Estensioni di NfSen per il monitoraggio delle reti

Massimo Ianigro – Claudio Marotta
Consiglio Nazionale delle Ricerche
Istitituto di Studi sui Sistemi Intelligenti per l'Automazione

9° Workshop GARR - ”Al servizio degli utenti”
Roma, 15-18 giugno 2009

Sommario

- Introduzione
- Cosa è NetFlow
- Gestione dei dati mediante NfSen
- Automazione dell'analisi dei dati e ambito di applicazione
- Risultati
- Sviluppi futuri

Introduzione

La conduzione di una infrastruttura di rete complessa si fonda sulla capacità di:

- Misurare i fenomeni fondamentali
- Rappresentare i valori misurati
- Interpretare il senso delle misure e trarne delle conseguenze

Massimo Ianigro – CNR ISSIA

Misurare: NetFlow

NetFlow è una tecnologia introdotta originariamente da Cisco a supporto del miglioramento delle performance di fast-switching (US Patent 6243667 – expire 2016)

- Differenti versioni rilasciate nel tempo, quelle correntemente più utilizzate sono v5 e v9
- Netflow v9 -> IPFIX attraverso un processo di standardizzazione IETF (RFC 3954, 5101-3)
- Non mostra il contenuto (payload)
- Possibilità di campionamento statistico

NetFlow

Un flusso è una sequenza di dati unidirezionale per la quale coincidono:

- IP sorgente
- IP destinazione
- Porta UDP/TCP sorgente (0 per altri prot.)
- Porta UDP/TCP destinazione (0 per altri prot.)
- Protocollo IP (6 TCP, 17 UDP, 1 ICMP,etc)
- Interfaccia di ingresso (SNMP index)
- IP Type of Service

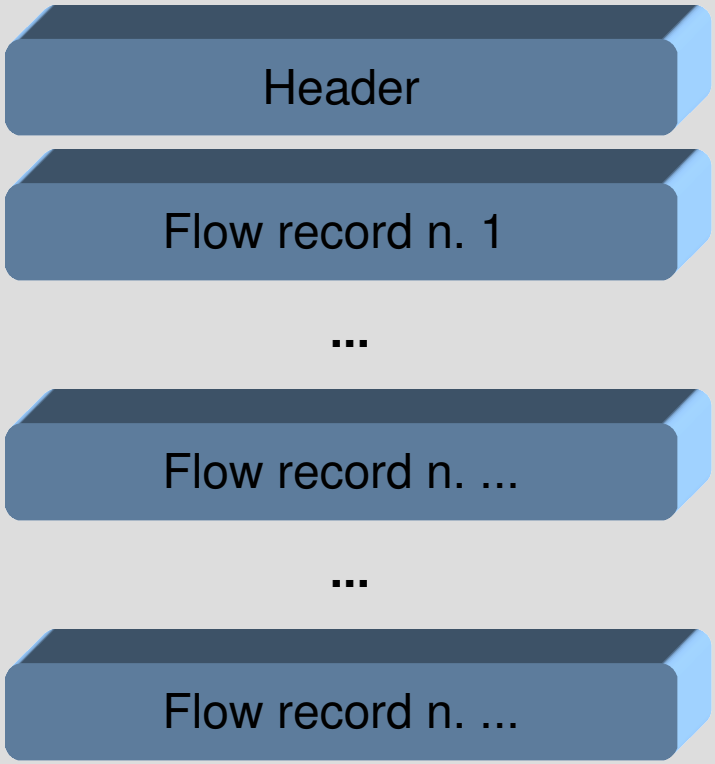
NetFlow

I dati vengono estratti quando

- Il flusso viene terminato (FIN/RST)
- E' trascorso un tempo massimo di assenza del traffico nel flusso
- E' trascorso un tempo massimo dalla apertura del flusso
- L'apparato non ha più risorse per memorizzare le informazioni per ulteriori nuovi flussi

NetFlow

Il set di dati esportato da un pacchetto NetFlow (UDP) è organizzato cosi:



NetFlow

Le principali informazioni presenti:

- Versione (header)
- System uptime (header)
- Modalità e tempo di campionamento (header)
- 7-pla identificativa del flusso (record)
- Pacchetti nel flusso (record)
- Bytes transitati al layer 3 (record)
- Riferimenti interfacce in-out (record)
- Tcp flags (record)
- Source/destination A.S.(record)

NetFlow

Le informazioni prodotte possono essere esportate dall'apparato di rete ed utilizzate per il monitoraggio del traffico

E' supportato anche da altri produttori di hardware (Juniper, Enterasys, Extreme, Foundry, Alcatel/Riverstone/Lucent, Packeteer, ...)

Esistono software che producono dati 'NetFlow' partendo dall'analisi del traffico 'by wire' (nProbe, softflowd, fprobe, ...)

NetFlow

Esistono molti software in grado di trattare i dati NetFlow

- Vasta offerta di prodotti commerciali
- Molte soluzioni sono orientate al capacity-planning, aggregazione&rappresentazione o implementano funzionalità orientate alle attività dei 'carrier' (accounting&billing, traffic engineering)
- NfSen (NetFlowSENsor) è una valida alternativa open-source (BSD license), ©SWITCH

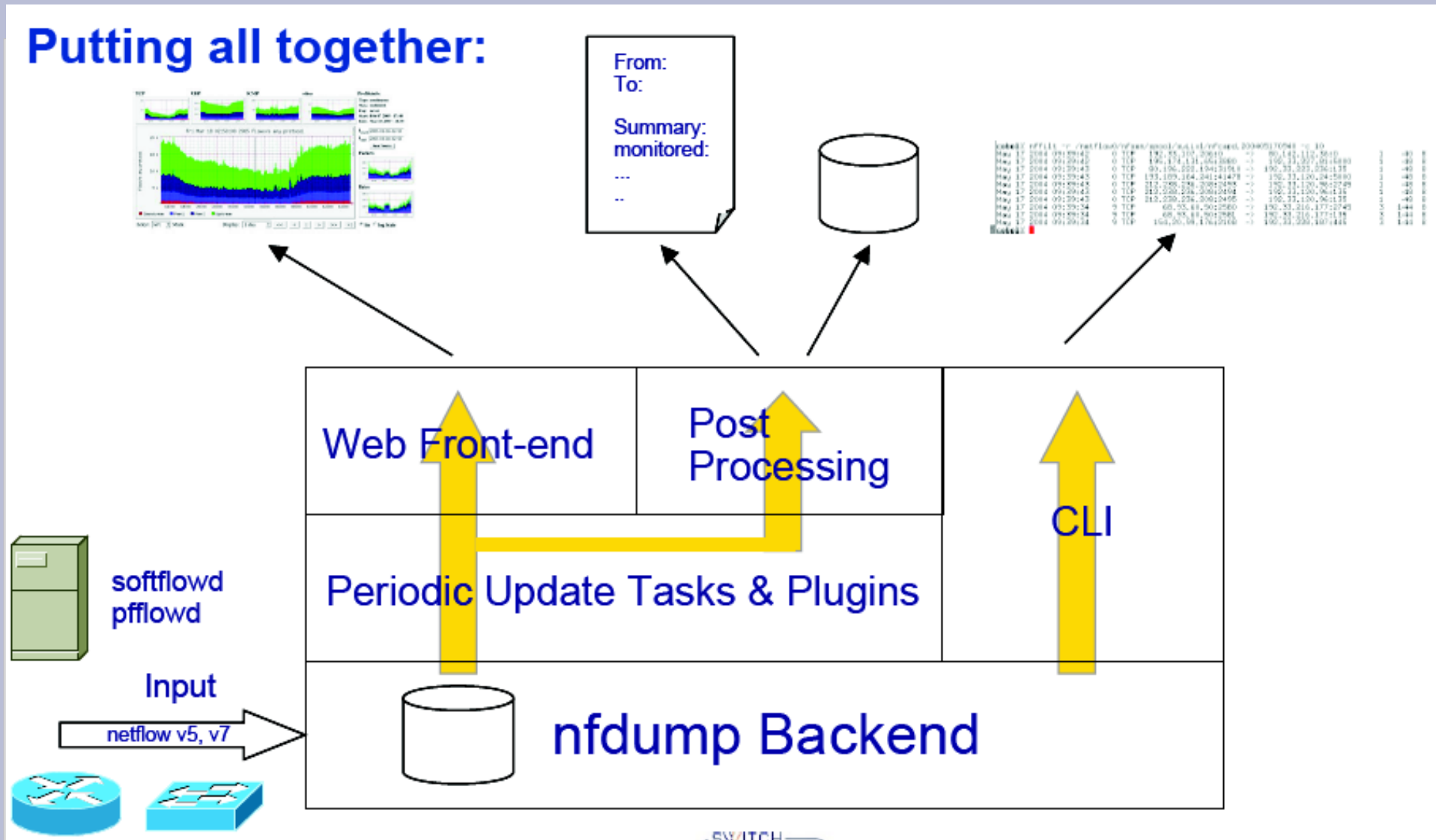
Rappresentare: NfSEN

NfSen è un front-end grafico web based che utilizza i tools di nfdump

Esso consente:

- Visualizzazione dei dati (RRD)
- Funzionalità di data mining con molteplici possibilità di selezione dei dati (per sorgente, per arco temporale, per host/protocollo/porta/rete,...)
- Meccanismi di alerting su varie condizioni
- **Possibilità di estendere le funzionalità tramite plugin**

NfSEN



Massimo Ianigro – CNR ISSIA

E allora?

Come un APM vorrebbe la propria rete:

- utenti disciplinati
- macchine censite
- traffico non ostile
- servizi dichiarati
- connettività mai satura
- ... telefono silenzioso

Invece...

Una rara foto di un APM nella sua quotidianità:

- Macchine non censite
- Applicazioni bandwidth wasting
- Virus, worm, botnet, ...

Ambito di applicazione

In considerazione della complessità della infrastruttura da gestire si è pensato di sviluppare degli strumenti 'automatici' per il monitoraggio e l'alerting della rete CNR di Bari:

- 9 sedi distinte
- circa 700 utenti
- 20 strutture indipendenti (Istituti o sezioni) gestite da vari referenti locali
- > 800 punti di rete connessi in una sola sede..

Ambito di applicazione

I problemi più frequenti:

- Attivazione di nuove macchine sulla rete
- IP-squatting
- Compromissione di host
- Traffico peer-to-peer
- Applicazioni bandwidth consuming
- ”geolocalizzazione” degli IP

Approccio utilizzato

Partendo dalle informazioni prodotte dal router di frontiera, ed estratte mediante NetFlow, sono stati messi a punto degli strumenti di monitoraggio e reporting (web-based, email)

E' in fase di consolidamento in un unico package l'insieme dei vari strumenti realizzati:

Monitoring, **A**lerting, **R**eacting, **P**lug-**I**n **O**n **N**fsen (MARPION) - www.ba.cnr.it/marpion

Cosa riusciamo ad ottenere

In presenza di una infrastruttura 'fully manageable', riusciamo a segnalare ai referenti locali eventi quali:

- Attivazione di un nuovo IP sulla rete
- Migrazione di un IP su altro hardware
- Migrazione di un IP su un'altra porta di rete (cambio di porta sullo switch e/o cambio di switch)
- Assenza di registrazione DNS

Cosa riusciamo ad ottenere

- Segnalazione di traffico ostile:
  - Scanning verso l'esterno
  - Traffico probabilmente riconducibile al peer-to-peer
- Elevato utilizzo della banda
- ...

Massimo Ianigro – CNR ISSIA

Struttura del sistema

- Plugin di NfSEN che analizza i dati acquisiti da nfcapd a intervalli regolari (5 minuti)
- Modulo di archiviazione degli eventi su database (postgresql)
- Modulo di interfacciamento con i dispositivi di rete per l'acquisizione di informazioni addizionali
- Modulo di gestione dei dispositivi di rete
- Modulo di notifica per la segnalazione real-time o in modalità 'digest' degli eventi

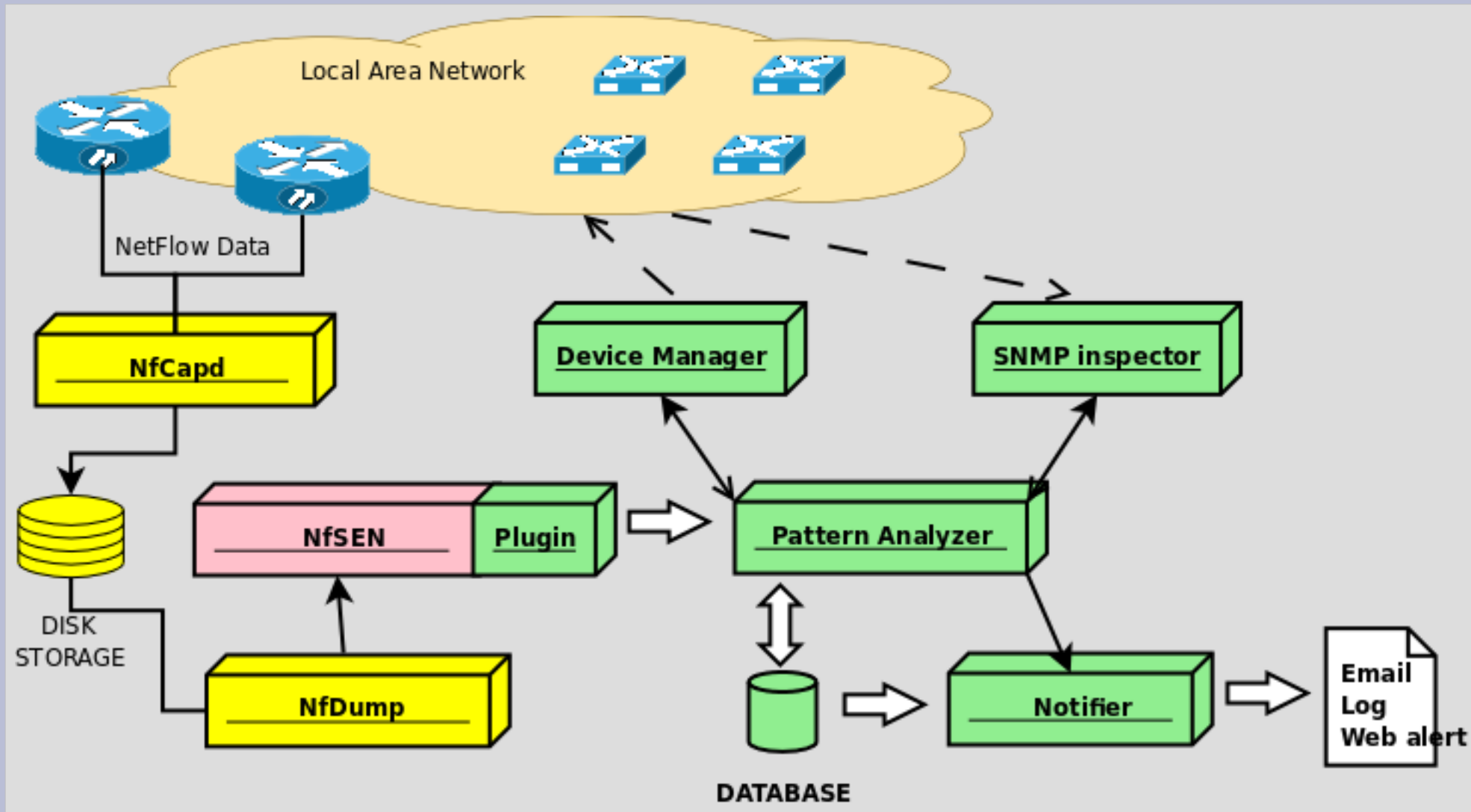
Struttura del sistema

- Componente di 'difesa attiva' (riconfigurazione dinamica del router di frontiera, shutdown della porta fisica sullo switch dove è connesso l'host).
  Al momento sono le modalità previste sono le seguenti:
  - Emulazione terminale (expect)
  - SNMP
  - NETCONF RPC (RFC 4741)

Struttura del sistema

- Riconoscimento eventi potenzialmente ostili:
  - Apertura di un elevato numero di flussi verso l'esterno (port-scanning, worm spreading, ...)
  - Apertura di un elevato numero di flussi dall'esterno (DDOS, peer to peer, ...)
  - Erogazione servizi (three-way handshaking) verso l'esterno
- Possibilità di definire differenti domini di competenza e differenti responsabili
- Elevata configurabilità (reti CIDR, referenti multipli, white-list, caratterizzazione host, ...)

The Big Picture



Risultati ottenuti

- Il referente locale non è più un semplice 'erogatore' di indirizzi IP ma diventa parte attiva nel processo di gestione e controllo della infrastruttura
- Determinate anomalie (es. Virus Conficker, P2P aggressivi, compromissioni) vengono rilevate con tempestività, talvolta prima degli utenti stessi e, sopratutto, prima che se ne accorga il GARR CERT

Open Issues

- Spoofing
- Corretta individuazione delle interfacce 'end-user' sugli switch
- Messa a punto di meccanismi di 'id lowering' per i P2P tipo ED2K
- Implementazione meccanismi di forecasting (es. Medie mobili, Holt-Winters, ...) o di learning che consentano di classificare il traffico ”medio” di un host e conseguentemente possano automatizzare il riconoscimento delle anomalie

What's next

I prossimi passi saranno:

- Re-ingegnerizzazione del software e automazione dei processi di installazione
- Realizzazione di interfacce verso altri dispositivi (es. configurazione/monitoraggio in emulazione web)
- ...
- Public release

The end

Massimo Ianigro: tel. 080 5929424 - email: ianigro@ba.issia.cnr.it

LINK UTILI

IETF IPFIX (RFC 3955)
http://www.ietf.org/rfc/rfc3955.txt

CISCO IOS NetFlow
http://www.cisco.com/go/netflow

TF-NGN@SWITCH - Realtime Traffic Flow Measurement
http://www.switch.ch/network/projects/completed/TF-NGN/floma/software.html

Tools NetFlow
http://www.networkuptime.com/tools/netflow/

NfSEN
http://nfsen.sourceforge.net/

Link utili

NfDump
http://nfdump.sourceforge.net/

MARPION - Monitoring, Alerting, Reacting, Plug-In On Nfsen
http://www.ba.cnr.it/marpion/

NETCONF (RFC 4741)
http://tools.ietf.org/html/rfc4741