THE ITALIAN RESEARCH & EDUCATION NETWORK | Consortium GARR

Tutorial Sicurezza

Gestione quotidiana della sicurezza

Roberto Cecchini, Simona Venuti

GARR WS14 | Roma, 2 e 4 dicembre 2014

Agenda

- wireshark
- NfSen
- argus

wireshark

wireshark perche'?

Nella gestione quotidiana della sicurezza wireshark risponde a dubbi e quesiti di questo tipo:

- Come mai la rete e' lenta/ferma/congestionata?
- Come funziona il routing della mia rete?
- Da cosa dipende il il malfunzionamento della subnet X?
- E perche' i PC del terzo piano vanno in rete pianissimo?
- Mi pare/Mi hanno segnalato di avere un virus ma l'antivirus dice di no

In reti complesse, oppure dove girano applicativi complessi e' oneroso risalire alla sorgente reale di un problema, o al malfunzionamento di un apparato di rete (magari uno stupido HUB nel sottoscala del laboratorio X), o alla rilevazione di un attacco informatico

Wireshark puo' essere utile

Elementi packet capturing

Vengono catturati pacchetti di livello 2 (frames)

Modalita' promiscua sull'interfaccia

- Richiede permessi di root per accedere all'interfaccia
- L'interfaccia riceve il traffico di tutto il segmento di rete
- Si comporta come bridge trasparente

In reti switched si configura una SPAN (o mirror) port sullo switch per avere tutto il traffico di tutti i segmenti

Wireshark cenni generali

Cattura pacchetti e frames, li ricompone li rende umanamente leggibili. Una volta convertiti il software permette la completa riclassificazione, ordinamento, raggruppamento

- Analizzatore in TEMPO REALE di tutti i protocolli
- Visualizzazione immediata dei problemi
- Potente interfaccia grafica
- Potente interfaccia a riga di comando (tshark)
- Possibilita' di scomporre il traffico in qualsiasi modo
- Esportazione di parti di traffico su criteri arbitrati (editcap)

wireshark requisiti

Wireshark si puo' utilizzare con profitto anche su semplici PC desktop

E' fondamentale capire in quale semento di rete mettere wireshark

- Una buona CPU per l'elaborazione in tempo reale
- Almeno 256Mb di RAM
- Almeno 100Mb di disco (dipende da quanti dati si vuole catturare)
- Una scheda di rete che supporti il modo promiscuo
- Permessi di root/administrator
- Librerie pcap

Wireshark funzionamento

Installazione:

- Linux:

  apt-get install wireshark

- Windows:

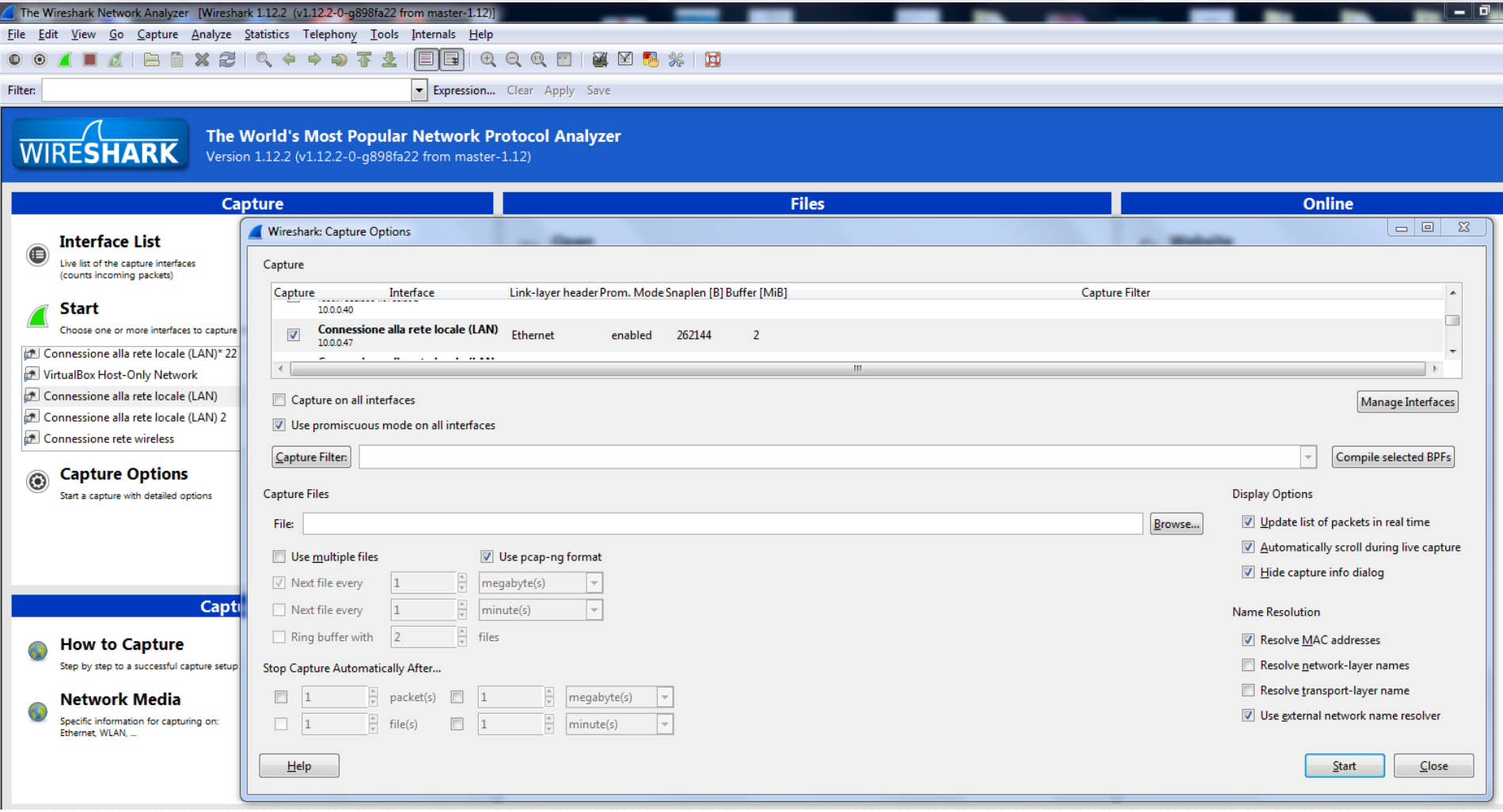
  Da http://www.wireshark.org scaricare l'eseguibile

  Lanciare l'eseguibile si installazione

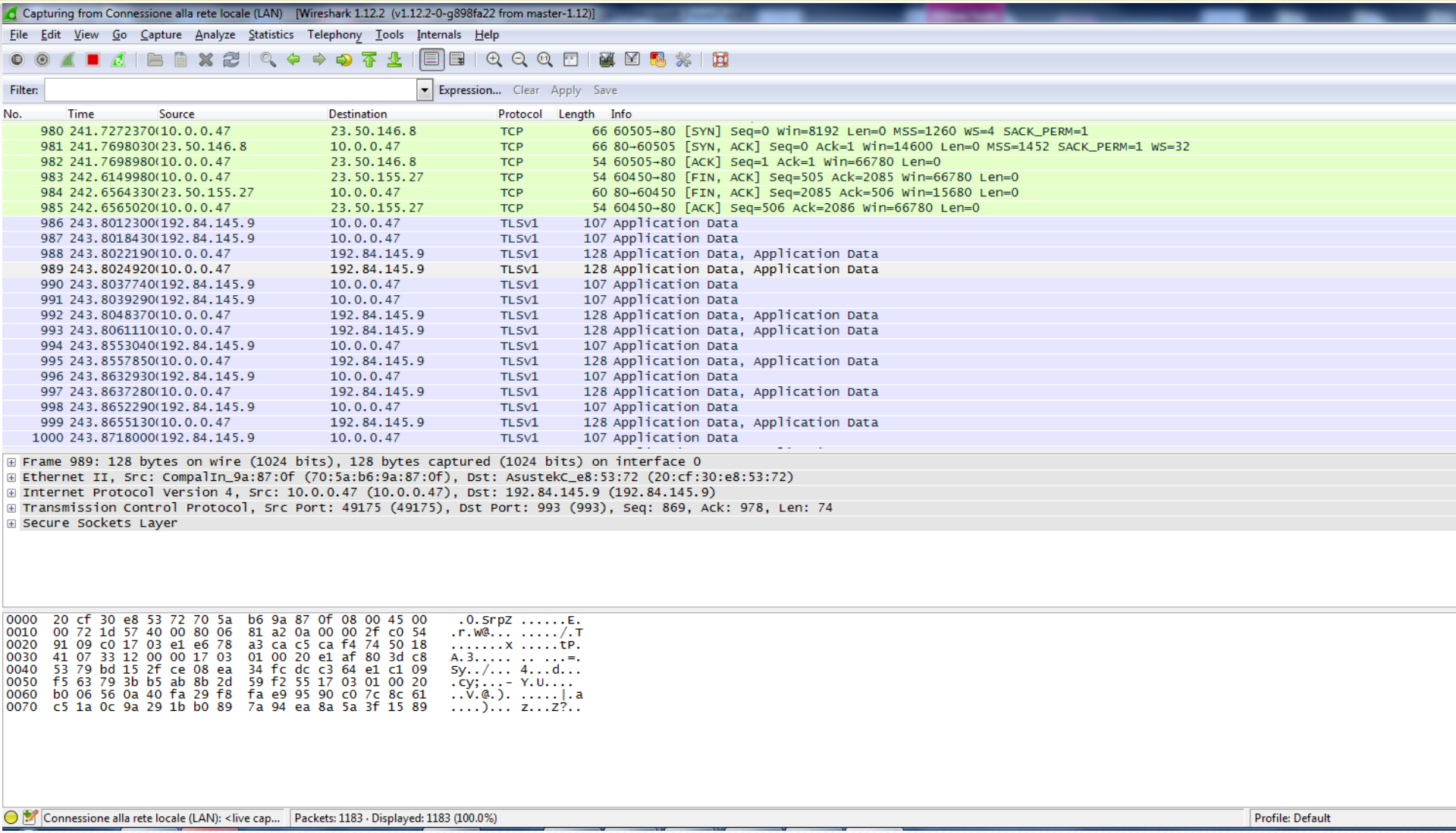
Eseguire wireshark:

- Linux: eseguirlo da root
- Windows: lanciarlo da Administrator

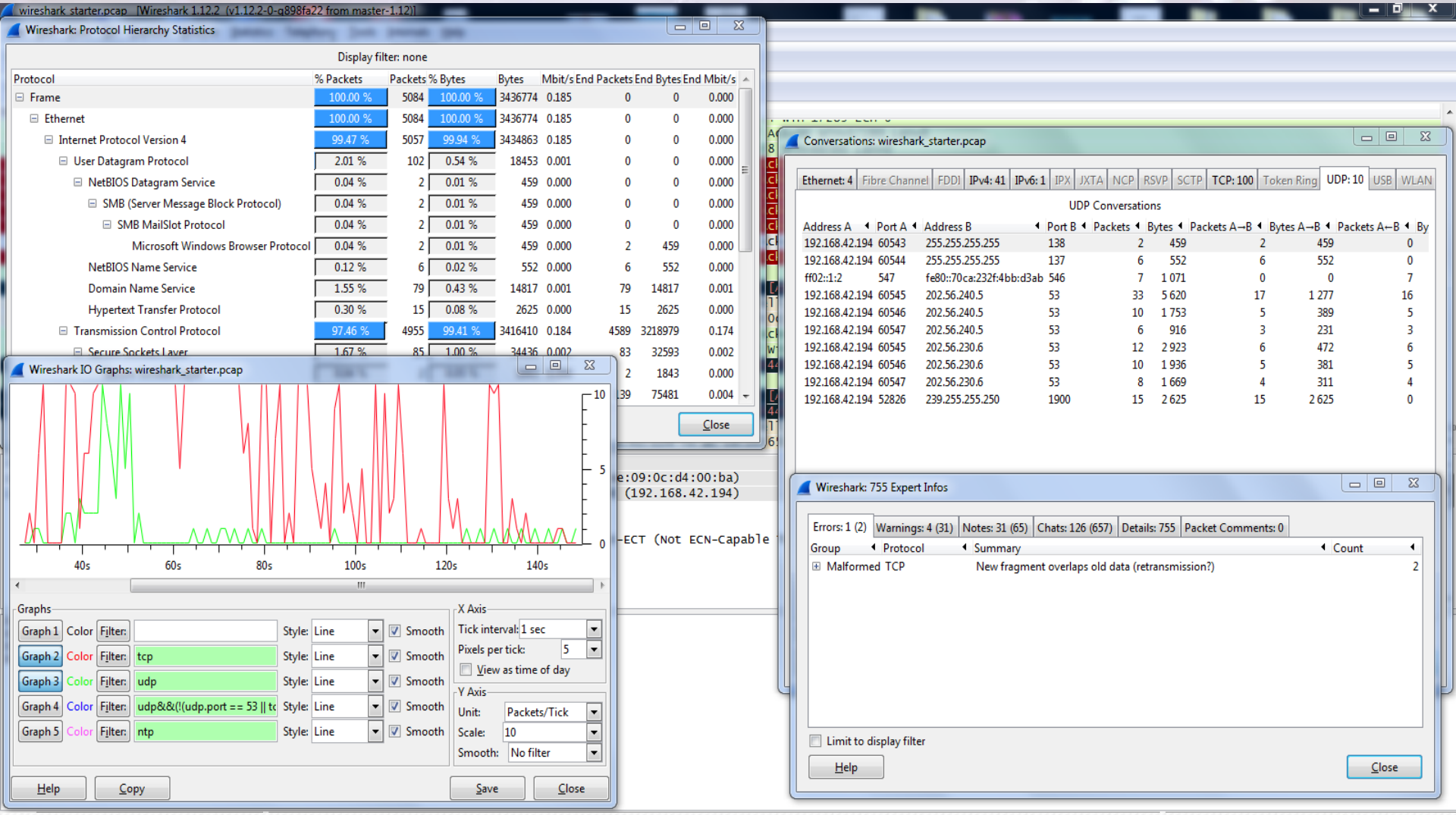
Wireshark cattura



Schermata di traffico



Wireshark analisi traffico



tshark

tshark [**-2**] [**-a** <capture autostop condition>] ... [**-b** <capture ring buffer option>] ... [**-B** <capture buffer size>] [**-c** <capture packet count>] [**-C** <configuration profile>] [**-d** <layer type>==<selector>,<decode-as protocol>] [**-D**] [**-e** <field>] [**-E** <field print option>] [**-f** <capture filter>] [**-F** <file format>] [**-g**] [**-h**] [**-H** <input hosts file>] [**-i** <capture interface>|-] [**-I**] [**-K** <keytab>] [**-l**] [**-L**] [**-n**] [**-N** <name resolving flags>] [**-o** <preference setting>] ... [**-O** <protocols>] [**-p**] [**-P**] [**-q**] [**-Q**] [**-r** <infile>] [**-R** <Read filter>] [**-s** <capture snaplen>] [**-S** <separator>] [**-t** a|ad|adoy|d|dd|e|r|u|ud|udoy] [**-T** fields|pdml|ps|psml|text] [**-u** <seconds type>] [**-v**] [**-V**] [**-w** <outfile>|-] [**-W** <file format option>] [**-x**] [**-X** <eXtension option>] [**-y** <capture link type>] [**-Y** <displaY filter>] [**-z** <statistics>] [**--capture-comment** <comment>] [<capture filter>]

tshark -G [column-formats|currentprefs|decodes|defaultprefs|fields|ftypes|heuristic-decodes|plugins|protocols|values]

tshark

E’ l’interfaccia a linea di comando di wireshark

Funziona come tcpdump, ma ha la superiore potenza di wireshark

E’ molto utile da utilizzare in script di shell o programmi

Lista delle interfacce disponibili: **thark –D**

Cattura solo 1000 pacchetti: **thark –i #interfaccia –w file_out –c 1000**

Legge da file: **thark –r file.pcap**

Applicazione di filtri: **tshark –i #i –f FILTRO_sintassi_tcpdump**

Applicazione filtro complesso su file: **tshark –i #i –R filtro_file**

tshark statistiche

E’ il comando che fa tutto quello che si puo’ fare da interfaccia grafica

tshark –z conv,type[.filter]
Restituisce tutte le conversazioni di un certo tipo per un filtro

tshark –z expert,note.tcp
Restituisce, dal menu «expert», tutti i frames TCP con severity >= note

tshark –z follow.prot.mode.filter[.range]
Restituisce lo streaming TCP o UDP fra due nodi

Esempio:
tshark -z "follow,tcp,ascii,200.57.7.197:32891,200.57.7.198:2906"

Altre statistiche

tshark -z hosts[,ipv4][,ipv6]

Restituisce qualsiasi pacchetto IPv4 o IPv6 in formato host

tshark -z http,stat, oppure -z http,tree oppure -z http_req,tree oppure -z http_srv,tree

Restituisce statistiche sull'utilizzo del protocollo HTTP

tshark -z icmp,srt[,filter]

Restituisce statistiche ICMP SRT

tshark -z smb,sids oppure -z smb,srt[,filter]

Restituisce statistiche sull'utilizzo del protocollo SMB

tshark -z sip,stat[,filter]

Restituisce statistiche sul protocollo SIP

etcetcetc

altre utility a linea di comando

rawshark

Legge lo stream dei pacchetti da un file

Esempio: **rawshark -d proto:http -r capture_file**

editcap

Compie ulteriori operazioni sui file binari pcap

Esempio: **editcap -d file.pcap file1.pcap 1 100**

Legge 100 pacchetti di file.pcap, -d droppa i pacchetti duplicati (DUP), scrive il risultato in file1.pcap1

mergecap

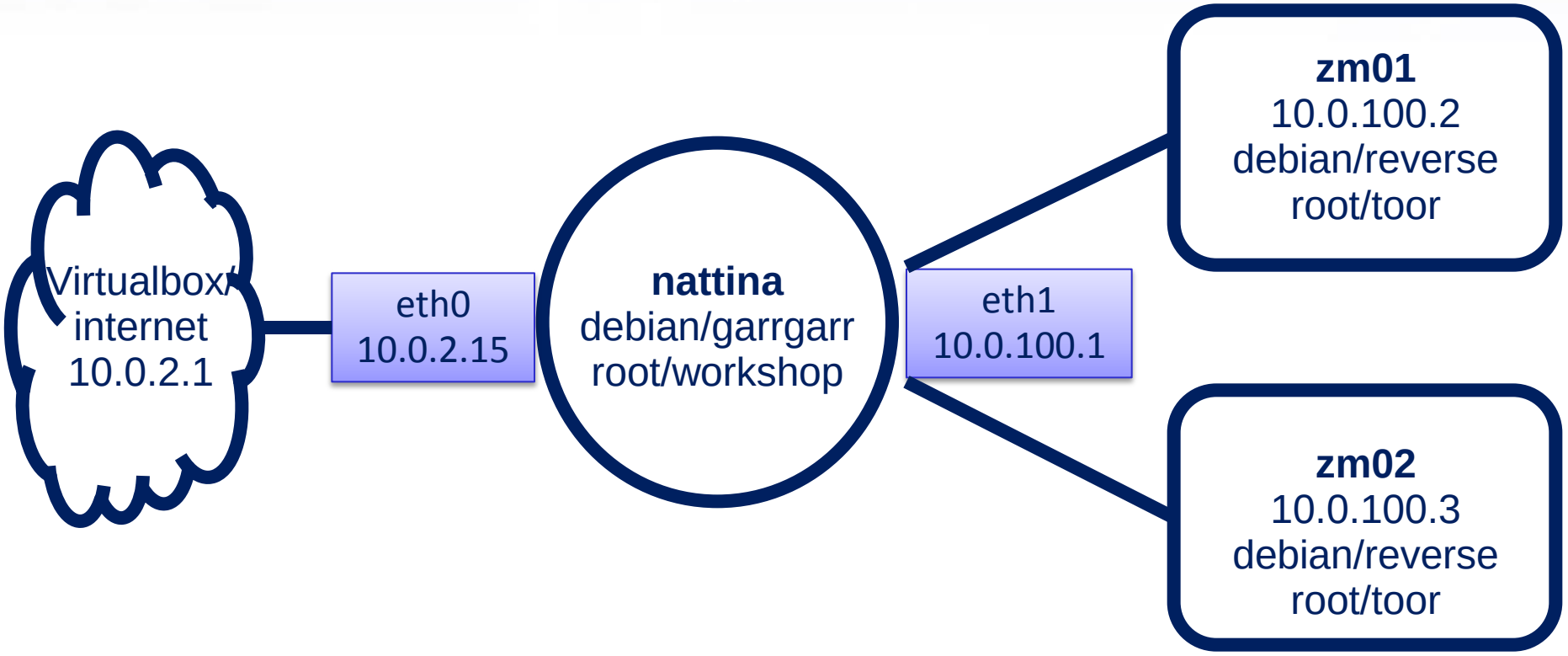
Mescola piu' file .pcap in un unico file, troncando o concatenando

Esempio: **mergecap -a -w newcapture.pcap capture.pcap capture1.pcap**

text2pcap legge ASCII hex dump file e li trasforma in formato .pcap

Esercitazione

Scenario



Esercitazione

Il GARR-CERT vi scrive che una vostra macchina X ha un virus non meglio specificato. Dai log inviati dal CERT non riuscite a trovare riscontro

Lo scopo e' trovare il malware installato sulla macchina, tramite wireshark.

Supponiamo che abbiate catturato una sessione di traffico della macchina X e che sia sul desktop di nattina

Su nattina entrare come utente debian/garrgarr

Lanciare wireshark

Aprire il file .pcap sul desktop

Trovare il malware

Suggerimento

Il malware solitamente viene preso/installato

navigando su pagine web:

Io controllerei traffico strano

E pacchetti HTTP

NfSen

NfSen perche'?

Ogni APM quotidianamente si trova ad affrontare domande di questo tipo:

- Cosa ha causato questo picco nelle statistiche di traffico?
- Quali sono i top talkers/ le top subnet della mia sede?
- Quali sono le applicazioni piú utilizzate dai miei utenti?
- Qual e' il traffico relativo a questo incidente avvenuto il tale giorno?
- Si puo' analizzare questo DoS? Da quali indirizzi IP parte?

Gli strumenti tradizionali di monitoraggio basati sul protocollo SNMP non sono in grado di rispondere …

NfSen e' una possibile semplice risposta

NfSen vs SNMP

SNMP	NfSen
Sorgente: i contatori dei router (numero dei pacchetti e ottetti)	Sorgente: qualsiasi apparato di rete router, switch, NAT server, server
Informazioni solo su interfacce fisiche Contengono solo il traffico aggregato	Informazioni relative a qualsiasi tipo di flusso, sessione, interfaccia
Traffico raw Servono altri strumenti per l'analisi	Traffico analizzabile per protocollo, ip, rete, porta etc. Analisi GRAFICA Analisi a linea di comando (nfdump)

NfSen vs IDS

IDS	NfSen
Pesantezza a livello di CPU, carico di rete, occupazione spazio disco	Leggero, flessibile, installabile ovunque, “zippabile”
Invasivo sulla privacy:ispezione del contenuto dei pacchetti	Rispettoso della privacy: ispezione solo degli header di pacchetto
Complessita' di configurazione di allarmi e individuazione traffico malevolo	GRAFICI! Sistema semplicissimo di allarmistica e potente nella personalizzazione

Elementi NetFlow

- Inizialmente sviluppato da Cisco
- Diventato uno standard “de facto”
- Implementato tutti i costruttori di hardware
- Esempi:
  - Juniper: c/jflowd
  - Alcatel:
  - Huawei: NetStream

NetFlow versioni

- V5, supportata da quasi tutti i vendor e ancora la più utilizzata
- V7, per gli switch catalyst della serie 5000
- V8, come la 7 con in più la possibilità di esportare flussi aggregati
- V9, più 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, il 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, le informazioni trasportate:
  - Indirizzi 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

NfSen – Cenni generali 1/2

NfSen puo' svolgere diversi compiti, sia a livello di analisi delle performance della rete che per la sicurezza della stessa

Analisi performance:

- gestione del traffico di rete
- l'ottimizzazione del routing
- la rilevazione di problemi
- Matrici di traffico
- Applicazioni e/o protocolli e/o porte piu' utilizzati
- Occupazione della banda

NfSen – Cenni generali 2/2

Per quanto riguarda la sicurezza di una rete:

- Analisi picchi di rete (picchi di flussi o di # di pacchetti o di traffico)
- Analisi incidenti di sicurezza
- Analisi e rilevamento BotNet e/o zombie
- Anomalie di traffico dovute a sfruttamenti di nuove vulnerabilita'
- Profilatura di macchine infette o compromesse
- Rilevazione scanport/probe
- Rilevazione server non autorizzati (DNS, NTP, WWW)

NfSen tutorial

Oggi invece vogliamo utilizzare questo strumento per aiutare gli APM ad individuare quale macchina dietro un NAT fa traffico malevolo

Scenario: Il GARR-CERT apre un incidente per una macchina della vostra rete e vi da' pochissime informazioni: data, IP, porta sorgente. L'IP in questione e' un NAT server che da' la rete a un elevato numero di client. Senza adeguati strumenti e' difficoltoso risalire alla macchina interna infetta e/o compromessa.

NB: il GARR nelle AUP chiede espressamente che in caso di incidente o violazione, una struttura deve sempre essere in grado di risalire al responsabile della macchina incriminata

NfSen tutorial

Tramite l'utilizzo di NfSen

vogliamo evidenziare

quanto sia semplice

ricavare l'ip interno al NAT della macchina incriminata

con quei pochi dati a disposizione

senza dover passare l'antivirus

o leggere i log

su tutti i client di quella rete

NfSen Architettura

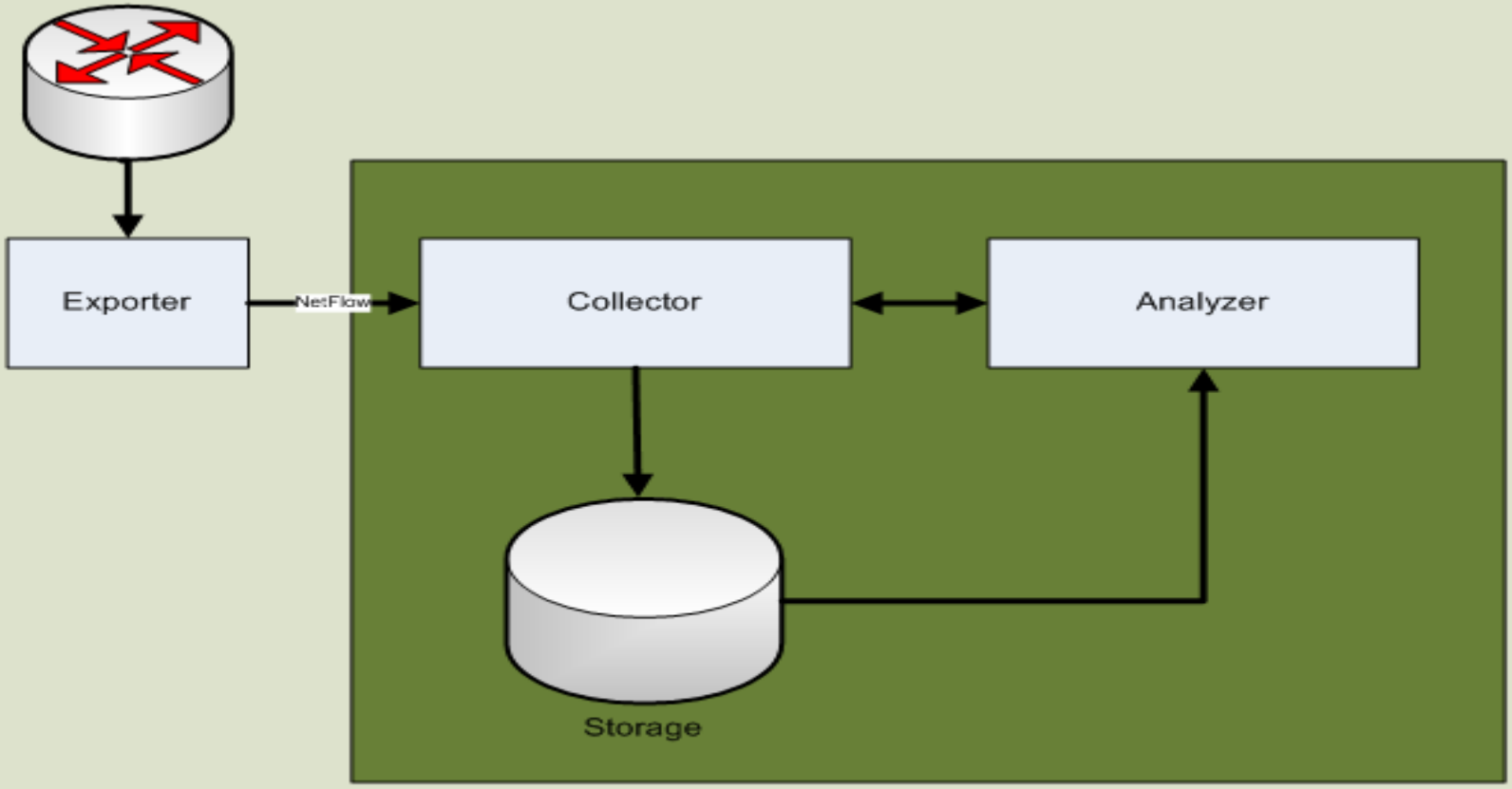
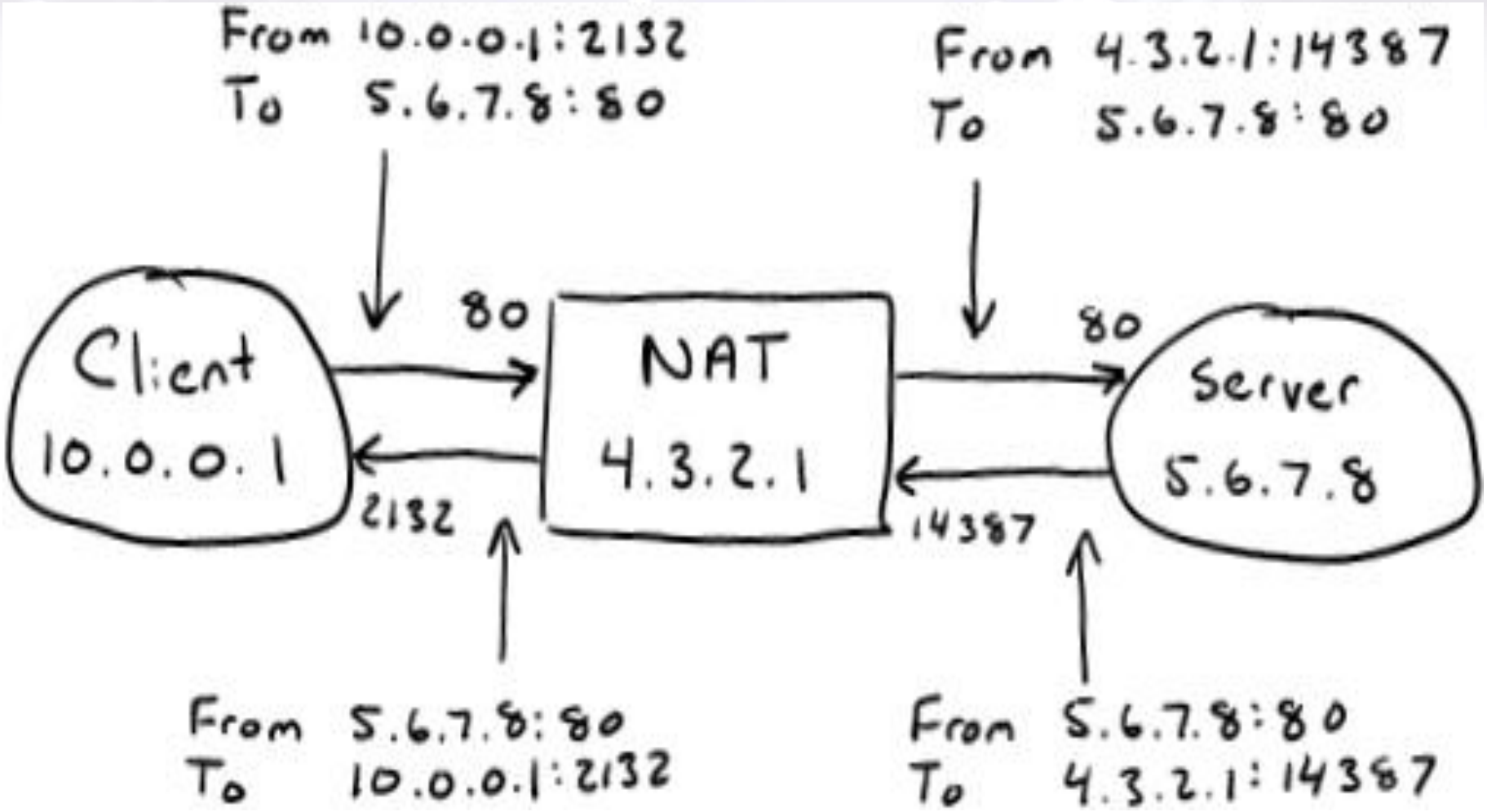
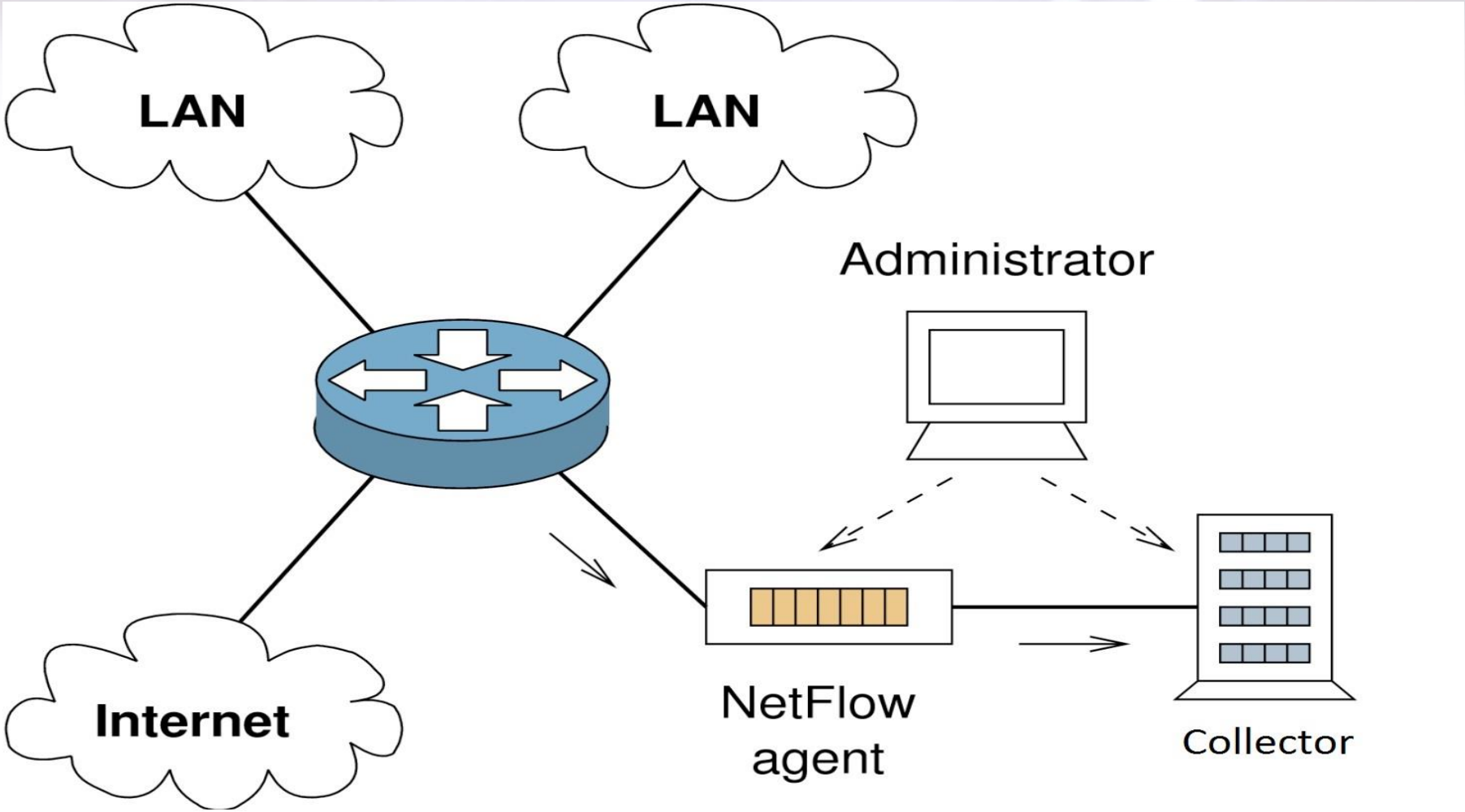


Figure 1: NetFlow Implementation Architecture

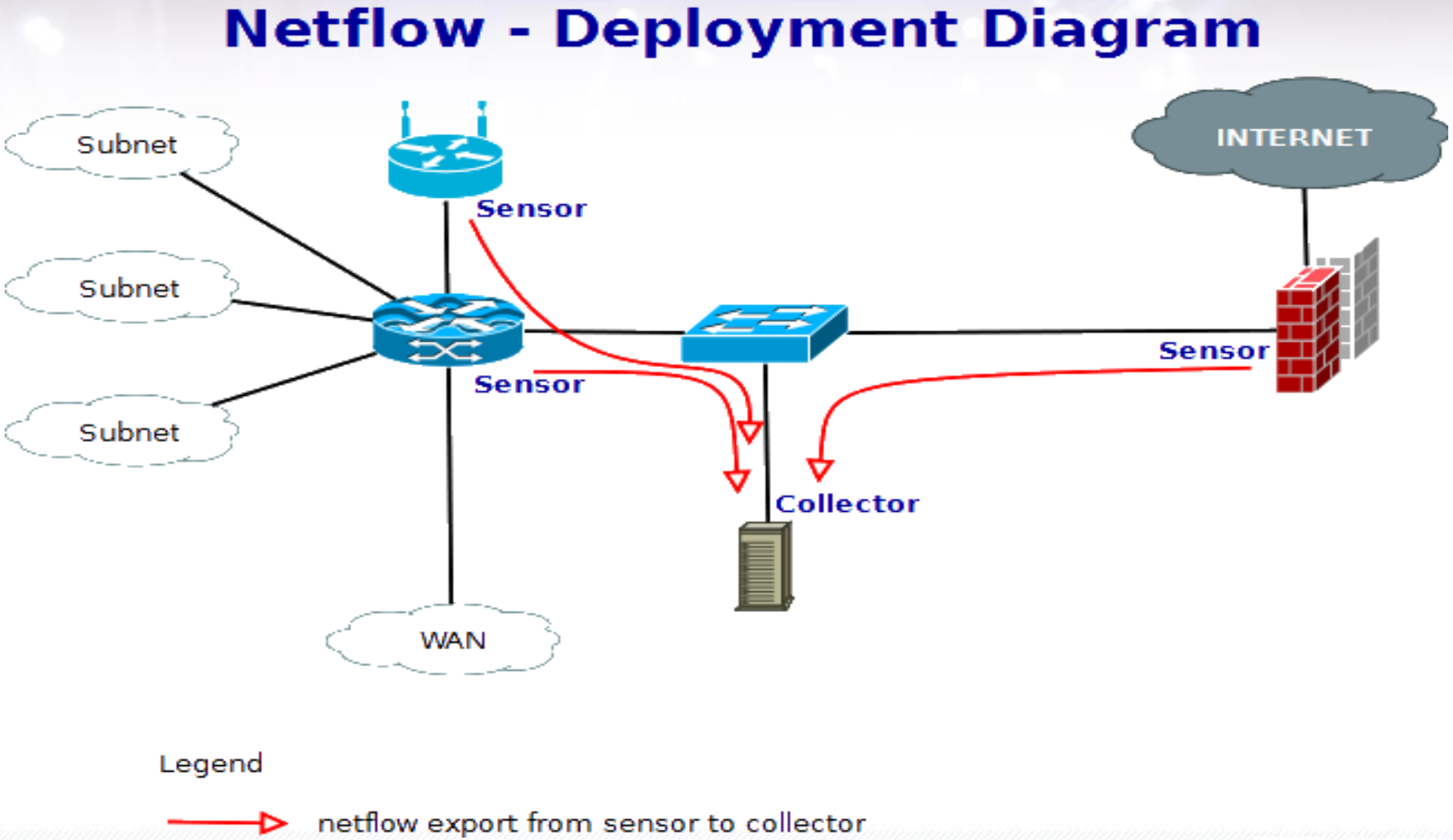
NAT Architettura



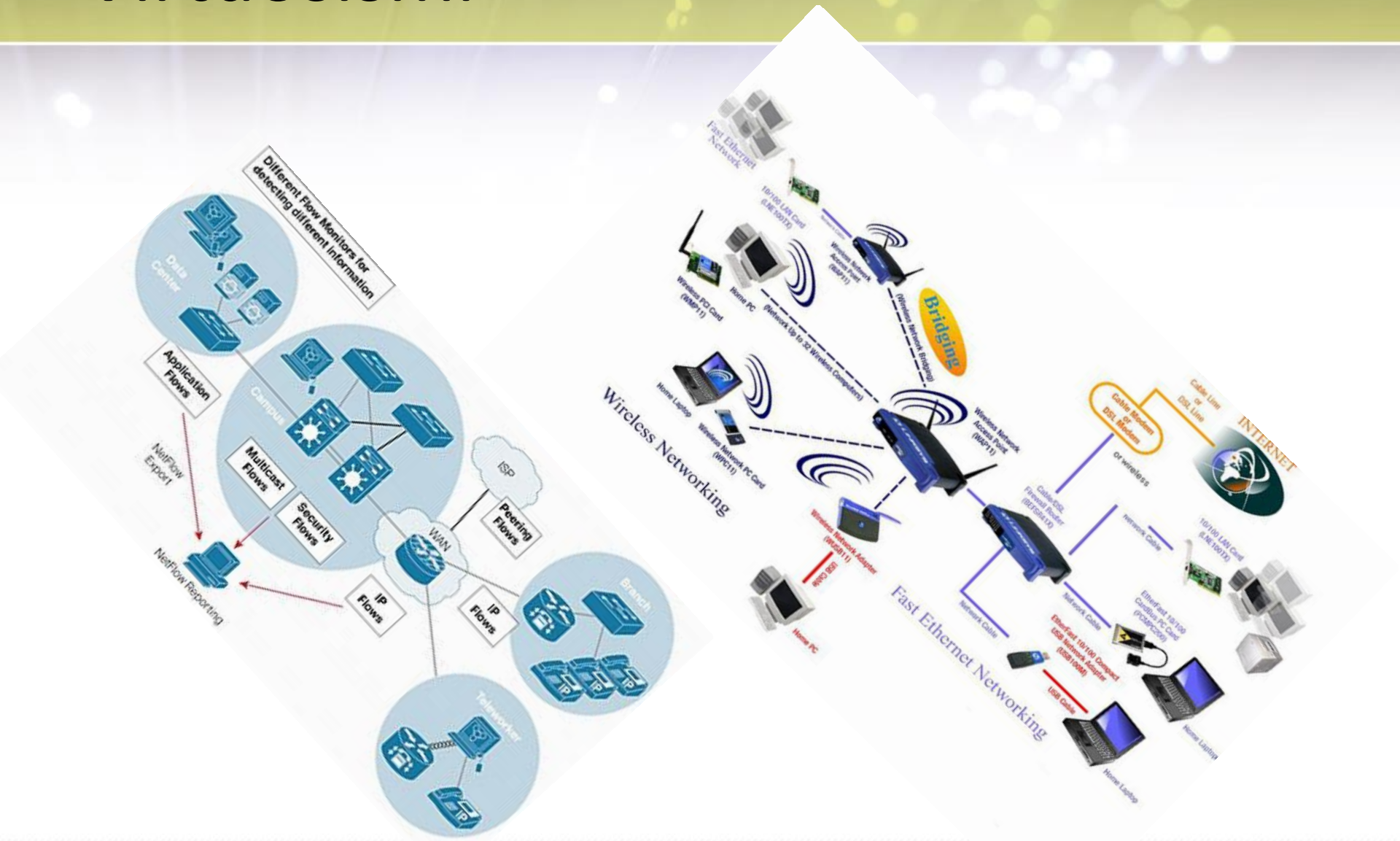
Architettura NfSen per NAT



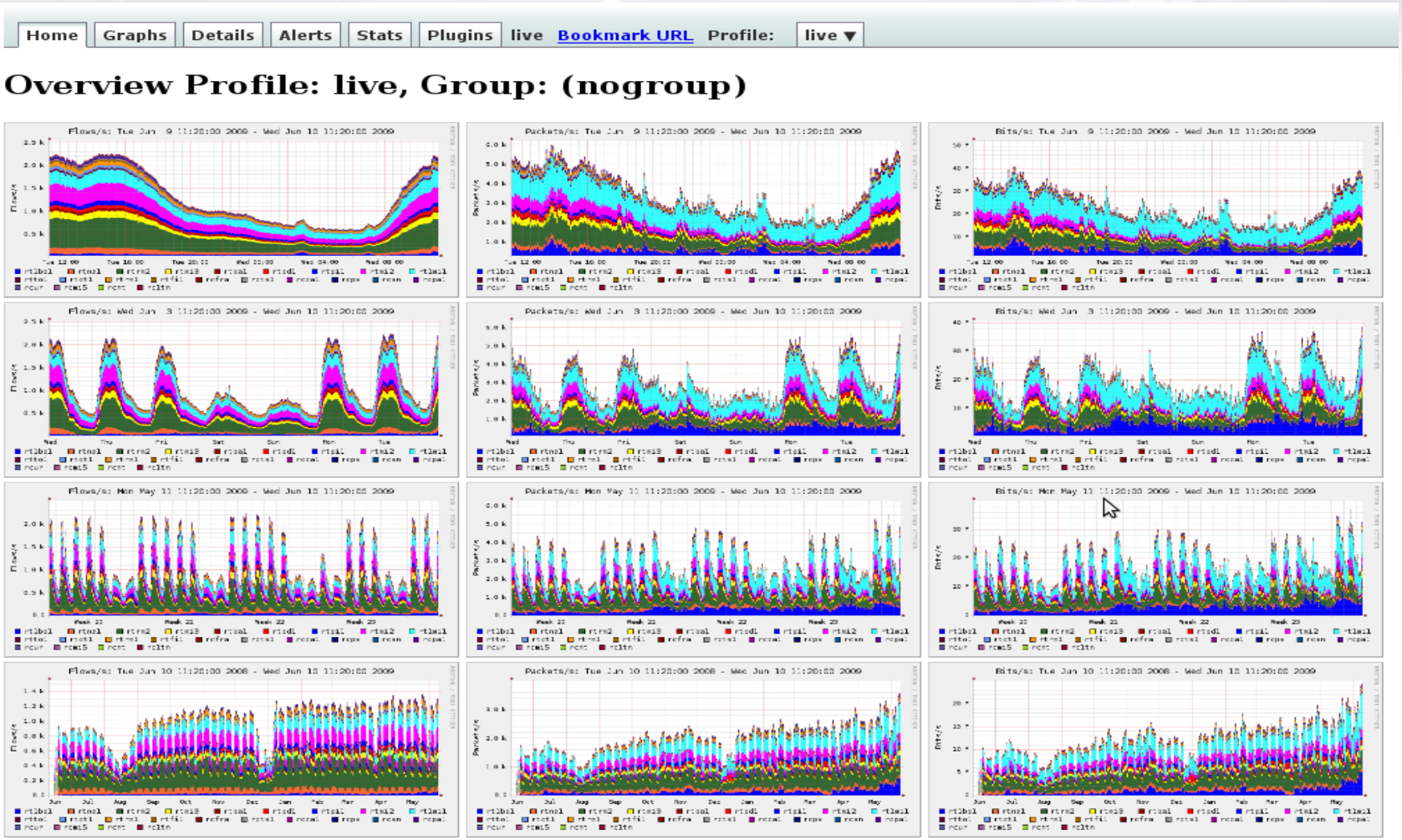
NfSen ambiente misto



Virtuosismi



Risultato


Home
Graphs
Details
Alerts
Stats
Plugins
live
Bookmark URL
Profile:
live
Overview Profile: live, Group: (nogroup)

Tool disponibili

Collector:

- flow-tools
- Stager
- Ntop
- Nerd
- nfdump/NfSen

Exporter:

- flowprobe
- NetFlow iptables module
- nProbe

Scelte operative

Collector: suite nfdump/nfsen

- Supporto NetFlow 9 (IPv6, MPLS)
- Tool da linea di comando per la collezione e l'analisi dei flussi (nfcapd, nfdump)
- Numerose utility per la gestione dei flussi (ri-esportazione dei flussi, cancellazione dei flussi più vecchi, conversione da altri formati, etc.)
- Possibilità di anonimizzare i flussi
- Sistema di plugin per l'estensione delle funzionalità
- Interfaccia grafica
- Software in continuo sviluppo (mailing list attiva!)
- Sviluppato da SWITCH.ch ; licenza BSD license

http://nfsen.sourceforge.net/

Scelte operative

Exporter di flussi dal NAT server: nProbe

- Affidabilita' altissima anche per carico pesante sulla rete
- Altissima stabilita'
- Altissime performance anche sotto stress
- sviluppato dal prof. Luca Deri, dell'Universita' di Pisa (ai tempi)
- OpenSource (per Universita' ed Enti di Ricerca)

http://www.ntop.org/nProbe.html

Requisiti minimi

CPU

- Minima: pentium 4 > 3Ghz
- Consigliata: bi o quadri multicore cpu > 2Ghz

RAM

- Minima: 2GB
- Consigliata: 4GB

Dischi di alta capacità e ad accesso veloce

- Da 40MB a 1.6G al giorno di dati per un router di trasporto

  Dipende dal numero di client dietro il NAT!

Architettura nel tutorial

nattina: macchina linux che fa da NAT ad una sottorete di due macchine: zm01 e zm02 che stanno dietro NAT

nattina:

eth0 → interfaccia verso l'esterno (10.0.2.15 DHCP di VirtualBox)
eth1 → interfaccia verso la rete interna (10.0.100.1)

zm01: linux 10.0.100.2 zm02: linux 10.0.100.3

nattina agisce come un router NAT (iptables MASQUERADE)

nattina esporta i pacchetti NetFlow delle sue due reti verso il collector (nProbe localhost:1000x)

nattina=il collector (conserva i file del traffico + interfaccia web NfSen)

Installazione NfSen

Nfdump su nattina:

Via distribuzione: es. apt-get install nfdump

Via sorgenti:

es. ./configure --enable-nfprofile && make && make install

Nfsen su nattina:

- Prerequisiti: PHP, Perl, RRDtools, Nfdump con «--enable-nfprofile»
- Installazione da sorgenti: copiare nfsen-dist.conf in nfsen.conf
- Modificare nfsen.conf definire gli exporter in %sources e i path
- Lanciare ./install.pl </path/nfsen.conf> **FINE!**

Configurazione NfSen 1/2

Nfsen.conf

$BASEDIR # directory base della suite
$BINDIR # directory dove di desiderano i binari
$HTMLDIR #root del webserver
$PROFILESTATDIR #dove devono essere salvati i dati
$back-end_PLUINGDIR #directory che ospita i plugin di back-end
$FRONTEND_PLUGINDIR #directory che ospita i front-end plugin
$SUBDIRLAYOUT #importante per motivi prestazionali

0 default
1 anno/mese/giorno
2 anno/mese/giorno/ora

@plugins #array per l'associazione tra il profilo e il plugin installato

Configurazione NfSen 2/2

Definizione delle fonti da cui mi arrivano i dati NetFlow da collezionare e analizzare (sempre dentro nfsen.conf):

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

Rilanciare: ./install.pl ./etc/nfsen.conf

nProbe

Installazione nProbe (solo su nattina!):

Scarico dei sorgenti da www.ntop.org

```
gzip -d nprobe-xxx.tgz
tar xvf nprobe-xxx.tar
./autogen.sh && make && make install
```

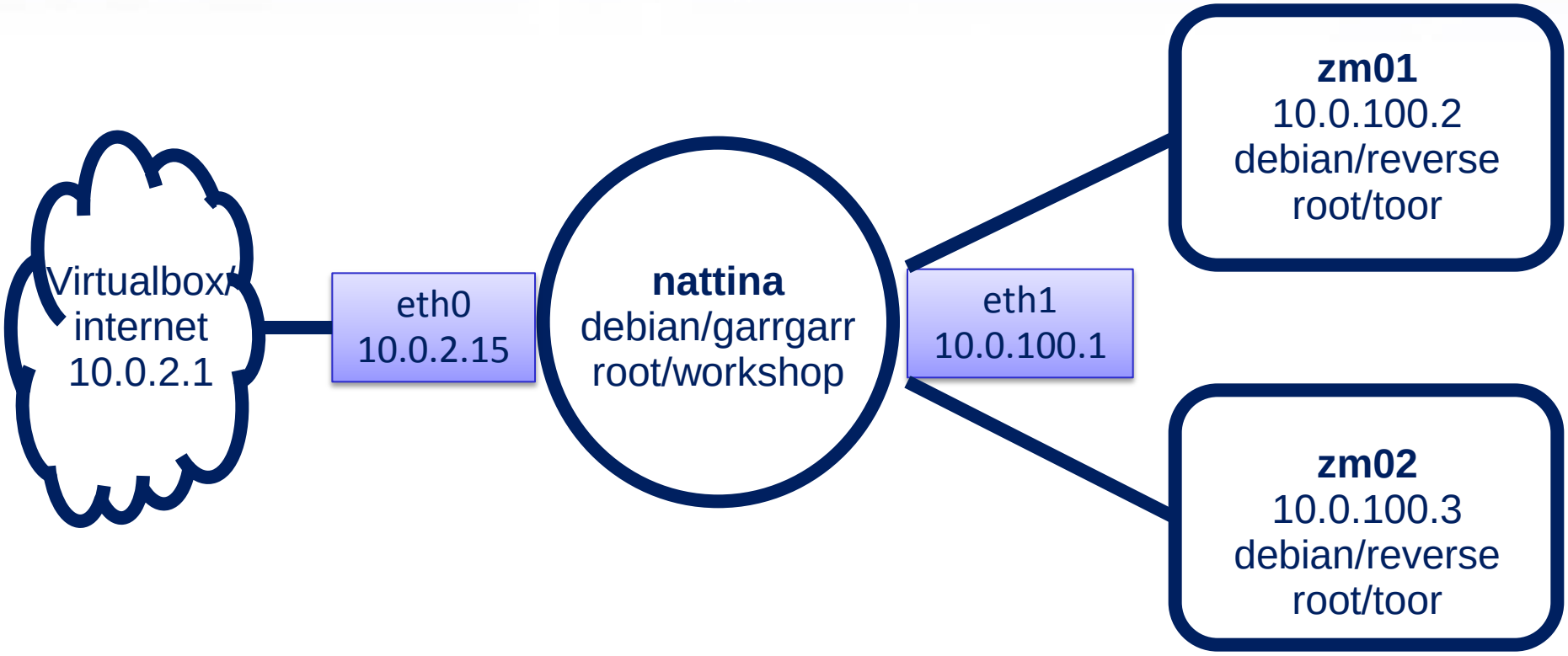
Comandi d'esportazione:

```
nprobe -G -i eth0 -n localhost:10000
nprobe -G -i eth1 -n localhost:10001
```

Vanno fatti partire al boot della macchina (es. rc.local)

Esercitazione

Scenario



Esercitazione

Il GARR-CERT vi segnala TRE incidenti sull' IP 10.0.2.15 (l'ip «pubblico» del NAT server):

Scanport
ssh probe
DoS

Le possibili vittime sono 192.84.145.55 o 192.84.145.67

L'esercizio consiste nel capire quale macchina dietro a NAT ha fatto cosa, in modo da curare e chiudere l'incidente

argus