La distribuzione della cattura dei flussi Netflow/sflow puo' fare la differenza…



Usare la VM come collettore sflow

Se lo switch supporta il protocollo sflow

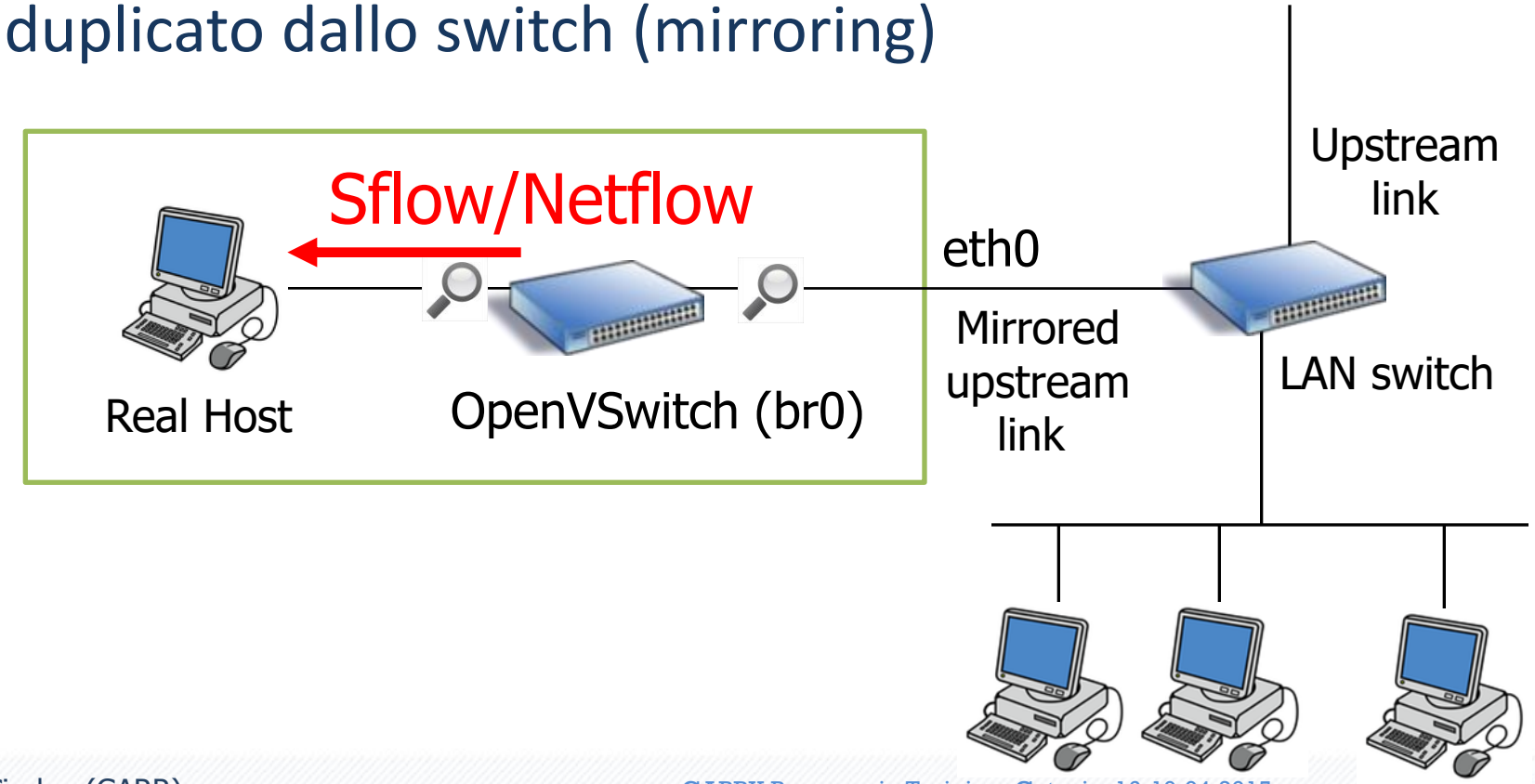
VM puo' usata come collettore dei flussi degli switch



Usare la VM come collettore sflow

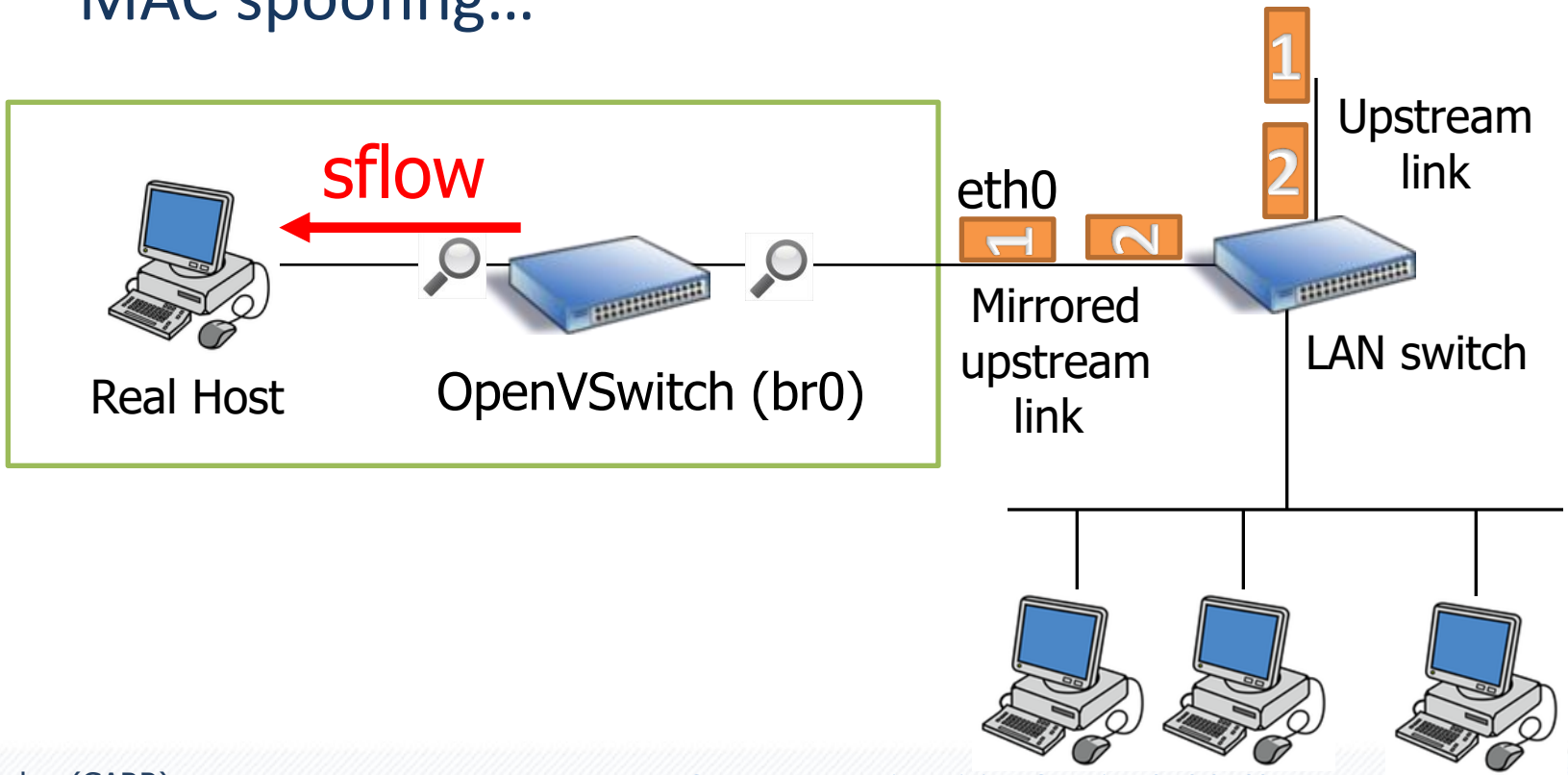
Se lo switch non supporta il protocollo sflow

OpenvSwitch puo' usato come sonda del traffico duplicato dallo switch (mirroring)



Usare la VM come collettore sflow

- Mirroring del traffico di un interfaccia verso la VM
- Tutto il traffico su interfaccia br0, inutile in caso di MAC spoofing…



Usare la VM come collettore sflow

- Collegare l'interfaccia «eth0» nel bridge
  - ovs-vsctl addport br0 eth0
- Configurare indirizzo IP al bridge «br0»
  - Ip addr add <IP>/<MASK> dev br0
- Accendere il collettore sflow
  - sfcapd –S 1 –n <souce name>,<source IP>,<source data path> -p 6343 –T all
- Configurare openvswitch per esportare i flussi verso il collettore
  - Es: ovs-vsctl -- --id=@sflow create sFlow agent=eth0 target=\"10.0.0.88:6343\" header=128 sampling=64 polling=10 \ -- set Bridge br0 sflow=@sflow
- Attenzione ai file di log…

Usare la VM come collettore sflow

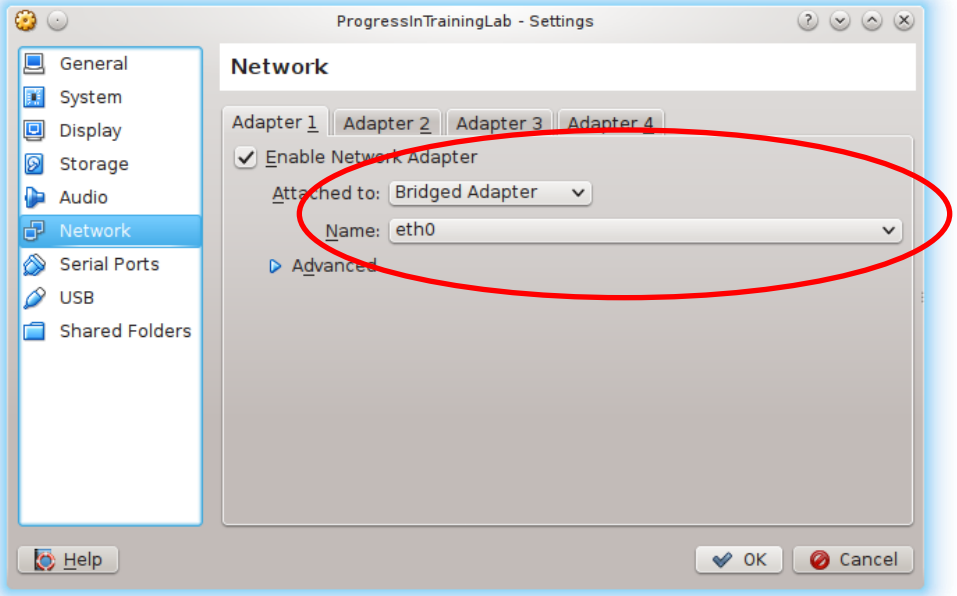
- Rendere la configurazione statica
  - Esempio di /etc/network/interfaces:

```
allow-ovs br0
iface br0 inet static
  address 192.168.1.1
  netmask 255.255.255.0
  gateway 192.168.1.254
  ovs_type OVSBridge
  ovs_ports eth0

allow-br0 eth0
iface eth0 inet manual
  ovs_bridge br0
  ovs_type OVSPort
```

Usare la VM come collettore sflow

- Necessario configurare VirtualBox o VMWare per collegare in bridge l'interfaccia della Virtual Machine all'interfaccia del computer ospitante



Domande?

Grazie

nino.ciurleo@garr.it

sw.dev@garr.it

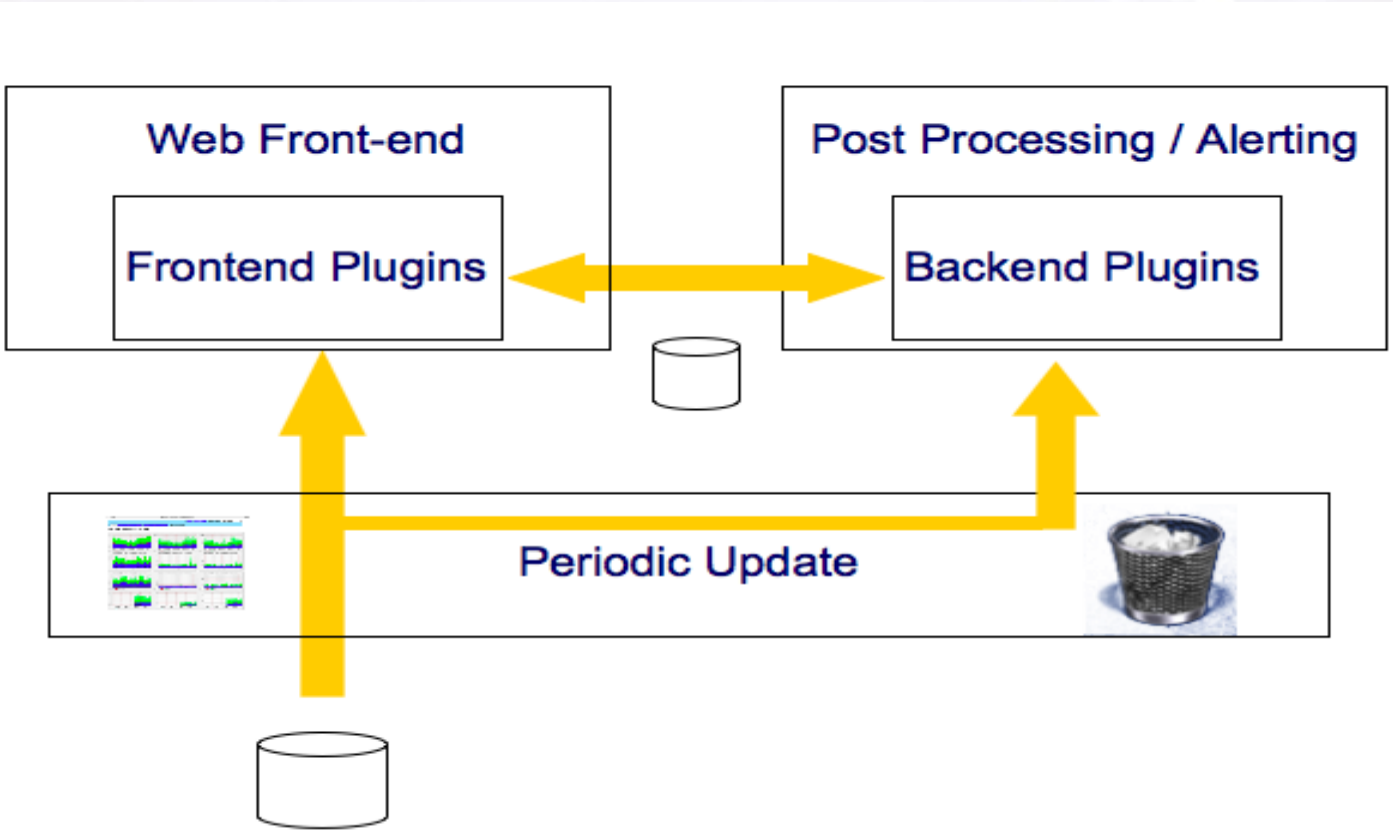
noc@garr.it

Esempio incidente 2

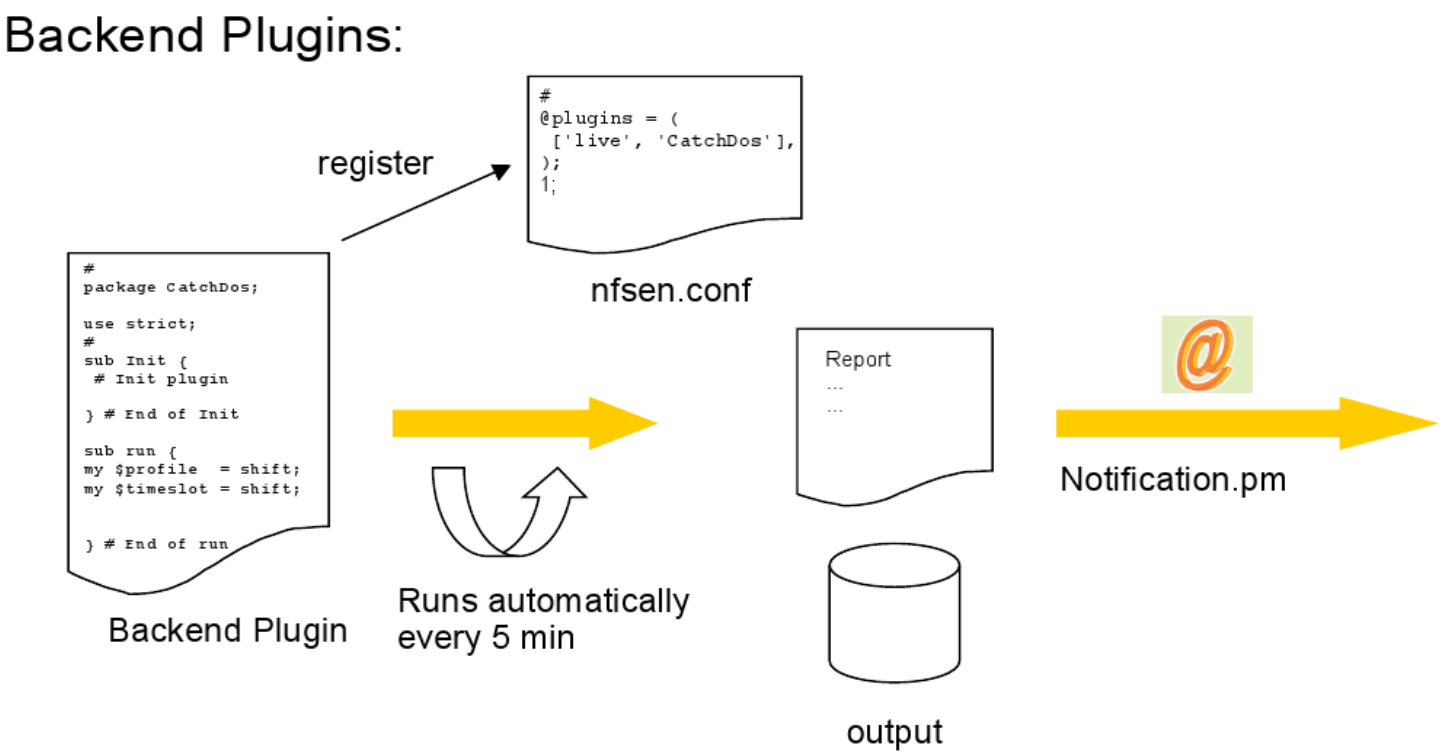
LAB# **ovs-ofctl show br0**
OFPT_FEATURES_REPLY (xid=0x2): dpid:0000e23795a7aa4e
n_tables:254, n_buffers:256
capabilities: FLOW_STATS TABLE_STATS PORT_STATS QUEUE_STATS ARP_MATCH_IP
actions: OUTPUT SET_VLAN_VID SET_VLAN_PCP STRIP_VLAN SET_DL_SRC SET_DL_DST SET_NW_SRC SET_NW_DST SET_NW_TOS SET_TP_SRC SET_TP_DST ENQUEUE

1(host1): addr:fe:10:7c:47:17:06
config: 0
state: 0
current: 10GB-FD COPPER
speed: 10000 Mbps now, 0 Mbps max
2(host2): addr:fe:ab:0e:02:98:1f
config: 0
state: 0
current: 10GB-FD COPPER
speed: 10000 Mbps now, 0 Mbps max
3(spoofer): addr:fe:90:03:81:36:d4
config: 0
state: 0
current: 10GB-FD COPPER
speed: 10000 Mbps now, 0 Mbps max
LOCAL(br0): addr:e2:37:95:a7:aa:4e
config: 0
state: 0
speed: 0 Mbps now, 0 Mbps max
OFPT_GET_CONFIG_REPLY (xid=0x4): frags=normal miss_send_len=0

Plugin: architettura (1/3)



Plugin: architettura (2/3)



Plugin: architettura (3/3)

Backend / Frontend Plugins:

register

```
#
@plugins = (
 ['live', 'CatchDos'],
);
1;
```

nfsen.conf

```
#
package CatchDos;

use strict;
#
sub Init {
 # Init plugin

} # End of Init

sub run {
my $profile  = shift;
my $timeslot = shift;


} # End of run
```

output

Runs automatically

Backend Plugin every 5 min

```
/* Port Tracker
 * Plugin
 */
function
PortTracker_Run($plugi) {
 $portinfo =
GetTopN($plugin_id,
$_SESSION["${plugin_id}

…
} // End of
PortTracker_Run
```

Frontend Plugin

Backend plugin

Funzioni predefinite:

Init

- Questa funzione viene chiamata quando il plugin viene caricato. Lo scopo e' di dare al plugin la possibilita' di inizializzarsi.
- I valori di ritorno sono 0 in caso di successo e 1 in caso contrario.
- Nel caso la funzione Init fallisca il plugin non viene caricato.

Es.

```
sub Init {
return 0;
}
```

Cleanup

- Questa funzione viene chiamata nel momento in cui nfsend viene fermato. Lo scopo e' di dare la possibilita' al plugin di terminare in maniera corretta.

Es.

```
sub Cleanup {
syslog("info", “plugin Terminato");
}
```

Backend plugin

Run

Questa funzione viene chiamata da nfsen ogni volta che ci sono nuovi flussi da analizzare.

- E' il cuore del plugin.

Es.

```
sub Run {
   my $argref = shift;
   my $profile = $$argref{'profile'};   #il nome del profilo sul quale e' installato
   my $profilegroup = $$argref{'profilegroup'}; #gruppo di profili
   my $timeslot = $$argref{'timeslot'}; #il timeslot corrente (es. 200905201015)

   # qui dovrebbe essere inserito il codice del plugin
}
```

Altre variabili disponibili nella funzione Run:

my **$profilepath** = NfProfile::ProfilePath($profile, $profilegroup); **#il path su disco che contiene i dati del profilo**

my **$all_sources** = join ':', keys %{$profileinfo{'channel'}}; **# la stringa con tutte i router sorgenti separate da ":"**

my **$netflow_sources** = "$NfConf::PROFILEDATADIR/$profilepath/$all_sources"; **# la stringa che contiene sia il path che le sorgenti (da passare a nfdump con l'opzione –R)**

my **%profileinfo =** NfProfile::ReadProfile($profile, $profilegroup); **#un hash table che contiene tutti i dati relativi al profilo in uso**

Frontend plugin (opzionale)

- Funzioni predefinite:

  <nome_plugin>_ParseInput (obbligatoria)

  - E' chiamata prima di ogni output sul browser ed ha la funzione

  di parsare i dati dei form.

  - Questa funzione viene chiamata solamente quando sull'interfaccia di nfsen e' selezionato il tab dei Plugin
  - Puo' essere utilizzata per ritornare messaggi

```
Es.
function plugindiprova_ParseInput( $plugin_id ) {
        SetMessage('error', "Errore dal plugin di prova!");
        SetMessage('warning', "Warning dal plugin di prova!");
        SetMessage('alert', "Alert dal plugin di prova!!");
        SetMessage('info', "Info dal plugin di prova!");
}
```

  <nome_plugin>_Run (obbligatoria)

  - Questa funzione viene chiamata dopo che sono stati spediti al browser l'header della pagina e la barra di navigazione

```
Es.
function <nome_plugin>_Run( $plugin_id ) {
        // qui va  il codice
}
```

Comucazione tra backend e frontend (1/2)

- Nel backend

Al fine di potere esequire una funzione del plugin di backend da quello di frontend, occorre definire alcune variabili.

- **Gestione delle richieste del frontend:**

```
our %cmd_lookup = (
'try' => \&RunProc,  #la funzione  RunProc del backend si chiamera' try nel frontend.

);
sub RunProc {
        my $socket = shift;  #la socket di comunicazione con il frontend
        my $opts = shift;  # contiene i parametri

} # End of RunProc
```

- **Ritorno dei risultati al frontend:**

```
$args{'string'}="Ciao dal Backend"
Nfcomm::socket_send_ok($socket, \%args);

Nfcomm::socket_send_error($socket, "Errore");
```

Comucazione tra backend e frontend (2/2)

- Nel frontend:
  - **Richieste al backend:**

    ```
    $out_list = nfsend_query("Pluginname::try", $opts);
    ```

    - Il primo parametro indica il nome della funzione del backend da chiamare
    - il secondo e' un hash table che contiene i parametri
    - $out_list e' l'hash table con i valori di ritorno

  - **Risposte del backend:**

    ```
    print $out_list['string'];
    ```

Esempio completo

Frontend:

```
// Richieste al backend:
$opts = array();

// due scalari
$opts['colour1'] = '#72e3fa';
$opts['colour2'] = '#2a6f99';

// un array
$opts['colours'] = array ( '#12af7d', '#56fc7b');

// chiamata alla funzione in backend
$out_list = nfsend_query("Pluginname::try", $opts);

//Risposte del backend:


// if $out_list == FALSE – it's an error
if ( !is_array($out_list) ) {
    SetMessage('error', "Errore del plugin di Backend");
    return FALSE;
}
$string = $out_list['string'];
$othercolours = $out_list['othercolours'];
print “Il Backend ha risposto: <b>$string</b><br>\n";
```

Backend:

```
#Gestione delle richieste del frontend:
our %cmd_lookup = (
    'try' => \&RunProc,
);
sub RunProc {
my $socket = shift;
my $opts = shift; # riferimento ad un hash


# Lettura dati del frontend
#due scalari
my $colour1 = $$opts{'colour1'};
my $colour2 = $$opts{'colour2'};

# un puntatore ad array
my $colours = $$opts{'colours'};

#Ritorno dei risultati al frontend:

# esempio controllo d’errore
if ( !exists $$opts{'colours'} ) {
    Nfcomm::socket_send_error($socket, "Missing value");
    return;
}
my %args;
my @othercolours = ( ‘rosso', ‘blu' );
$args{'string'} = “Ciao dal plugind di backend."
$args{'othercolours'} = \@othercolours;

 Nfcomm::socket_send_ok($socket, \%args);
} # fine della funzione RunProc
```

Alert Condition

Condizione di Alert computata da un plugin:

- Per far saltare un Alert in base ad una condizione complessa, si usa un plugin per matcharla.
- La funzione **alert_condition** viene lanciata da nfsen dopo l'applicazione dei filtri ai flussi.

```
sub alert_condition {
  my $argref = shift;
  my $alert      = $$argref{'alert'};
            my $alertflows = $$argref{'alertfile'};
            my $timeslot   = $$argref{'timeslot'};
            syslog('info', "Alert condition called:  alert: $alert, alertfile: $alertflows, timeslot: $timeslot");
  # Add your code here
  return 1;
 }
```

Alert Action

- Impostare un'azione complessa scaturita da un alert: si usa un plugin con la funzione **alert_action**

```
sub alert_action {
my $argref = shift;
my $alert    = $$argref{'alert'};
my $timeslot = $$argref{'timeslot'};

syslog('info', "Alert action function called: alert: $alert, timeslot: $timeslot");
# Add your code here
return 1;
}
```

La funzione ParseForm

- Nfsen fornisce una funzione che consente di accedere ai dati presenti nell'array $_POST di php: ParseForm.
- Essa ritorna una lista con i dati e gli errori:

list ($process_form, $has_errors) = ParseForm($parse_opts);

$parse_opts e' un array che contiene tanti elementi quanti sono gli elementi di $_POST che si vogliono parsare.

Ad ogni elemento e' associato un array associativo che descrive le opzioni legate al parametro; le chiavi dell'array sono:

- Required (0 o 1)
- Allow_null (0 o 1)
- Default (valore di default della variabile)
- Match (reg exp o array per verificarne il valore)
- Validate (nome della funzione per un'ulteriore validazione del valore)
  function function_validate(&$var,$opts)
  &$var e' il puntatore al valore da validare
  $opts e' l'array di parametri di quel valore.

Esempio: plugin DoS

- Cosa fa:
  - Plugin di alert che ogni volta che il traffico UDP supera una certa soglia definita come DoS, riempe una pagina web con l'ip della macchina GARR coinvolta nel DoS e l'orario in cui e' avvenuto

Esempio: plugin DoS

- Come funziona:
  - un plugin di backend: calcola il traffico UDP e lo confronta con delle soglie stabilite precedentemente
  - Un plugin di alert: se la soglia e' superata fa scattare alcuni script che calcolano gli IP coinvolti, estrapola l'ip GARR e dati di interesse
  - Un plugin di frontend: visualizza una tabella HTML con l'ip GARR e i dati relativi all'attacco DoS

Esempio: plugin DoS

- Backend plugin NOC.pm:

```
package NOC;
my $nf_filter = 'proto UDP';
my @output =      `$nfdump -M $netflow_sources -T \
                        -r nfcapd.$timeslot  -n 100 -s ip/flows \
                  '$nf_filter'`;
system ("/mnt/nfsen/plugins/NOC_creo_tabella 2>
                              /mnt/nfsen/plugins/appoggio.noc")
```

Esempio: plugin DoS

- Alert plugin: NOC_alert.pm:

```
package NOC_alert;
my $nf_filter = 'proto UDP';
my @output =      `$nfdump -M $netflow_sources -T -r \
                  nfcapd.$timeslot -n 10 -s ip/flows \
                        '$nf_filter'`;
system ("/mnt/nfsen/plugins/elaboro_NOC $timeslot \
2> /mnt/nfsen/plugins/log_NOC");
```

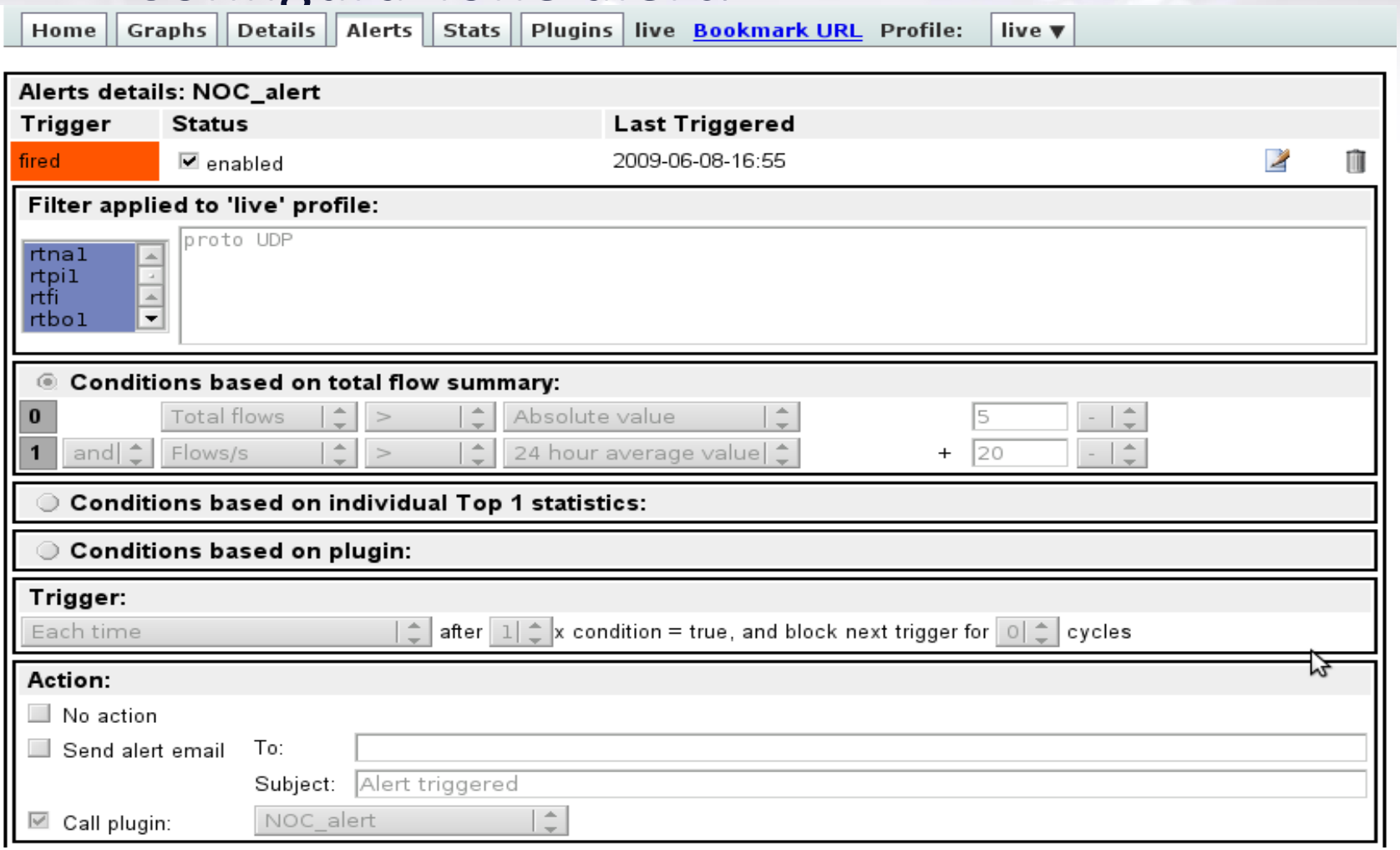
Esempio: plugin DoS

- Frontend plugin $http_dir/plugins/NOC.php:

```
<?php
 /* NOC plugin*/
function NOC_ParseInput( $plugin_id ) {}
function NOC_Run( $plugin_id ) {
$VARDIR = "/mnt/nfsen/www/plugins";
print "<h3>NOC Logfile</h3>\n";
$logfile = "$VARDIR/NOC_output.log";
echo htmlspecialchars($logfile) ;
include $logfile;
print "</pre>\n";
} // End of NOC_Run
?>
```

Esempio: plugin DoS

- Configurazione alert:



Esempio: plugin DoS

- RISULTATO:

Domande

1. Quale protocollo si usa per l'esportazione dei flussi sugli switch:
    1. Netflow
    2. Sfow (CORRETTA)
    3. Sugli switch non e' possibile esportare flussi
2. Nel protocollo Neflow un flusso e':
    1. Unidirezionale (CORRETTA)
    2. Bidirezionale
    3. Uguale ad un pacchetto
3. I profili di nfsen servono per:
    1. Generare allarmi in base alle condizioni veficatesi nei flussi
    2. Ottenere una rappresentazione grafica di un particolare tipo di traffico (CORRETTA)
    3. Estendere le funzionalita' di nfsen
4. I plugins di nfsen servono per:
    1. Generare allarmi in base alle condizioni veficatesi nei flussi
    2. Ottenere una rappresentazione grafica di un particolare tipo di traffico
    3. Estendere le funzionalita' di nfsen (CORRETTA)

Nfsen

Demo:

- Navigazione
- Dettagli
- spostamento cursore
- scelta intervallo di tempo singolo o “lungo”
- demo per processare filtri e dati
- cambio protocollo/unita' di misura
- vedere qualche picco
- aggregazioni varie
- finestra “lookup”

Identificazione di traffico “malevolo”

Esempio (Presunti IP che fanno DoS):

nfdev:~$ ***nfdump -r /data/nfsen/profiles-data/live/router1/2009/05/20/nfcapd.200905201400 -a -l 40000 -o extended 'proto udp and bpp < 200'***

Date flow start *Duration* *Proto* *Src IP Addr:Port* *Dst IP Addr:Port* *Packets* *Bytes* *pps* *bps* *Bpp* *Flows*

2009-06-03 14:37:50.813 414.316 UDP 210.188.235.117:32807 -> xxx.xxx.8.9:53 87874 3.6 M 212 72960 43 16

2009-06-03 13:59:17.225 3922.643 UDP XXX.XX.80.47:1194 -> 84.221.68.167:6244 119843 19.3 M 30 41373 169 106

Summary: total flows: 651996, total bytes: 92.4 M, total packets: 1012985, avg bps: 193379, avg pps: 252, avg bpp: 95
Time window: 2009-06-03 13:58:17 - 2009-06-03 15:05:06
Total flows processed: 7938624, Records skipped: 0, Bytes read: 412816524
Sys: 1.268s flows/second: 6260354.4 Wall: 1.190s flows/second: 6666272.6

Identificazione di traffico “malevolo”

Esempio (Presunti IP sorgenti di scanning e porte bersaglio):

nfdev:~$ ***nfdump -r /data/nfsen/profiles-data/live/router1/2009/05/20/nfcapd.200905201400 –A srcip,dstport -s record/packets "not proto icmp and bytes < 100 and bpp < 100 and packets < 5 and not port 80 and not port 53 and not port 110 and not port 123 and not port 22"***

Aggregated flows 30404
Top 10 flows ordered by packets:

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2009-05-20 13:58:56.362	289.563	0	**87.177.37.47**:0	->	0.0.0.0:**1080**	185	7614	182
2009-05-20 13:58:50.298	296.047	0	**195.155.76.158**:0	->	0.0.0.0:**443**	66	2912	66
2009-05-20 13:59:52.617	282.893	0	**168.170.104.98**:0	->	0.0.0.0:**445**	54	2584	54
2009-05-20 13:58:53.117	295.026	0	**212.238.91.31**:0	->	0.0.0.0:**445**	47	2256	45
2009-05-20 13:58:51.228	292.875	0	**168.170.128.34**:0	->	0.0.0.0:**445**	45	2160	45
2009-05-20 13:58:51.678	292.002	0	**168.173.164.192**:0	->	0.0.0.0:**445**	43	1995	43
2009-05-20 13:58:52.974	289.299	0	**169.113.129.189**:0	->	0.0.0.0:**445**	42	2016	42
2009-05-20 13:59:51.397	295.530	0	**168.170.170.9**:0	->	0.0.0.0:**445**	42	2016	42
2009-05-20 13:58:51.872	296.238	0	**168.170.186.180**:0	->	0.0.0.0:**445**	38	1824	38
2009-05-20 13:58:50.895	287.792	0	**168.170.118.100**:0	->	0.0.0.0:**445**	36	1720	35

Summary: total flows: 41946, total bytes: 2.1 M, total packets: 45408, avg bps: 47839, avg pps: 126, avg bpp: 47
Time window: 2009-05-20 13:58:49 - 2009-05-20 14:04:49
Total flows processed: 185341, Records skipped: 0, Bytes read: 9637876
Sys: 0.128s flows/second: 1447897.4 Wall: 0.682s flows/second: 271443.8

Cisco vs Juniper router (1/2)

- Esempi di configurazione (v5):
  - Cisco
    - Configurazione interfacce

      interface FastEthernet0/0

      ip route cache flow
    - Esportazione dei flussi

      ip flow-export

      ip flow-export version 5

      ip flow-export destination 172.16.0.1 20000

      ip flow-cache timeout active 5

      ip flow-cache timeout inactive 1000

Cisco vs Juniper router (2/2)

- Juniper
  - Definizione del filtro:

    set firewall family inet filter NETFLOW-SAMPLE term default then sample

    set firewall family inet filter NETFLOW-SAMPLE term default then accept
  - Configurazione interfacce:

    set interfaces fe-0/1/0 unit 0 family inet filter input NETFLOW-SAMPLE

    set interfaces fe-0/1/0 unit 0 family inet filter output NETFLOW-SAMPLE
  - Configurazione collezionatore

    set forwarding-options sampling input family inte rate 1000

    set forwarding-options sampling output cflowd 172.16.0.1 port 20000

    set forwarding-options sampling output cflowd version 5

    set forwarding-options sampling output cflowd autonomous-system-type [peer|origin]