



SEC/SKA – Skydda ditt nät och dina kunder

Integritet, Spårbarhet och Tillgänglighet

Workshop

Vem är jag?



Marcus Friman, Netrounds

15 års erfarenhet:

- Säkerhetstester i bredbandsnät – partner till SSNf sedan 2009, testat ett femtontal nät genom åren
- Test av företagsnät, operatörstjänster och triple-play-nät
- Brinner för att förbättra nät drift och kundupplevelse



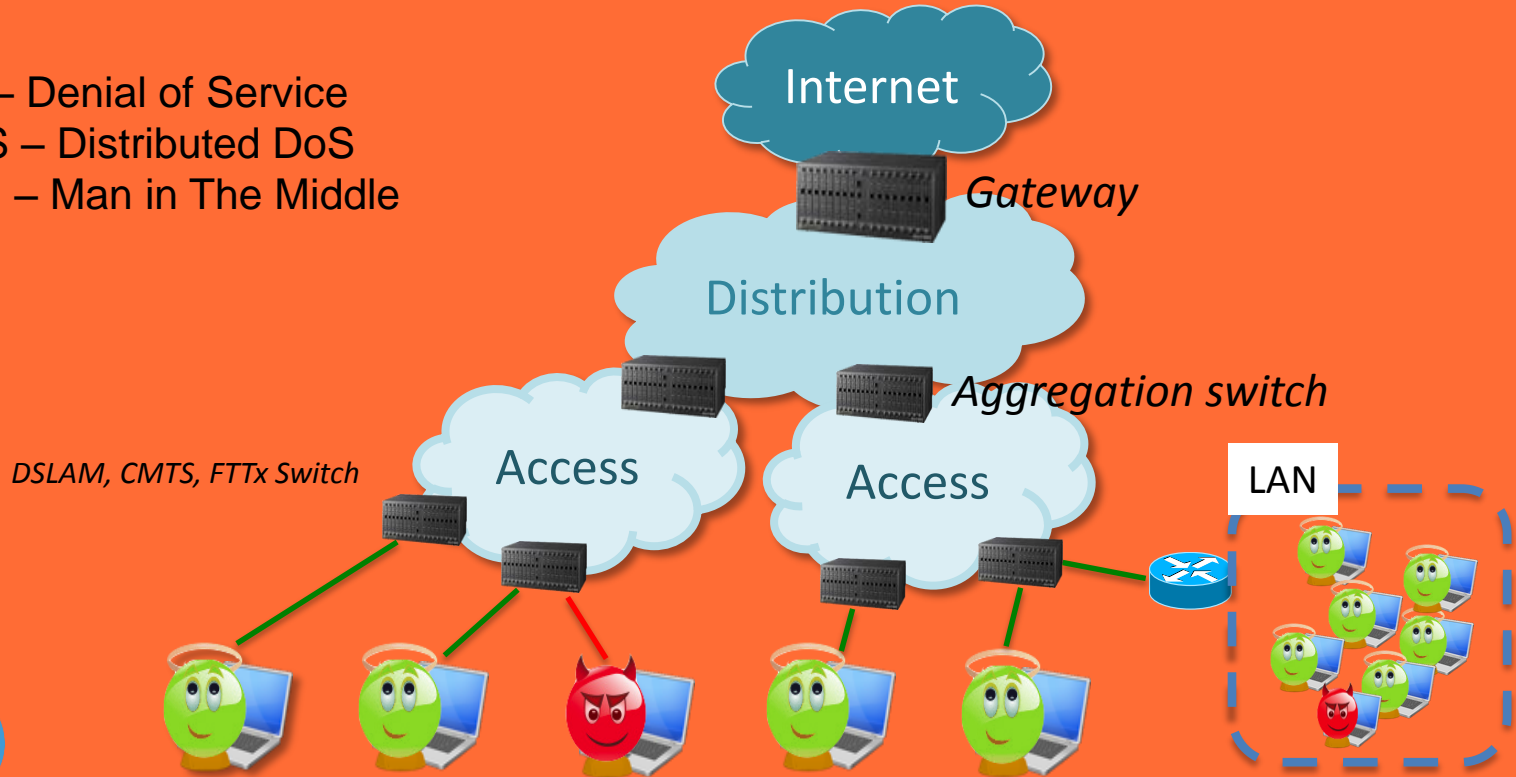
Format & agenda

- Vad är SEC/SKA?
- Exempel på hot och dess påverkan
- Diskussion: Varför bry sig?
- Diskussion: SEC/SKA-specifikation – nytta?
- saknas något?
- Nyheter
- Summering



Vad är SEC?

DoS – Denial of Service
DDoS – Distributed DoS
MiTM – Man in The Middle



Hot och påverkan

1. Integritet

- Skydda kundernas integritet
- Förhindra Man-in-the-Middle (MitM) attacker/avlyssning
- Säkerställ isolation mellan kunder

2. Spårbarhet

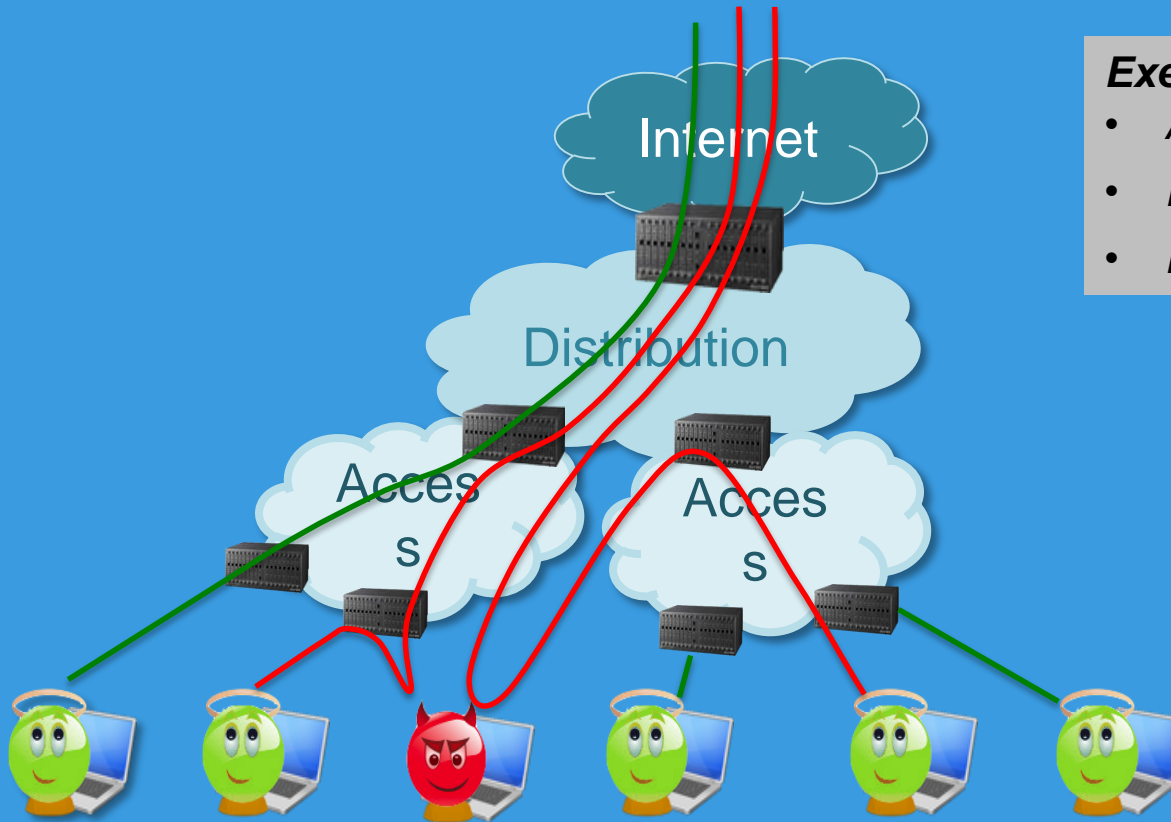
- Säkra möjligheten att spåra vid exvis abuse
- Lagkrav? (datalagringsdirektivet)

3. Robusthet

- Förhindra DoS-attacker
- Reducera “konstiga och svårhittade problem”



1. Integritet (MitM attack)



Exempel på hot:

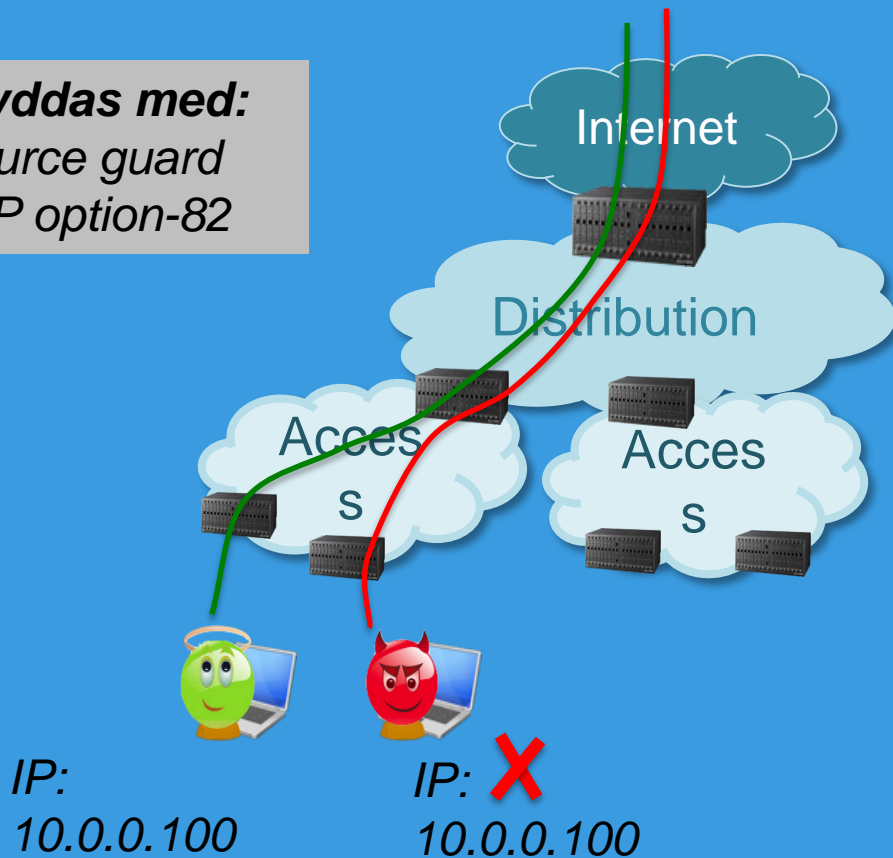
- *ARP Poisoning*
- *ICMP Redirect*
- *Rogue DHCP*



2. Spårbarhet

Kan skyddas med:

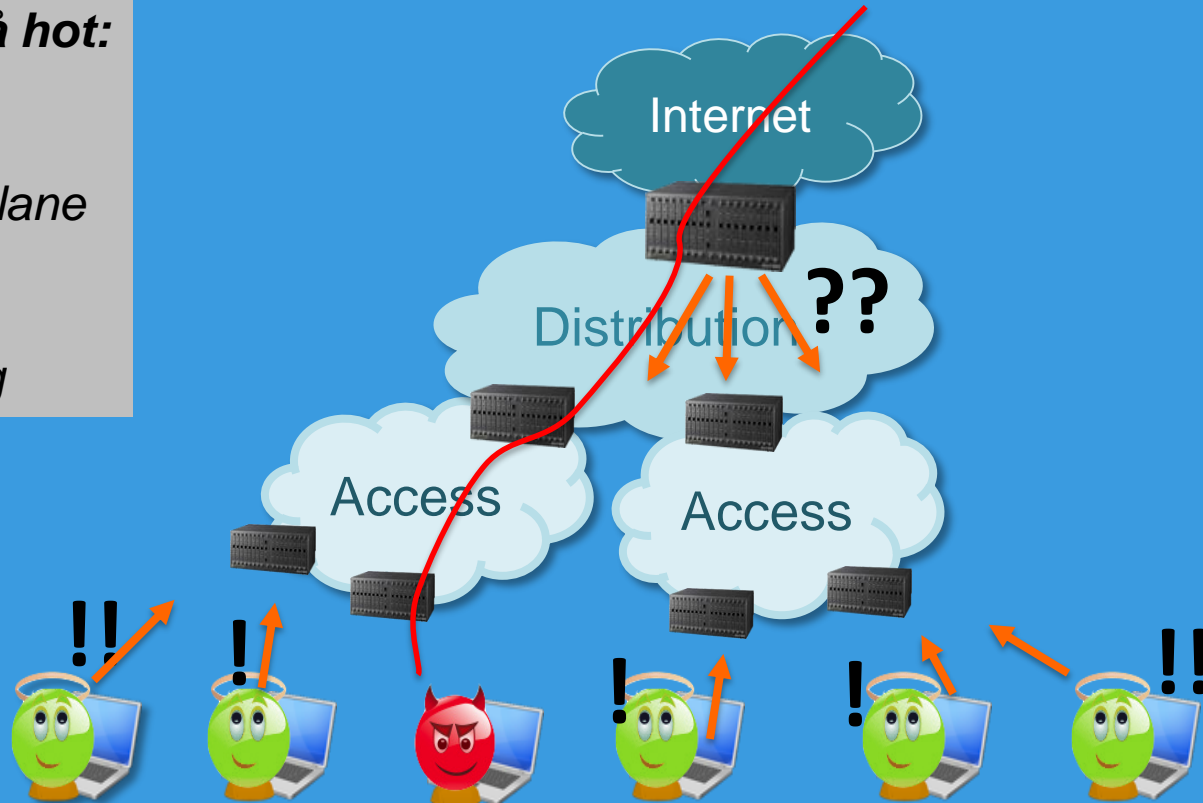
- *IP source guard*
- *DHCP option-82*



3. Tillgänglighet

Exempel på hot:

- DHCP flooding
- Control plane overload
- ARP poisoning



Varför ska du bry dig?

1. Dina kunder förväntar sig det
2. Du tappar marginal
3. Du är en del av globala DDoS-problematiken
4. Du bryter (kanske) indirekt mot lagen



Gör du tillräckligt?



SEC

Secure End-User Connection

- Bästa referensdokumentet för IPv4-säkerhet
- <http://secureenduserconnection.se/wp-content/uploads/2012/02/SEC-Secure-End-user-Connection-2014-05-30.pdf>
- Inkluderar även IPv6-säkerhet
- *Vad tycker du om detta dokument?*



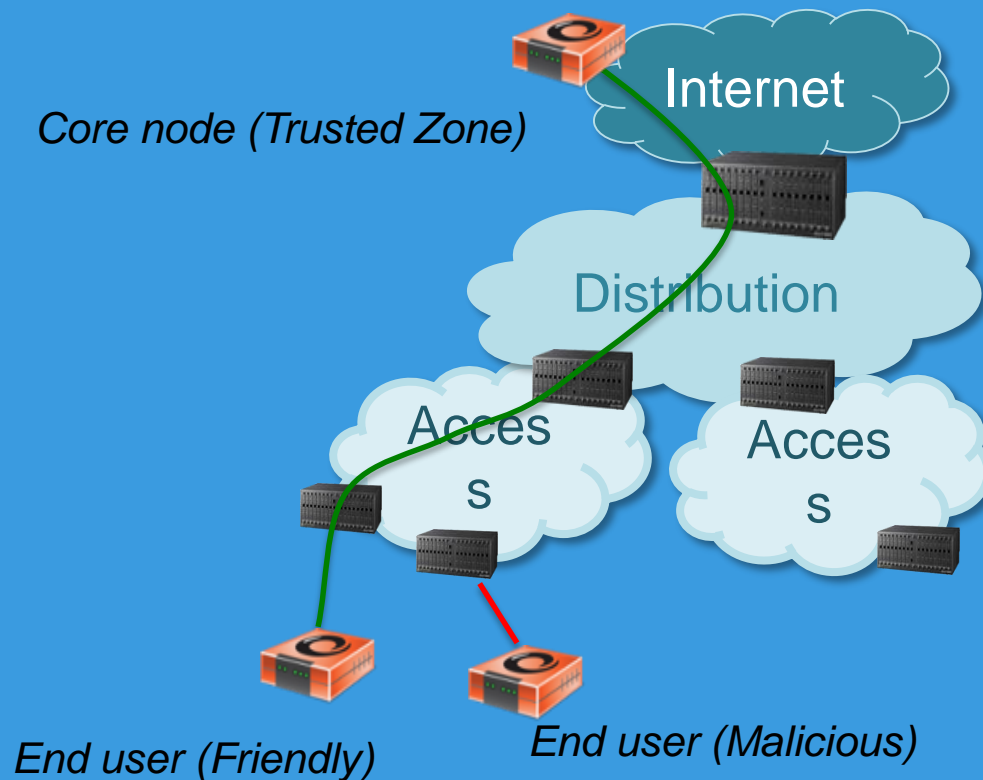
Nyheter

1. Alla nät som testats och godkänts för mer än två år sedan kommer att rensas bort från hemsidan – inte relevant helt enkelt
2. Ett test vartannat år ersätts med kontinuerliga automatiserade tester (dygnsvisa)
3. Intresselista för IPv6-certifiering – när fler än 10 stadsnät anmält intresse startar arbetet
4. D-link – först ut med certifiering av ett antal switchar för IPv6 – grattis!!!



Ett säkert nät – version 2

I ett SEC-certifierat nät garanteras säkerhet genom **dygnsvisa** automatiserade tester



Sammanfattning

- Certifiera utrustning IPv4/IPv6
 - Kontakta Torbjörn Eklöv på Interlan
- Certifiera nät IPv4
 - Kontakta sales@netrounds.com
- Övriga/generella frågor samt intresselista certifiering nät för IPv6
 - Jimmy Persson, SSNf



Tack

Frågor?



