KRESTEN JACOBSEN

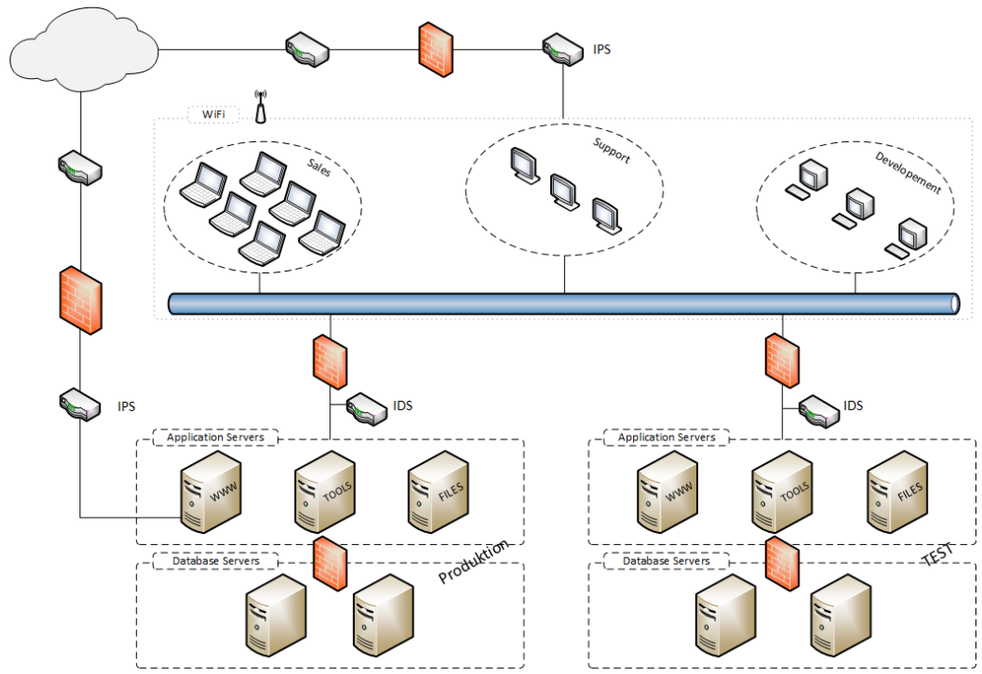
NETWORK ARCHITECTURE

Hvad: Intrusion Detection System & Intrusion Protection System

Hvorfor:*IDS* - Opdage angreb (alarmer) for efterfølgende at kunne rette services / firewalls til og evt. genoprette "normal drift".

IPS - Opdage og blokere angreb direkte i netværket.

OVERBLIK: 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).

ARKITEKTUR: NETFLOW

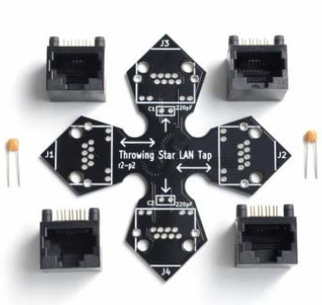

```
Date first seen          Duration    Proto       Src IP Addr:Port Dst IP Addr:Port              Flags       Tos         Packets     Bytes       Flows
2013-10-20 13:07:08.618 15.465      TCP         192.168.169.2:59579 -> 2.17.221.15:80          .AP.SF      0           11          4783        1
2013-10-20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

- Unidirectional
- To flows
- Aggregeret metadata

[burde have screenshot / demo af netflow capture]

ARKITEKTUR: 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.

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