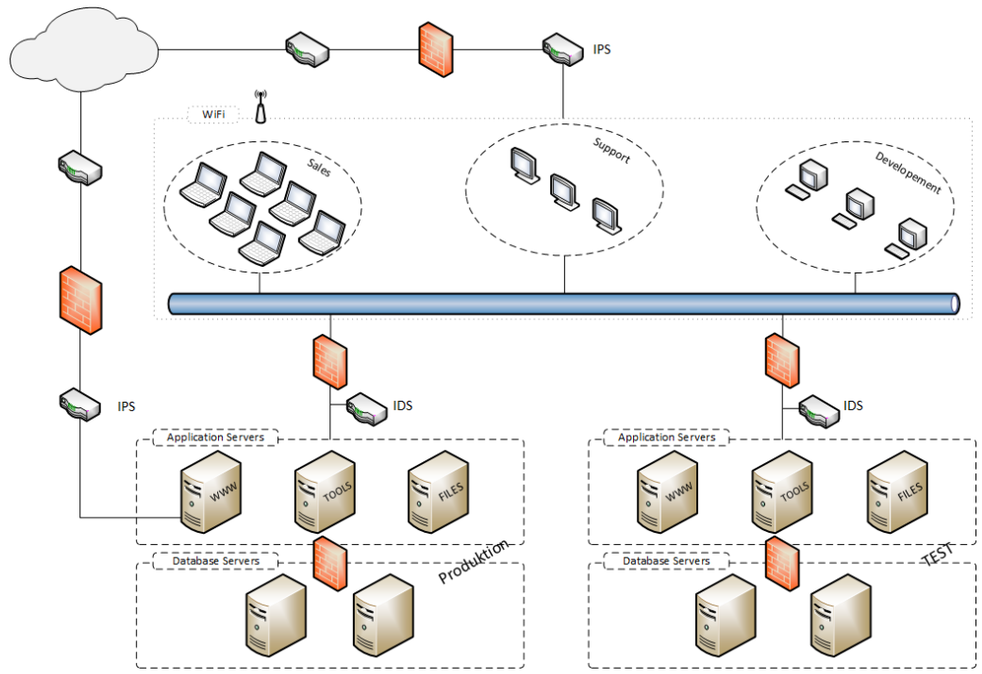
KRESTEN JACOBSEN

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.

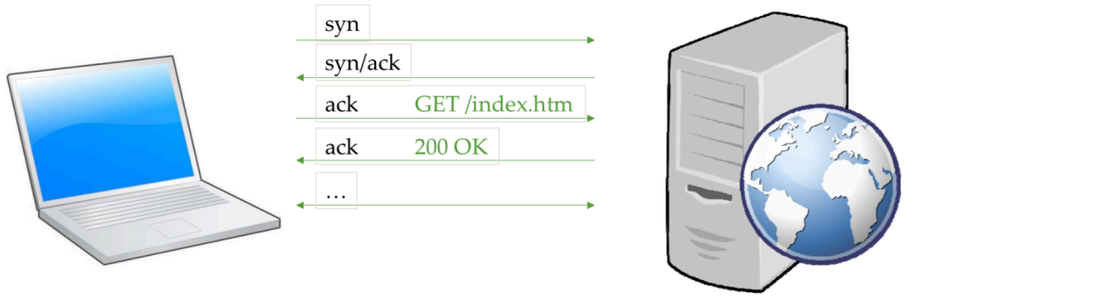
TEORI: NETFLOW

- 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



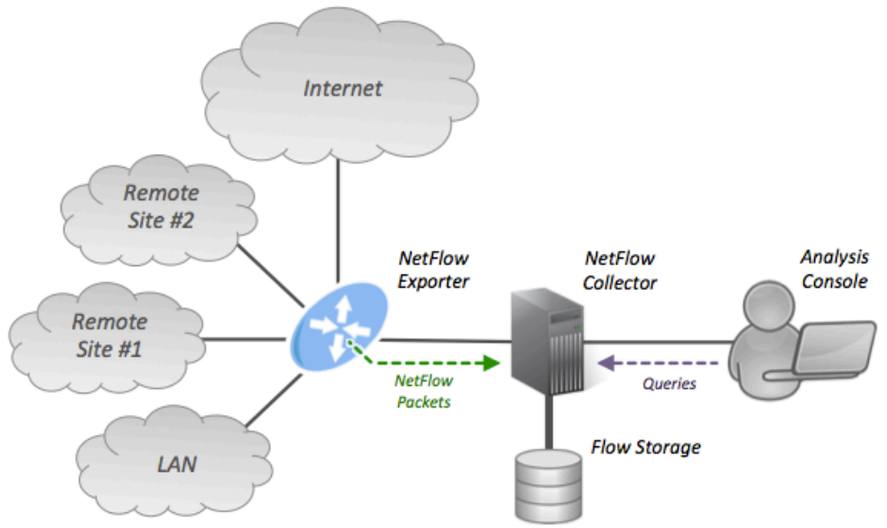

```
Date first seen          Duration    Proto       Src IP Addr:Port Dst IP Addr:Port              Flags       Tos         Packets     Bytes       Flows
2013-10-20 13:07:08.618 15.465      TCP         192.168.169.2:59579 -> 2.17.221.15:80          .AP.SF      0           11          4783        1
2013-10-20 13:07:08.664 15.419      TCP         2.17.221.15:80 -> 192.168.169.2:59579          .AP.SF      0           13          10768       1

Date first seen          Duration    Proto       Src IP Addr:Port Dst IP Addr:Port              Flags       Tos         Out Pkt In Pkt Out Byte In Byte Flows
2013-10-20 13:07:08.618 15.465      TCP         192.168.169.2:59579 <-> 2.17.221.15:80         .AP.SF      0           13      11     10768    4783    2
```

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

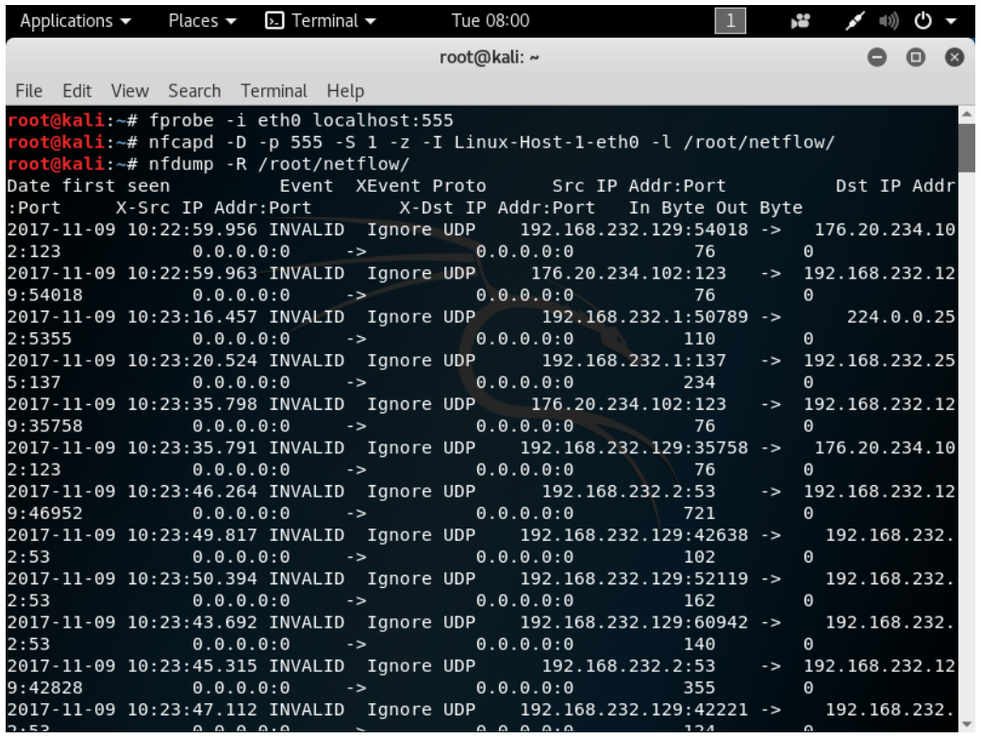


Flow exporter: aggregates packets into flows and exports flow records towards one or more flow collectors.

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



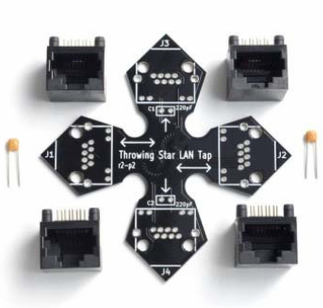
fprobe
: This is the exporter that generates the netflow updates

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



SNORT® + sguil

"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.

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