

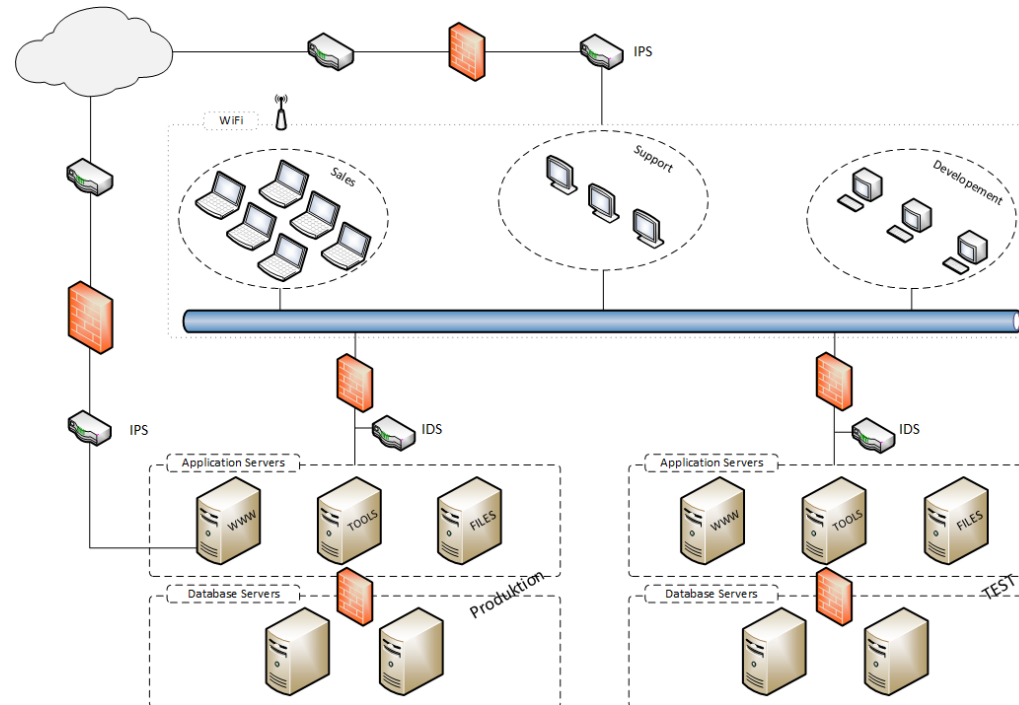
KRESTEN JACOBSEN

NETFLOW

Hvad: Opsamling af metadata om netværksstrømme

Hvorfor: Fordi full packet capture er for tungt / fylder for meget og fordi det ofte vil være metadata, der er interessante after-the-fact.

BAGGRUND: NETWORK ARCHITECTURE



- Opdeling af servere vertikalt i hhv. TEST og PROD.
- Opdeling af servere horisontalt i hhv. brugerrettede og DB.
- Segmentering af klient-netværk, således at adgange til servere kan gives per-netværkssegment.
- Udgang til internettet NAT.
- Webserver i prod tilgås via anden ip-adresse.
- IDS'er (Intrusion Detection System) mellem klient og server
- IPS'er (Intrusion Protection System) mellem internet og internt net (x2)
- Evt. opsætte NetFlow collectors på de to ydere routere (men det kunne egentligt også være interessant mellem klient / server og "lagene" i serverrummet).

Kombination af full packet captures med netflow er at foretrække.

Eks: at rulle full packet capture efter en uge, men at beholde netflow data et helt år.

Eks: sæt netflow sensorer op på alle routere, men kun full packet capture på kritiske segmenter.

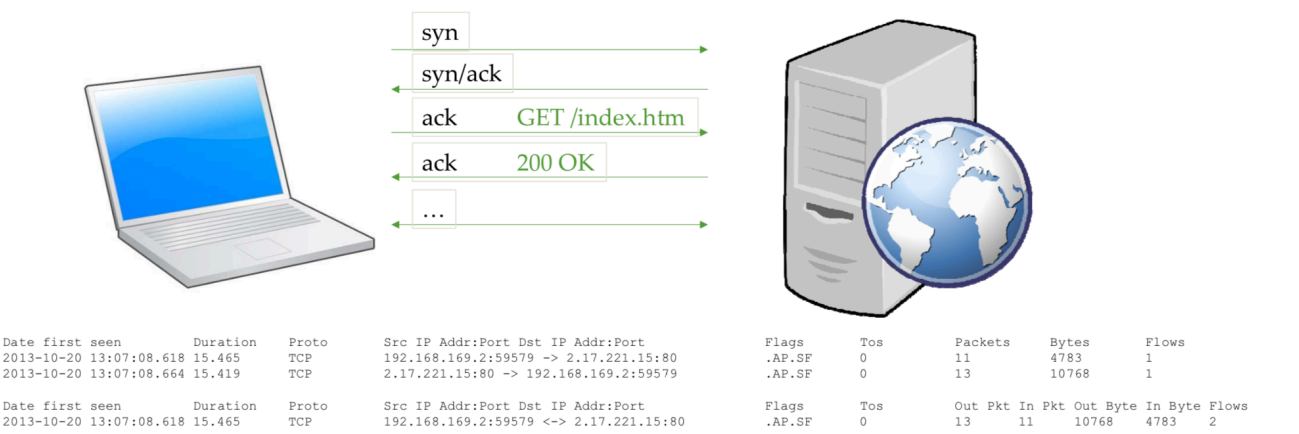
TEORI: NETFLOW

- ▶ Unidirectional
- ▶ To flows
- ▶ Aggregeret metadata

| Fordele | Ulemper |
|--|---------------------------------------|
| Hurtigt! | Fanger ikke indholdet af datastrømmen |
| Optager ca. 0.01% af 'full packet capture' | |
| Ingen forskel på krypteret og ukrypteret trafik | |
| Effektivt til at opdage afvigelser i trafikmønstre | |

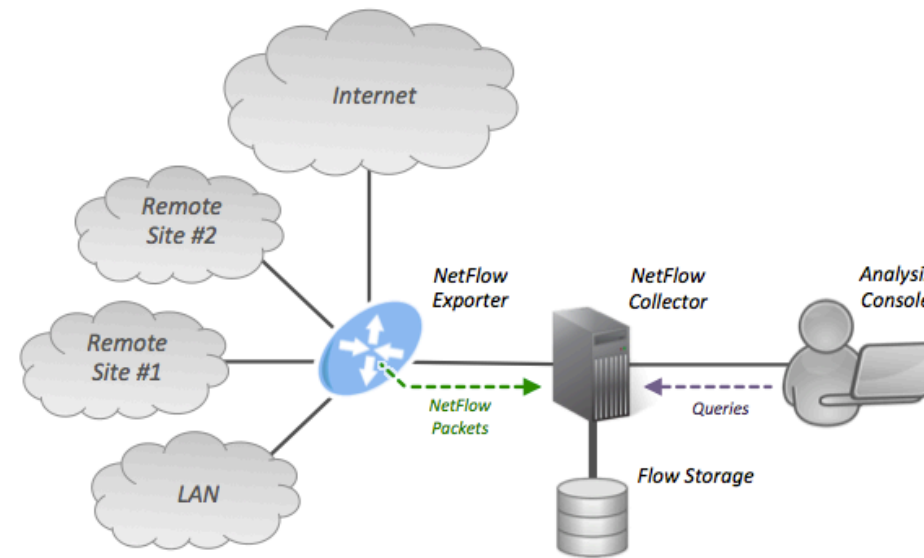
Tre begreber skal forklares...

TEORI: NETFLOW



Kombination af full packet captures med netflow er at foretrække.
Eks: at rulle full packet capture efter en uge, men at beholde netflow data et helt år.
Eks: sæt netflow sensorer op på alle routere, men kun full packet capture på kritiske segmenter.

TEORI: NETFLOW



Flow exporter: aggregates packets into flows and exports flow records towards one or more flow collectors.

Flow collector: responsible for reception, storage and pre-processing of flow data received from a flow exporter.

Analysis application: analyzes received flow data in the context of intrusion detection or traffic profiling, for example.

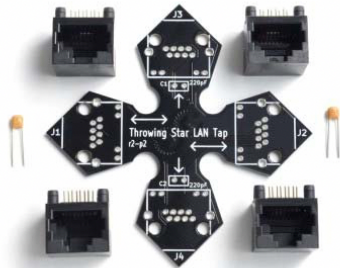
DEMO: NETFLOW

```
Applications ▾ Places ▾ Terminal ▾ Tue 08:00 1
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# fprobe -i eth0 localhost:555
root@kali:~# nfcapd -D -p 555 -S 1 -z -I Linux-Host-1-eth0 -l /root/netflow/
root@kali:~# nfdump -R /root/netflow/
Date first seen      Event  XEvent Proto      Src IP Addr:Port      Dst IP Addr
:Port      X-Src IP Addr:Port      X-Dst IP Addr:Port  In Byte Out Byte
2017-11-09 10:22:59.956 INVALID Ignore UDP      192.168.232.129:54018 -> 176.20.234.10
2:123      0.0.0.0:0 -> 0.0.0.0:0 76 0
2017-11-09 10:22:59.963 INVALID Ignore UDP      176.20.234.102:123 -> 192.168.232.12
9:54018      0.0.0.0:0 -> 0.0.0.0:0 76 0
2017-11-09 10:23:16.457 INVALID Ignore UDP      192.168.232.1:50789 -> 224.0.0.25
2:5355      0.0.0.0:0 -> 0.0.0.0:0 110 0
2017-11-09 10:23:20.524 INVALID Ignore UDP      192.168.232.1:137 -> 192.168.232.25
5:137      0.0.0.0:0 -> 0.0.0.0:0 234 0
2017-11-09 10:23:35.798 INVALID Ignore UDP      176.20.234.102:123 -> 192.168.232.12
9:35758      0.0.0.0:0 -> 0.0.0.0:0 76 0
2017-11-09 10:23:35.791 INVALID Ignore UDP      192.168.232.129:35758 -> 176.20.234.10
2:123      0.0.0.0:0 -> 0.0.0.0:0 76 0
2017-11-09 10:23:46.264 INVALID Ignore UDP      192.168.232.2:53 -> 192.168.232.12
9:46952      0.0.0.0:0 -> 0.0.0.0:0 721 0
2017-11-09 10:23:49.817 INVALID Ignore UDP      192.168.232.129:42638 -> 192.168.232.
2:53      0.0.0.0:0 -> 0.0.0.0:0 102 0
2017-11-09 10:23:50.394 INVALID Ignore UDP      192.168.232.129:52119 -> 192.168.232.
2:53      0.0.0.0:0 -> 0.0.0.0:0 162 0
2017-11-09 10:23:43.692 INVALID Ignore UDP      192.168.232.129:60942 -> 192.168.232.
2:53      0.0.0.0:0 -> 0.0.0.0:0 140 0
2017-11-09 10:23:45.315 INVALID Ignore UDP      192.168.232.2:53 -> 192.168.232.12
9:42828      0.0.0.0:0 -> 0.0.0.0:0 355 0
2017-11-09 10:23:47.112 INVALID Ignore UDP      192.168.232.129:42221 -> 192.168.232.
2:53      0.0.0.0:0 -> 0.0.0.0:0 134 0
```

- fprobe
This is the exporter that generates the netflow updates
- nfcapd
This is the collector that, accepts the updates from the exporter
- nfdump
This is the analysis tool, that enables up to query the netflow data

RELATERET EMNE: IDS / IPS – DATA COLLECTION + SOFTWARE STACK

| | Hardware tap | Switch port mirroring |
|-----|----------------------|-------------------------------------|
| Pro | Kan skaleres nemt | Kræver (sikkert) ikke ekstra udstyr |
| Con | Kan være rigtig dyrt | Hastighed på porten begrænser |



+



"Ninja stjernen" er et eksempel på en billig hardware network tap, men den kører altså også maksimalt 100MBIT.

Snort bruges af en IDS / IPS til at "sniffe" trafik.

squid er et "Management interface", som kan rapportere på snort-regler.