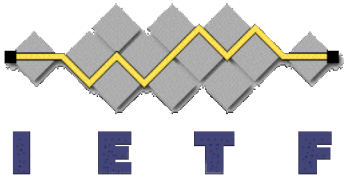
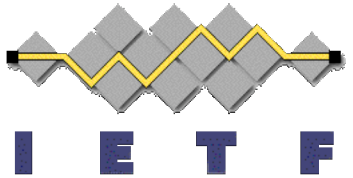


God nätverksdesign och distribuerade brandväggar

Patrik Fältström

<paf@cisco.com>



Brandväggar?

- Brandvägg är en funktion
  - En bra brandvägg får man enbart genom att kombinera olika skyddsmekanismer
- Färist är ett bättre namn…

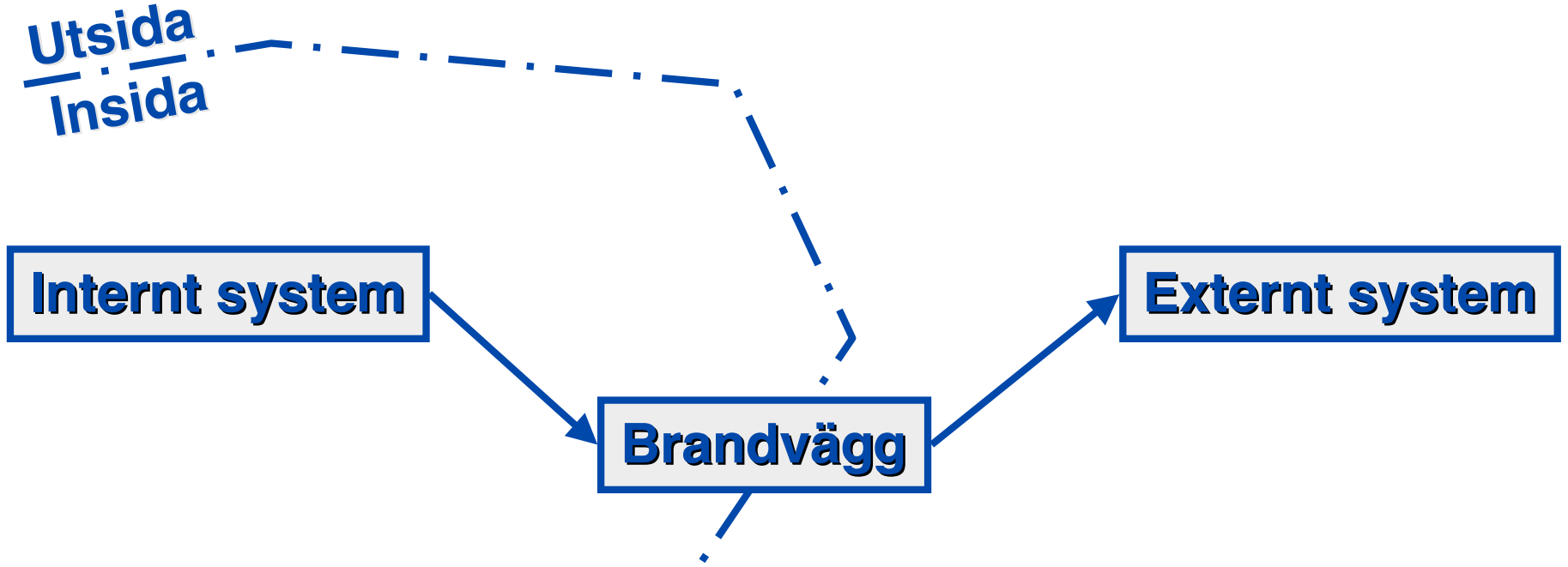
Behövs Brandväggar?

Vad är målet?

- Ingen obehörig ska komma åt känslig information i interna system
- Ingen information ska spridas av misstag
- Ingen extern händelse ska kunna störa interna system

Hur kunde man göra?

- Skilj på interna och externa system
- Implementera filter mellan interna och externa systemen



Gammal brandvägg

- Filtrera kommunikation på port/adress

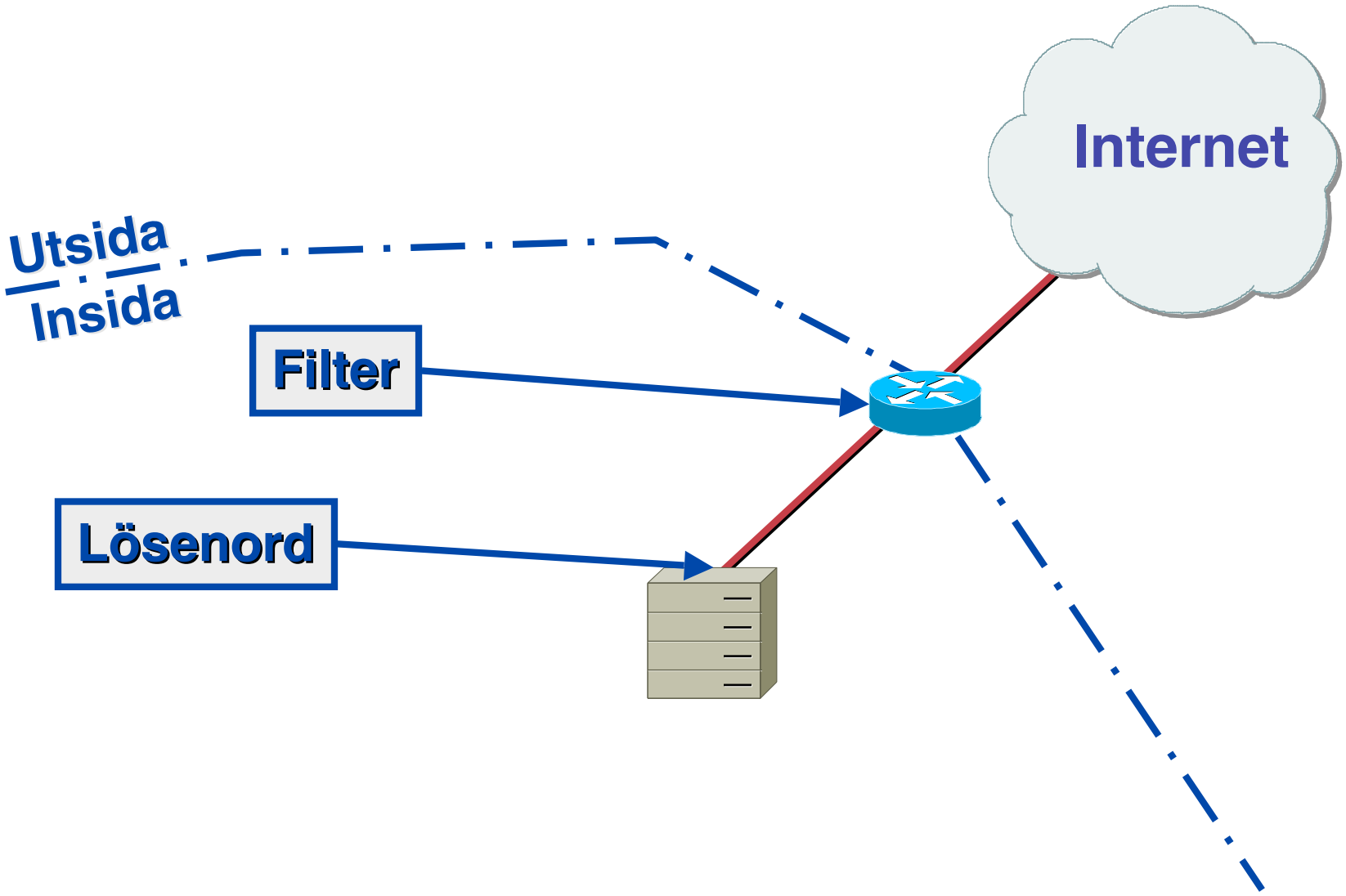
  access-list 20 permit 192.168.0.0 0.0.255.255

  access-list 20 permit 195.66.31.64 0.0.0.15

  access-list 20 deny   any

- Varje port/adress motsvarande en applikation eller tjänst
- En del tjänster hade separat accesskontroll (lösenord i Telnet/POP)

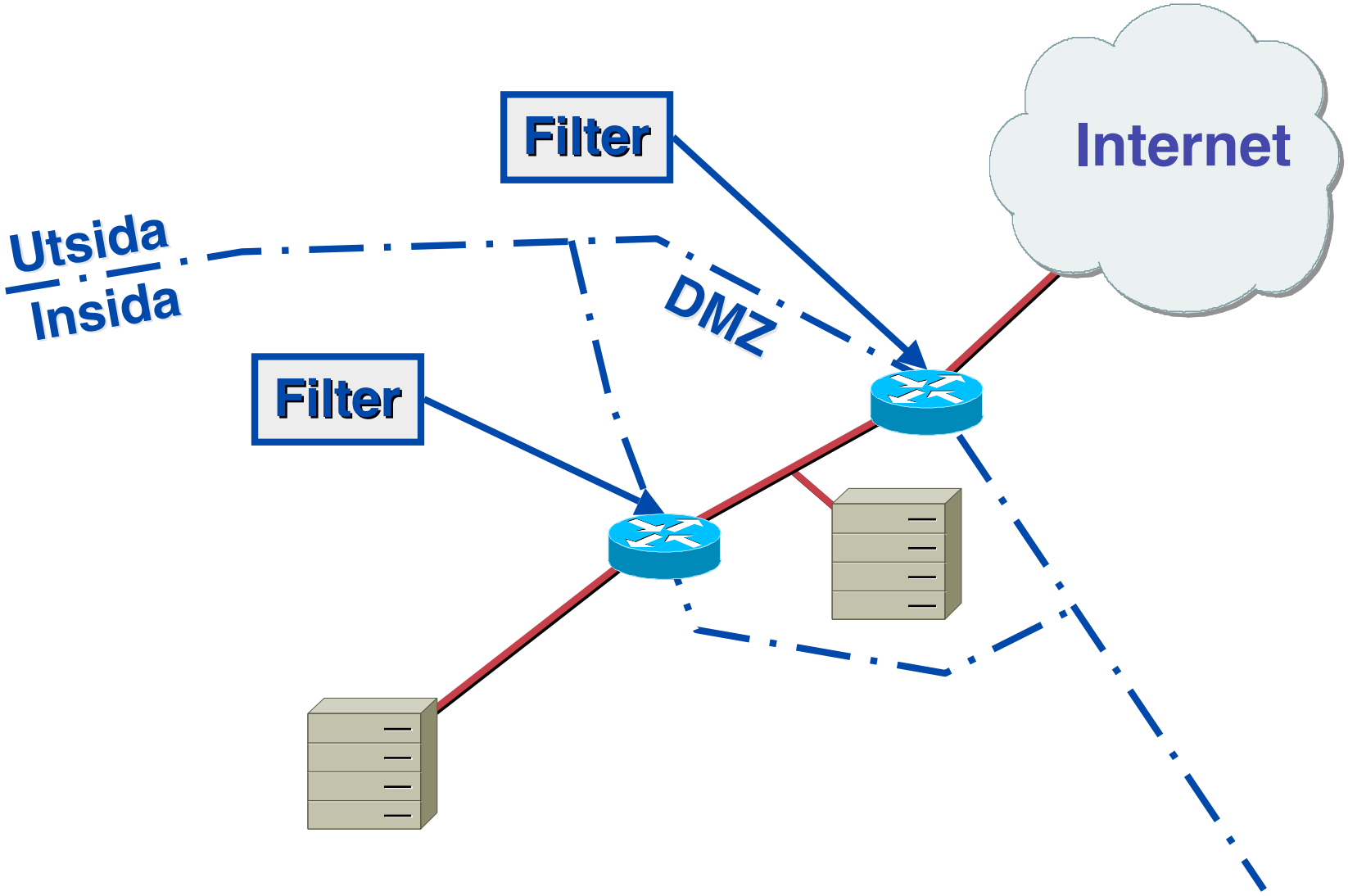
Hur det såg ut

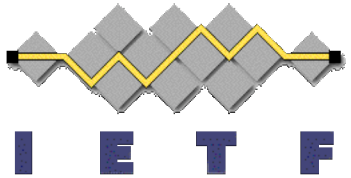


Mer komplicerat

- Allt eftersom behövdes tjänster som man skulle kunna komma åt från utsidan
  - ”Websida” för externa tittare
  - Men samtidigt behöver man en ”websida” för interna tittare
- Två filter?

DMZ

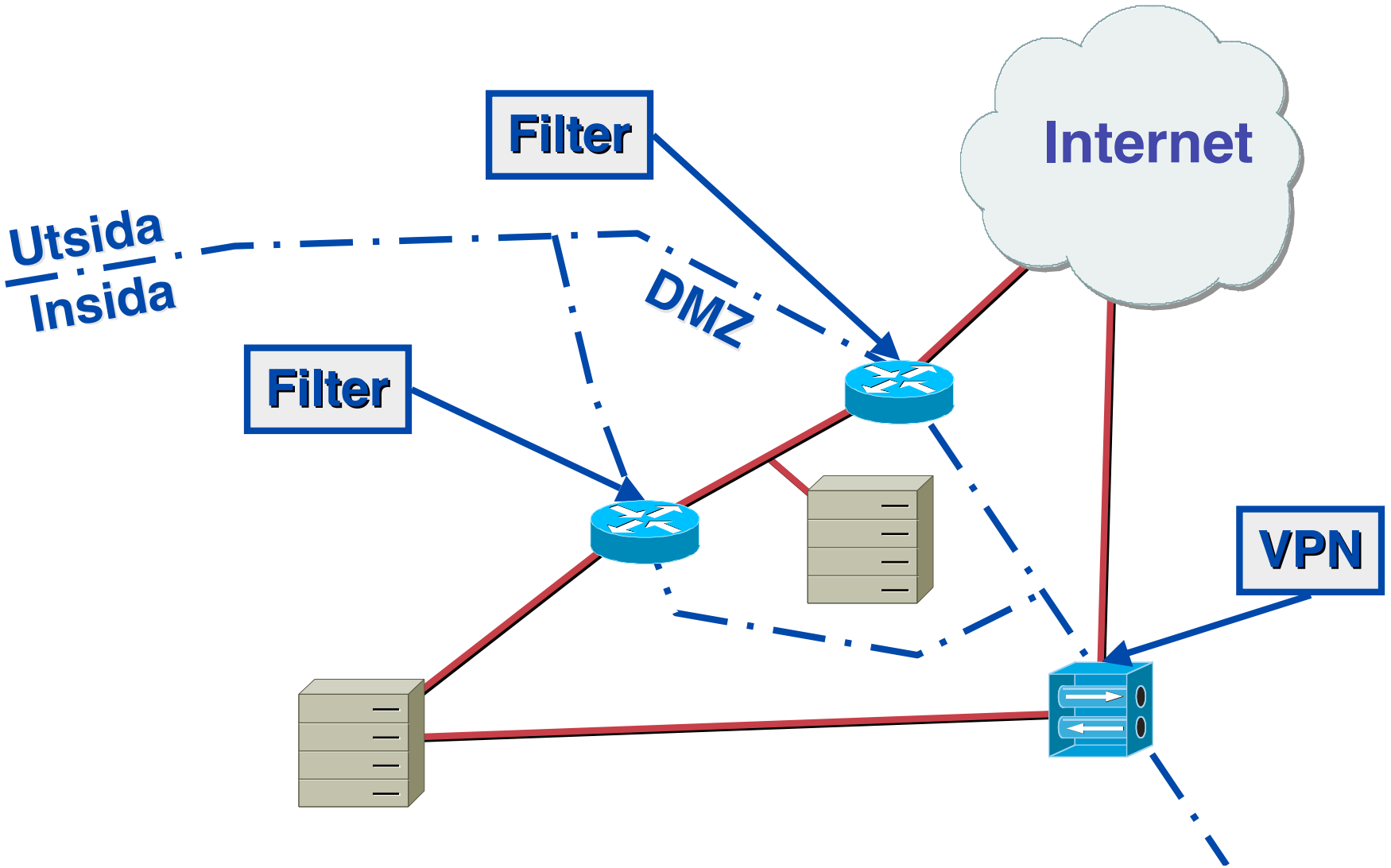




Mer komplicerat

- Det måste gå att komma åt interna tjänster från utsidan
- Detta görs med VPN, och om man inte tillåter access till interna nätet med VPN behövs en tredje säkerhetszon

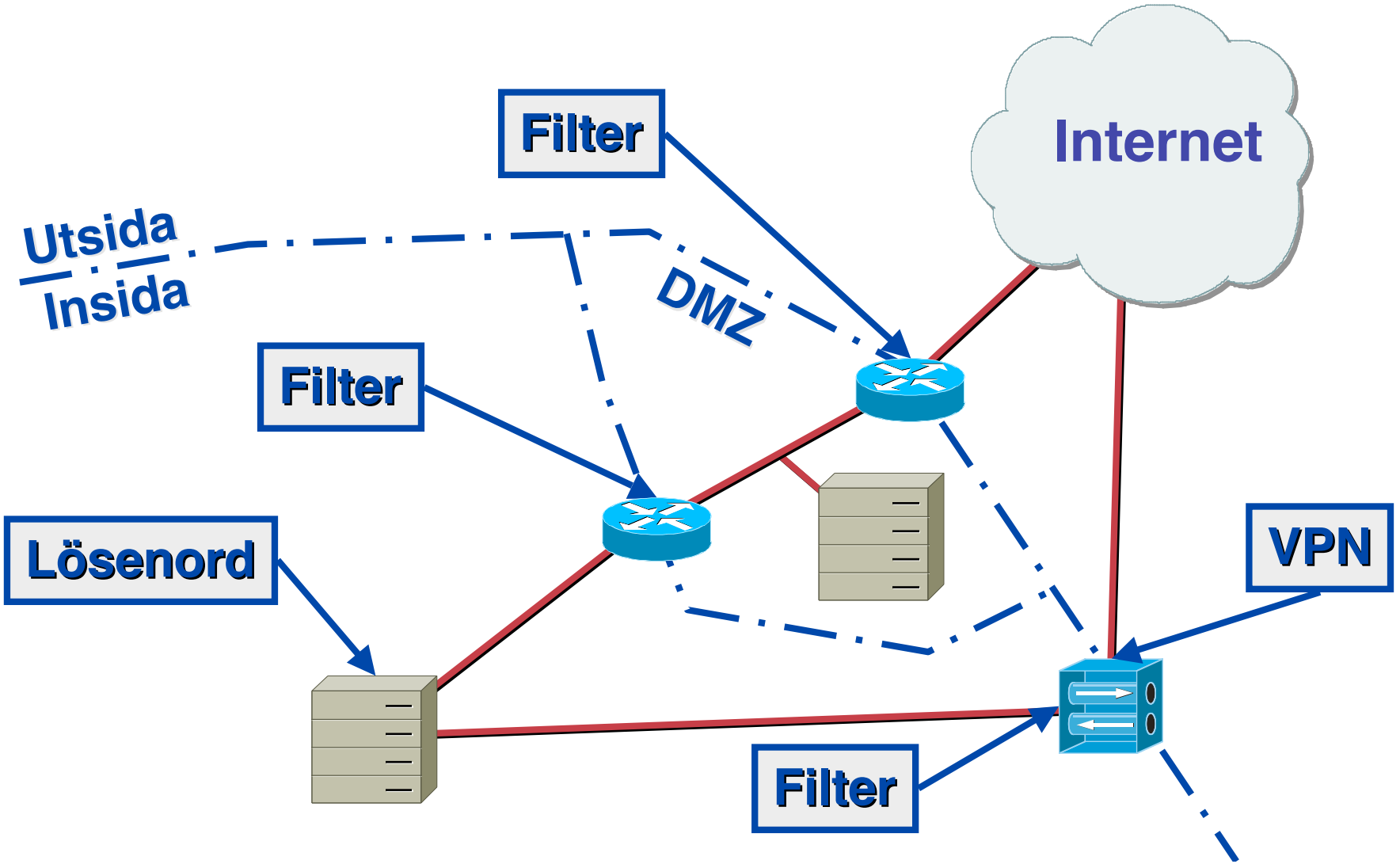
VPN



VPN med filter

- För säkerhets skull kanske man vill begränsa vad man kan komma åt via VPN-access
- VPN-termineringsburken har också filter
- System med interna tjänster har lösenord

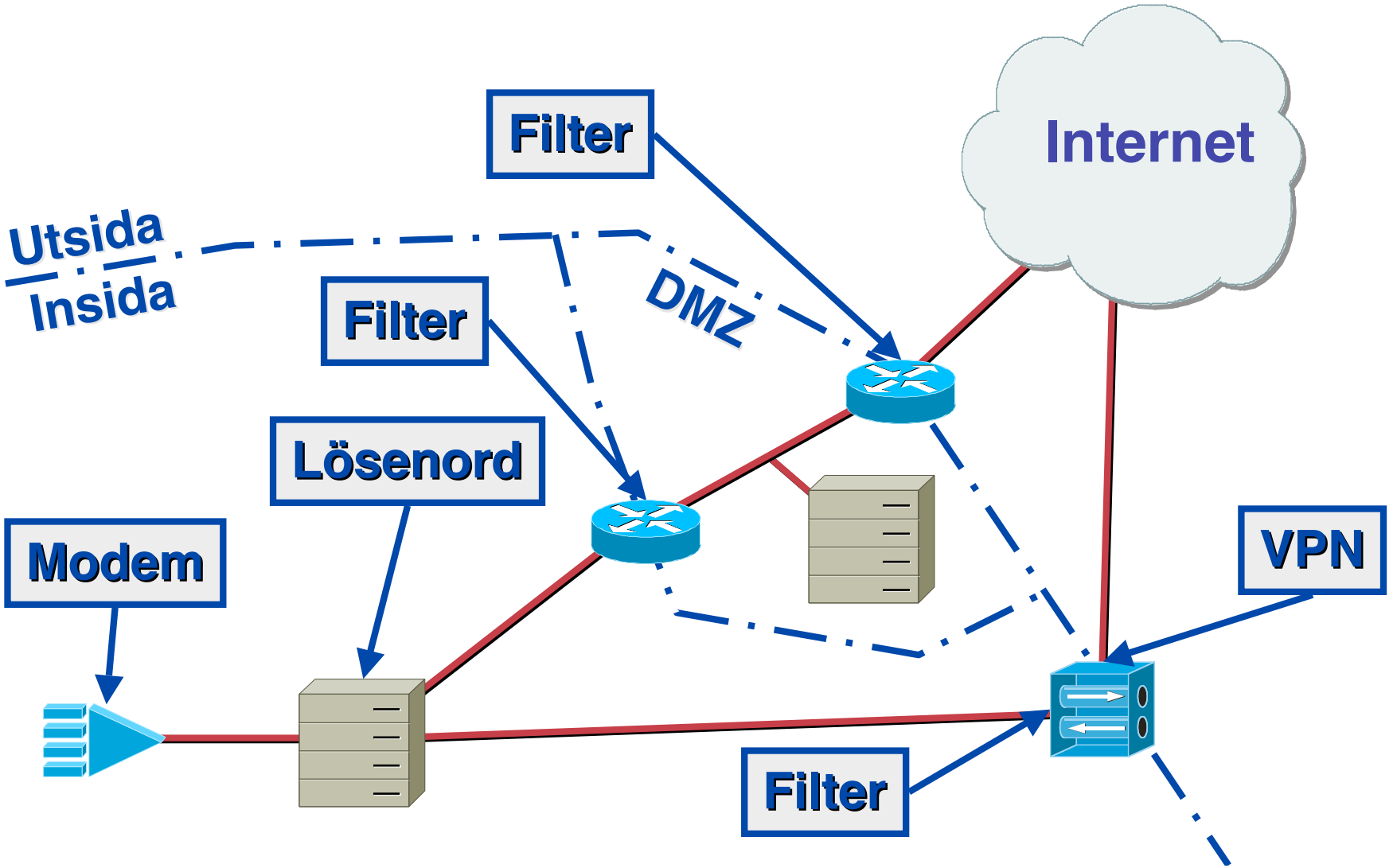
VPN med filter



Accesskontroll internt

- Alla användare kanske inte ska ha access till alla tjänster
  - Man kan dela in nätet i flera delar
  - Man kan ha accesskontroll
- Speciellt om man kan komma in direkt på interna nätet (via modem/ISDN?)

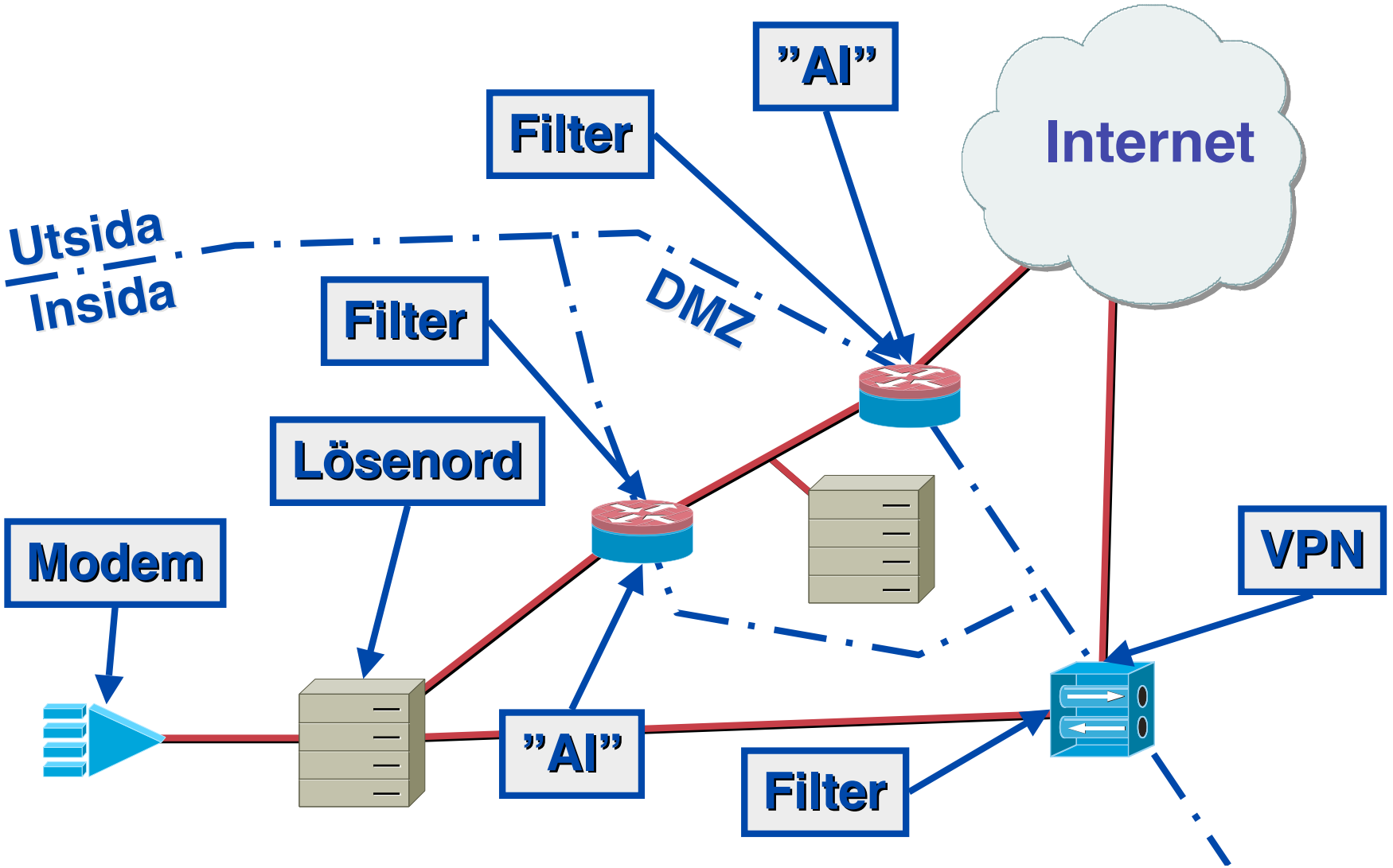
Direkt access internt



En attack?

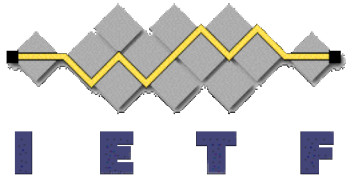
- Attacker kan komma som massiva denial of service-attacker
- Saker som slinker igenom kanske har felaktiga TCP-paket, falsk avsändare etc
- Mer intelligens behövs vid de filter man har, samt vid de olika applikationer som tar emot trafik

Mer intelligens



”Protocol layering”

- Idag kan man använda ”web services”
- Det innebär att man kör
  - Remote procedure call
  - XML/SOAP
  - HTTP
- Detta är inte samma som normal ”webaccess”
- Hur ska man skilja på det?

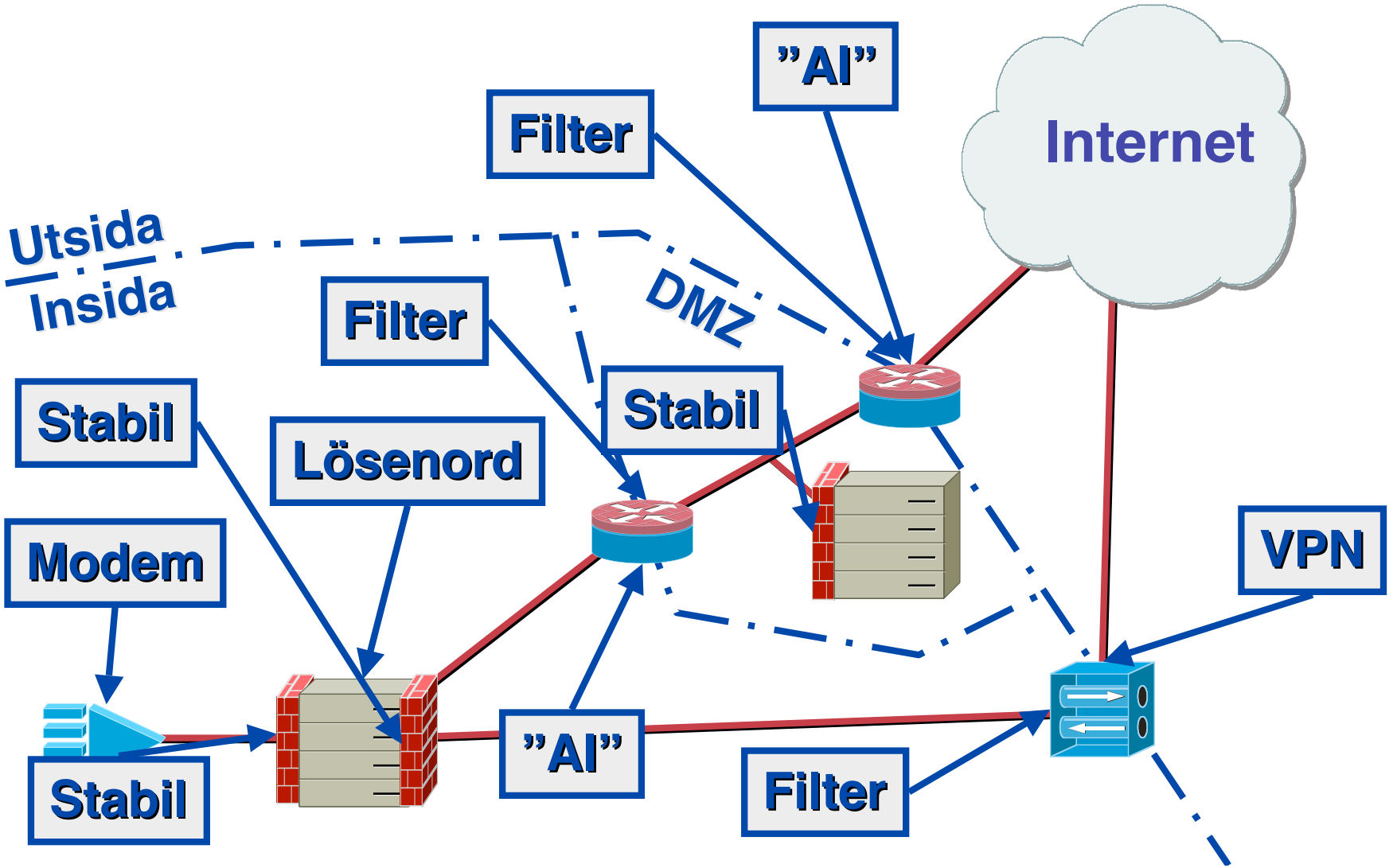


Mer stabil tjänst

- Tjänsten själv måste vara stabil
- Trots att den normalt ska ta emot tex SOAP, så måste den klara annan användning

- Den får inte krascha när det kommer felaktiga kommandon

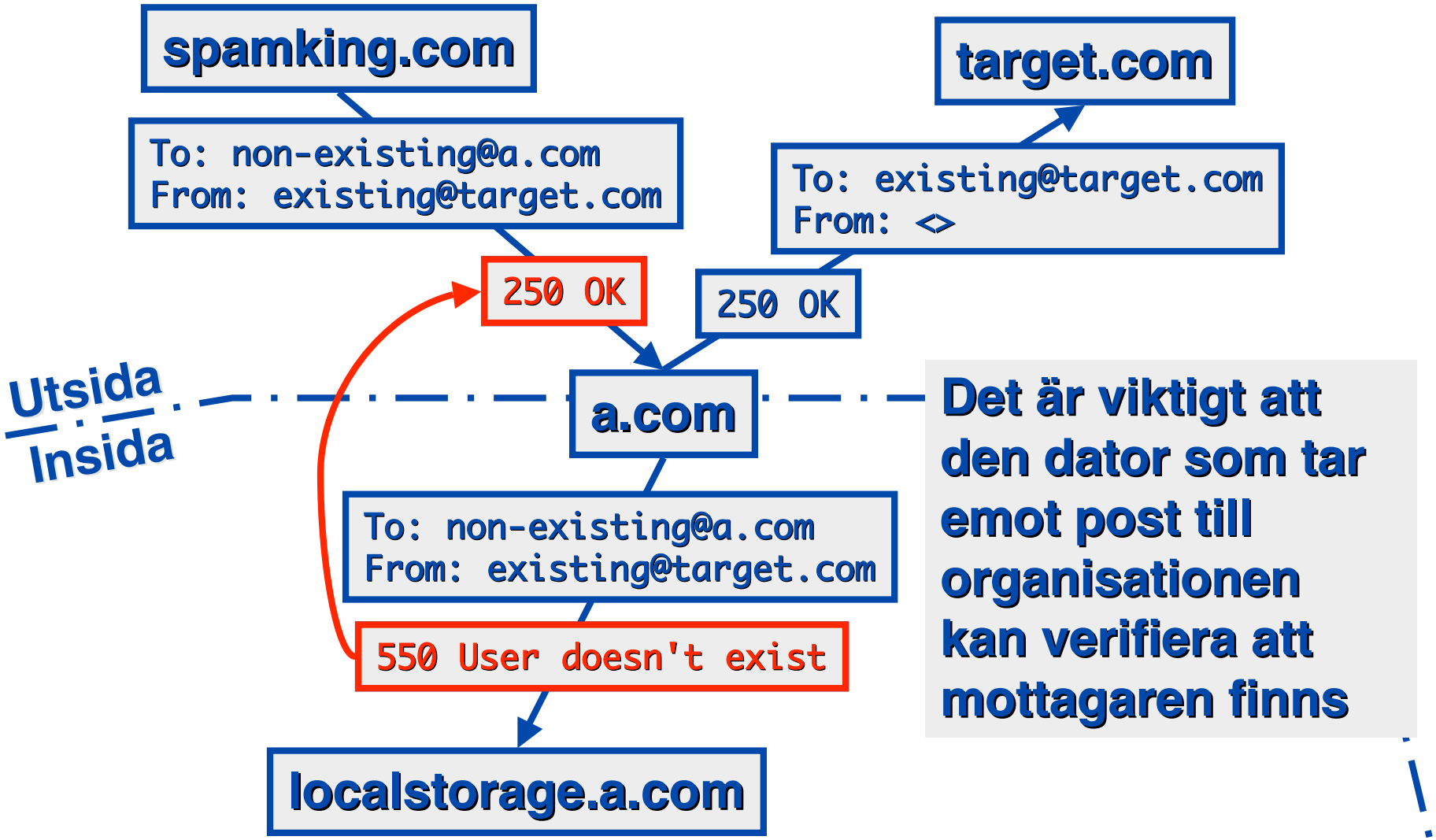
Stabila applikationer



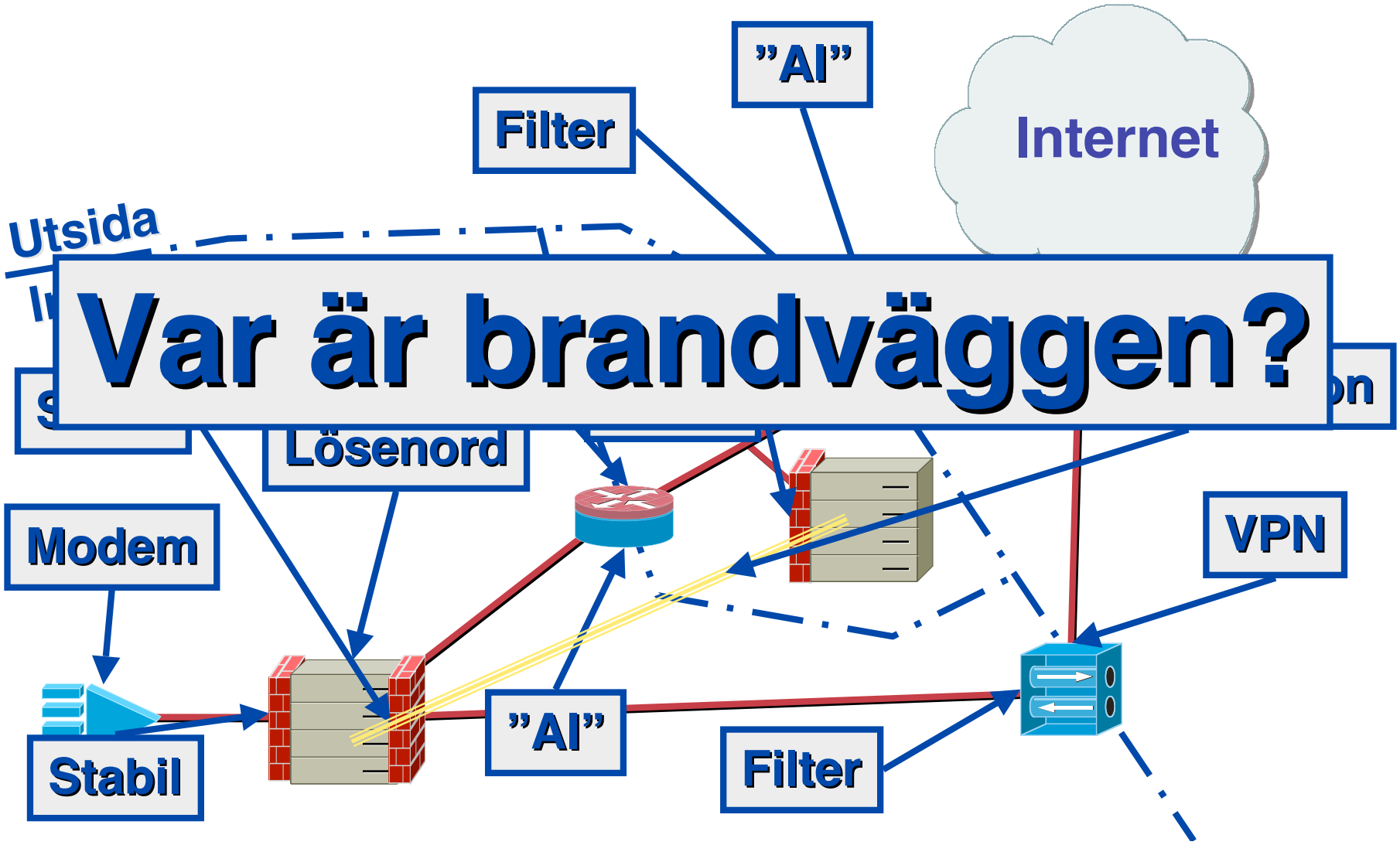
Attacker mot organisationen

- I en del fall skapas det en attack som ger andra typer av biverkningar
- Skapa ”badwill” för företaget
- Tex, spam önskas inte, så man kan få spam att se ut att komma från vem man vill
- Mailsystem måste i detta fall vara stabilt och korrekt implementerat

Indirekt attack

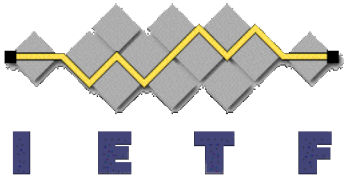


Slutsats…


Var är brandväggen?
”Al”
Filter
Internet
Utsida
Lösenord
Modem
VPN
Stabil
”Al”
Filter

Brandvägg?

- Den svarta boxen har tappat sitt värde
- Varje nod måste vara säker
- Inklusive datorer som flyttas mellan publika och interna nätet (speciellt…)
- Vet du vad alla saker i ditt nät gör?



Patrik Fältström
paf@cisco.com