NetFlow Überwachung mit nfdump/nfsen

Jens Link

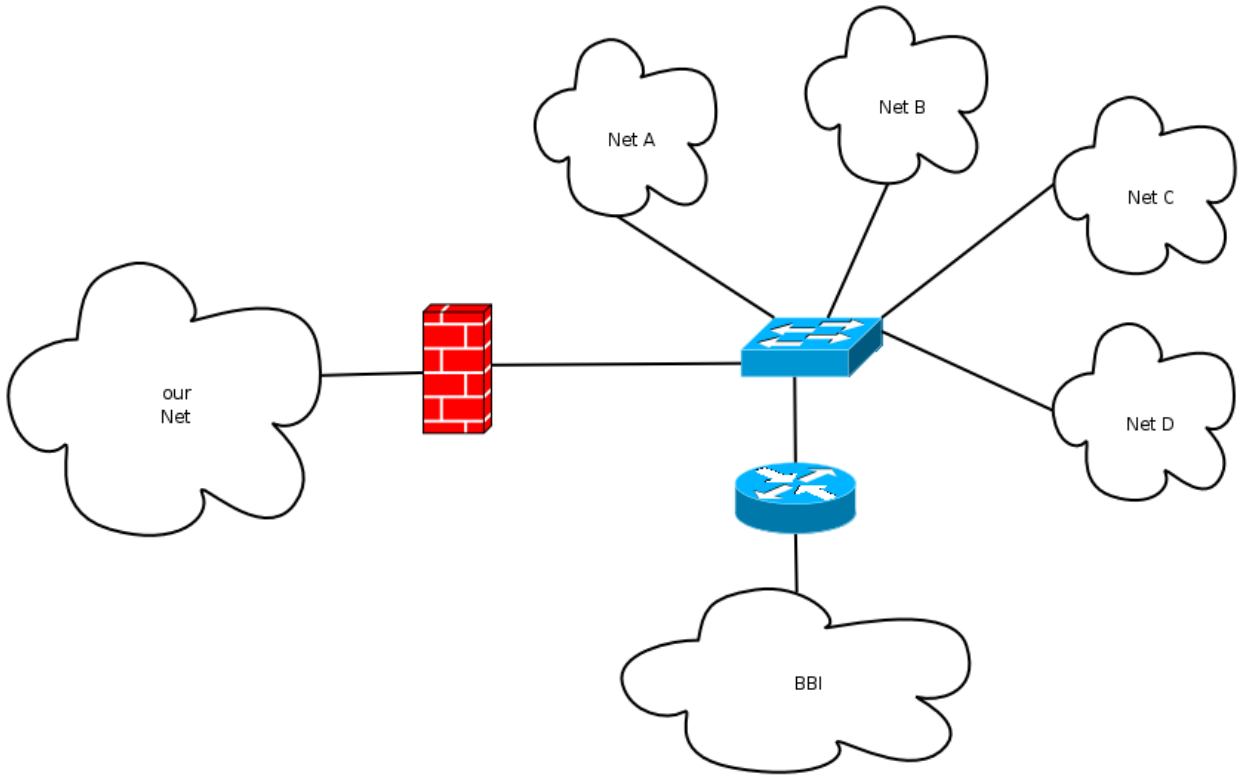
jenslink@quux.de

OSDC Nürnberg, März 2009

Übersicht

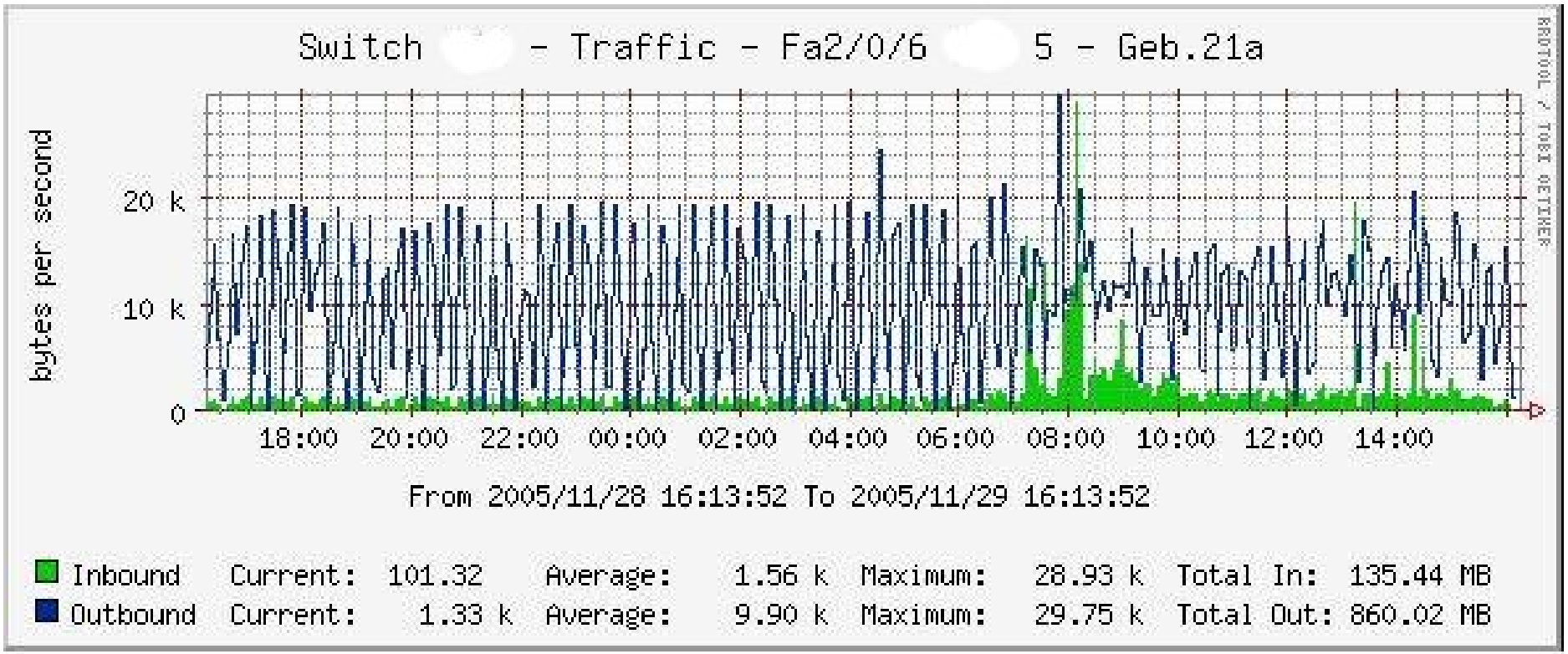
Wie alles begonnen hat (I)

- Netzwerkadmin in einem großen Campus Netz
- Teile des Netzes waren über das bestehende Telefonnetz realisiert (G.SHDSL-Modem)
- Viele verschieden Nutzer, einige davon machten ihre IT selbst und lehnten Hilfe an



Wie alles begonnen hat (II)

- Netzwerküberwachung mit NAGIOS und Cacti
- Bei einigen Graphen war der Traffic nicht zu erklären
- Min. ein Rechner im Netz hatte einen Blaster



Mögliche Lösungen

- tcpdump / etherealŴwireshark
  - Im Einzelfall durch nichts zu ersetzen
  - Analyse ist teilweise zu aufwendig, da zu viele Details
- IDS (snort)
  - Aufwendig in im Tuning
- NetFlow
  - Klang ersteinmal gut, weil es anscheinend direkt auf der von uns eingesetzten Hardware zu laufen schien

NetFlow (I)

- Ursprünglich von Cisco als Switchingverfahren entwickelt
- Verschiedenen Versionen und Varianten (z.B. sFlow)
- NetFlow Version 9 ist in RFC 3995 spezifiziert
- Datenübertragung per UDP
- Viele Werkzeuge zur Analyse (vorallem kommerziell)
- Möglichkeit des Sampled Netflow (z.B. nur jeden 1024ten Flow)

NetFlow (II)

Grobe Funktionsweise:

- Ein Sensor (z.B. Router) sammelt Daten und sendet sie weiter
- Ein Collector nimmt die Daten an und speichert sie in einer Datenbank
- Über andere Software können diese Daten dann ausgewertet werden

Was ist ein Flow?

Datenstrom zwischen zwei Devices.

- Zeitstempel
- Byte-Zähler
- Quell- und Ziel IP
- Quell- und Ziel Port
- Interfaces
- TOS
- ggf. AS-Nummern
- TCP-Flags
- Protokoll (UDP, TCP, ICMP, ...)

NetFlow Daten erfassen - Linux

Verschieden Tools, u.A. fprobe-ng

```
cat /etc/default/fprobe
#fprobe default configuration file

INTERFACE="eth0"
FLOW_COLLECTOR="localhost:555"

#fprobe can't distinguish IP packet from other (e.g. A
OTHER_ARGS="-fip"
```

NetFlow Daten erfassen - Cisco (I)

```
....
ip flow-export version 9
ip flow-export destination 192.168.73.9 9995
ip flow-top-talkers
 top 5
 sort-by bytes
...
```

NetFlow Daten erfassen - Cisco (II)

Schnelle Auswertung ohne zusätzliche Tools:

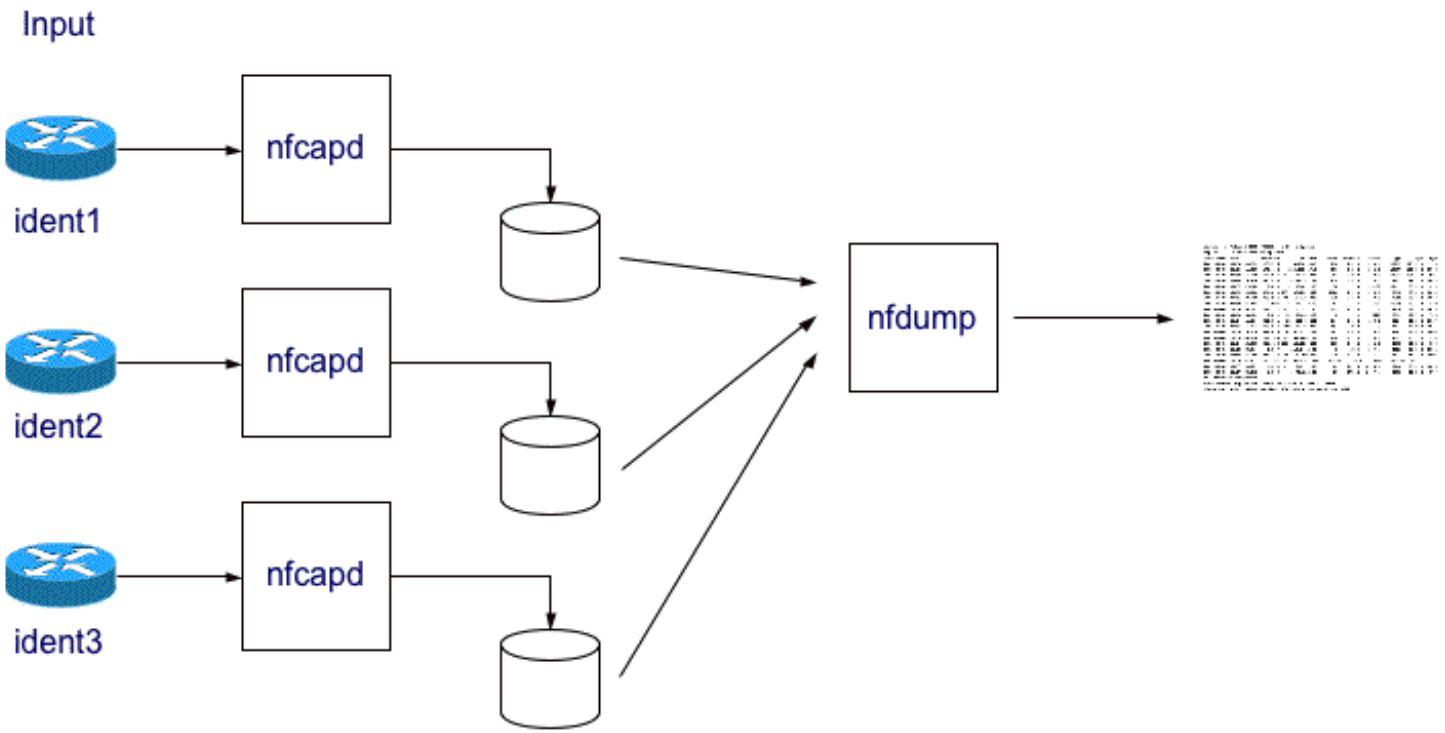
```
jl-home#sh ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress
Vl1           88.74.12.234    Di1*          82.113.121.164
Di1           82.113.121.164  Vl1           88.74.12.234
Vl1           88.74.12.234    Di1*          212.227.83.207
Vl1           88.74.12.234    Di1*          207.46.124.199
Di1           207.46.124.199  Vl1           88.74.12.234
5 of 5 top talkers shown. 6 flows processed.
```

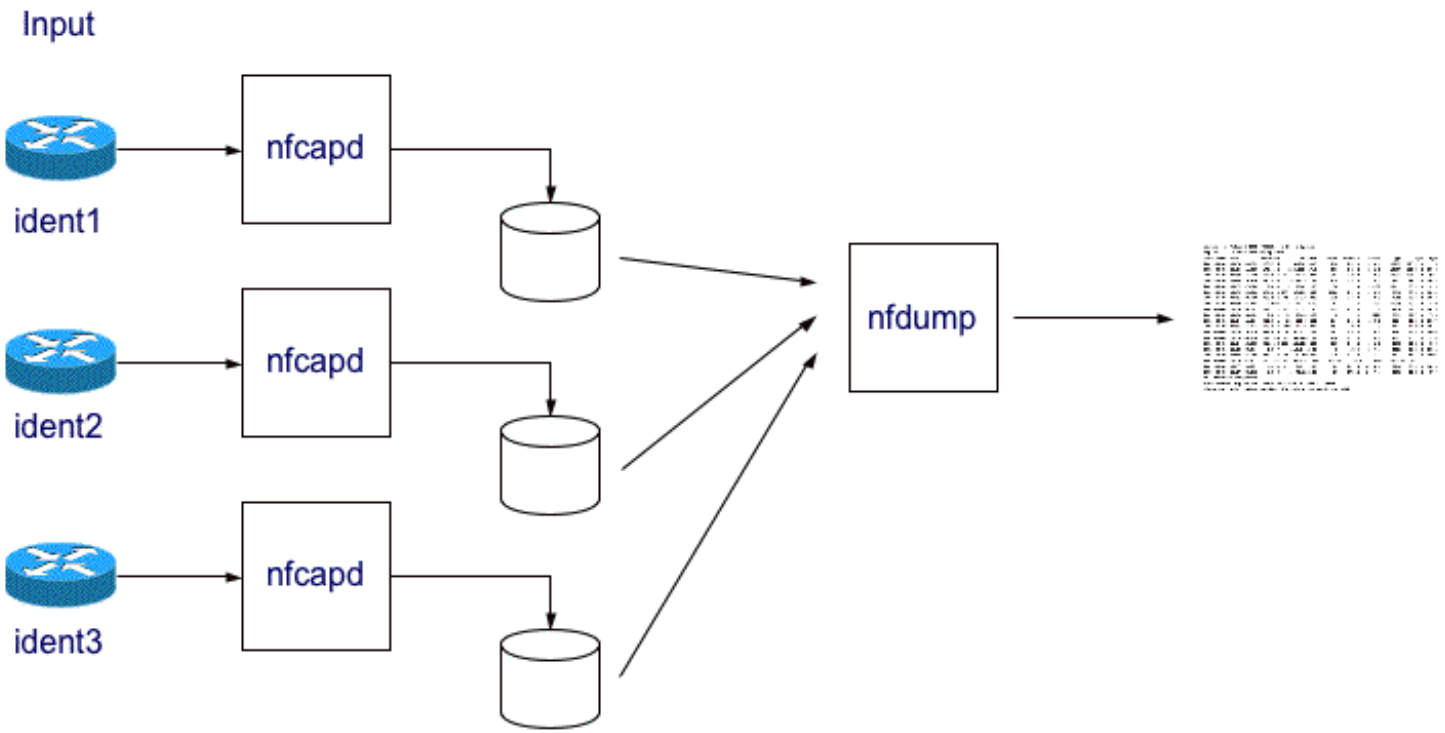
nfsen/nfdump(I)

- **nfdump** - Sammlung von Programmen um Netflow Daten zu sammeln und zu analysieren
  - **nfcapd** - Netflow Capture Daemon.
  - **nfdump** - Analyse der Daten
  - **nfprofile** - Spllitten der Daten anhand von Profielen
  - **nfreplay** - Senden der Daten an einen anderen Host
  - **nfclean.pl** - Löschen alter Daten
  - **ft2nfdump** - Konvertieren von flow-tools Daten
- **nfsen** - WEB GUI als komfortables Frontend zu nfdump

nfsen/nfdump (II)



nfsen/nfdump (II)



blaster

```
Flows analysed: 1696 matched: 1000, Bytes read: 82944
Date flow start    Len Proto  Src IP Addr:Port    Dst
IP Addr:Port Packets Bytes
Sep 01 2005 14:45:14    0 TCP      192.168.17.9:4593
      152.9.118.119:135       2   96 B 1
Sep 01 2005 14:45:14    0 TCP      192.168.17.9:4590
      152.9.118.116:135       2   96 B 1
Sep 01 2005 14:45:14    0 TCP      192.168.17.9:4594
      152.9.118.120:135       2   96 B 1
Sep 01 2005 14:45:14    0 TCP      192.168.17.9:4595
      152.9.118.121:135       2   96 B 1
```

Kontakt

eMail	jenslink@quux.de
Jabber	jenslink@guug.de
PGP Fingerprint	D9FF E215 6686 6194 FFC8
	A135 19CF A676 DB85 EF91