

Verktyg

Detta dokument: <https://goo.gl/oWxj6x>

Slänga ut

- observium
- nagios
- librenms
- eget IPAM-system (örebro?)
- NCS/NSO
- cisco prime?
- alla verktyg som genererar alerts
- argus
- befintligt system för acl-hantering
- Microsoft SCOM

Behålla

- nagios
- KTH gillar sitt IPAM-system
- rancid
- fortinet-brandväggar
- alien vault (1)
- graylog
- nån "lösenordsportal" (missade namnet)

Saknar

- verktyg för ACL:er
 - <https://opensource.google.com/projects/capirca>
- automatisk uppgradering av switchar - spec:a bara att man vill köra "stable-track"
- Backup-verktyg för switch/router-config
- 100G-kapabel IDS/IPS/flowanalys +1
- integration mellan verktyg
- aggregering för flera larmsystem

ACL-hantering

- förtätning av kontor/lokala lab osv ger behov av lokala switchar
- svårt att genomföra strikt policy
- hur möter man behoven?
- många kör mac-authn
- autentisering på device, inte på användare gäst/icke-gäst (känd/okänd dator)
- för vissa är det bara burkarn inköpta och drivna av IT-avdelningens som kan bli "kända"
- acl:er på serversidan, print, iot (?)
- behöver diagnosverktyg för acl:er
- tidsbegränsad rensning av acl:er - ägare+tidsstämpel

Brandvägsregler

- Tidsbaserade regler med ägare+tidsstämpel (CMDB typ itop?)

Dokumentation (fysiskt och logiskt)

- CSV-format som underhålls veckovis (chalmers?)
- visa NI
- dokumentera i switcharna

IPAM

- IPAM med nätverkshistorik, kontrollerar om IP-address/arp varit sed senast
- DHCP-funktioner

Visning av Sunet/Nordunet, HV system.

HV

VLAN på alla switchar,

Program distribution och installation

Saknar historik av var den switch har varit

Umu.se

Utgående/Ingående ACL vissas mot klientern, med filter som visar vad acl:n matchar.

Befintlig utrustning

10mbps halvduplex

Finns behov, bla tryckpress med XP.

Övervakning

Klassificering, Prioritering av övervakning, switchar 247, dagtid.

Mängd larm, många (valbart) låg prio ger prioritets ökning.

Access-switch

Finns den där

Redundans?

Environment

Power supply

Portar

Errors

Poe last?

Spårning

Mac-address per port

247 övervakning

1 miljonairs 3d skrivare

Passage System

Vad ingår i CNAAS

[blocked URL](#)

SOC

Korrigeringsverktyg, inventera sina system vad man har och vem som äger. Nät och servrar.