Att Säkra Internet Backbone

Håkan Nohre

hnohre@cisco.com

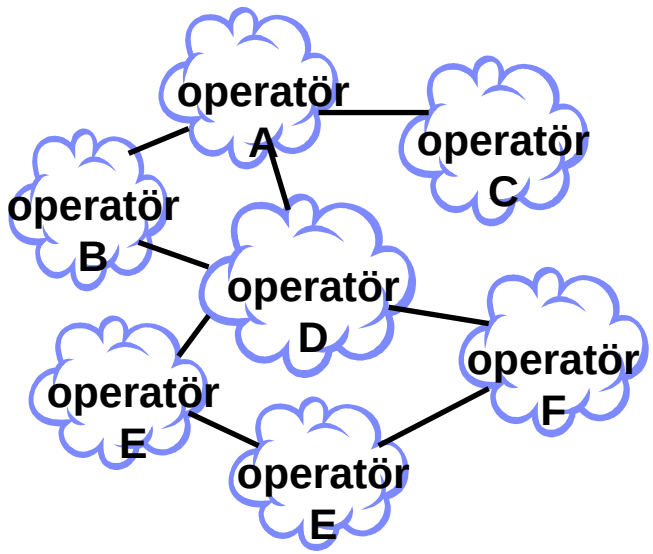
Vad kan attackeras

Attackera routrar/switchars förmåga att vidarebefordra data
- **logiska attacker (mot buggar, protokoll)**
- **paketstormar (mot bandbredd, CPU)**

Attackera routingen (BGP)
- **slå ut BGP peerer**
- **injicera falsk information**

Attackera DNS
- **slå ut DNS servrar**
- **injicera falsk information**

Attackera backendsystem
- **billing, kundregister etc.**



Zombies, DDOS, Belastningsattacker

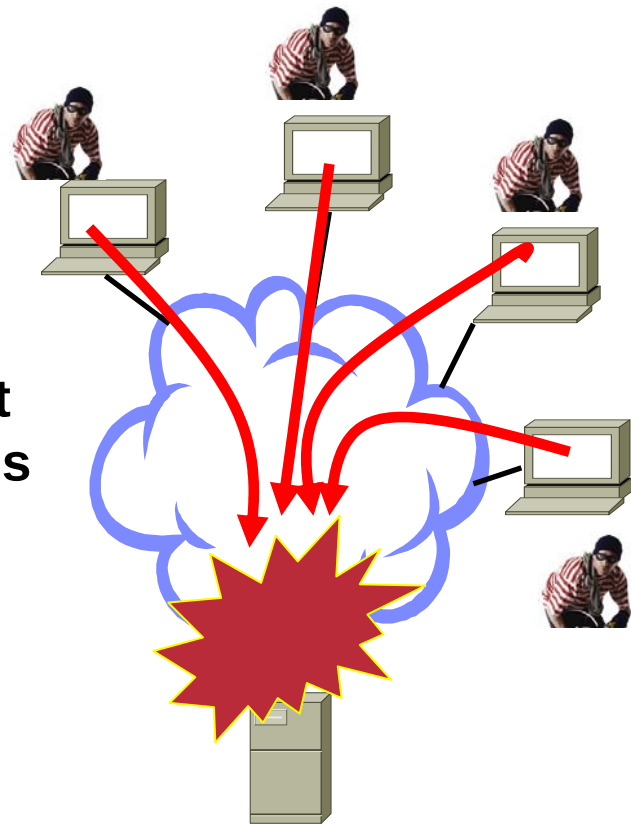
Hacker kontrollerar ett stort antal hackade maskiner (via t.e.x mask, trojan, virus)

Kan på given signal generera en paketstorm mot mål (kan vara operatörens kund eller operatörens egen utrustning)

I bland spoofas (förfalskas) avsändaradress

Kan attackera bandbredd (stora paket) eller CPU (många paket per sekund)

Collateral Damage



Målet

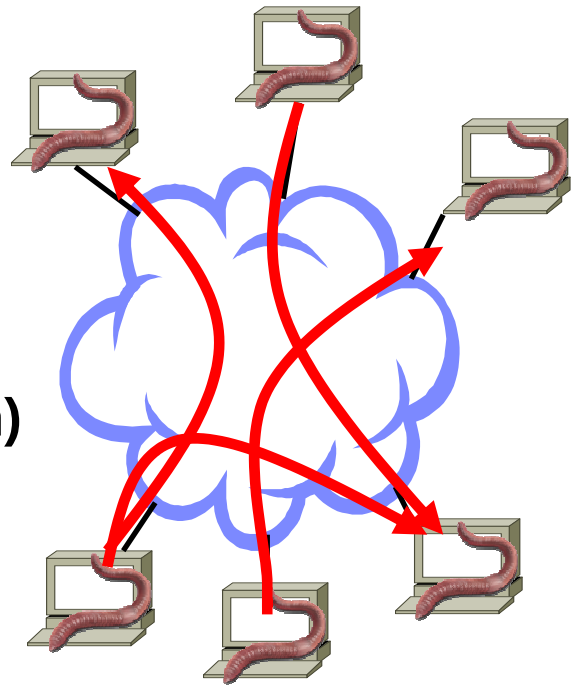
Maskar

Maskens primära mål är slutstationer ej nätverket

Kan dock generera onormala traffikmängder

....med abnorma traffikmönster (oändligt antal destinationsaddresser och mycket korta flöden)

Collateral Damage

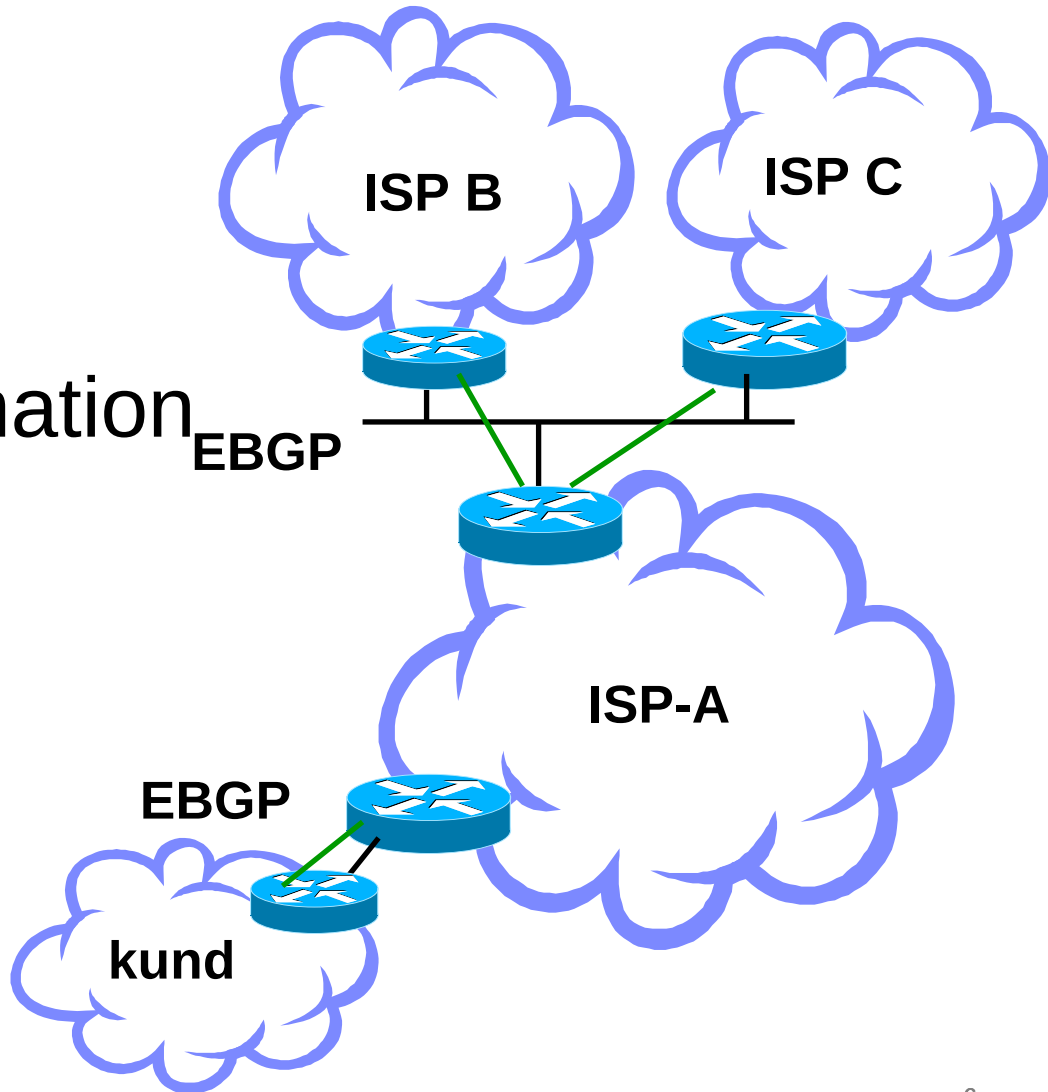


Hur skyddar sig Operatörer ?

- Förberedelser är A&O
- Processer och Policys
- Utbildat & Förberett OPSEC (IRT) team
- Förberedda kontakter med
  - andra ISP:er (konkurrenter)
  - leverantörer
  - viktiga kunder
- Verktygslåda med tekniska knep

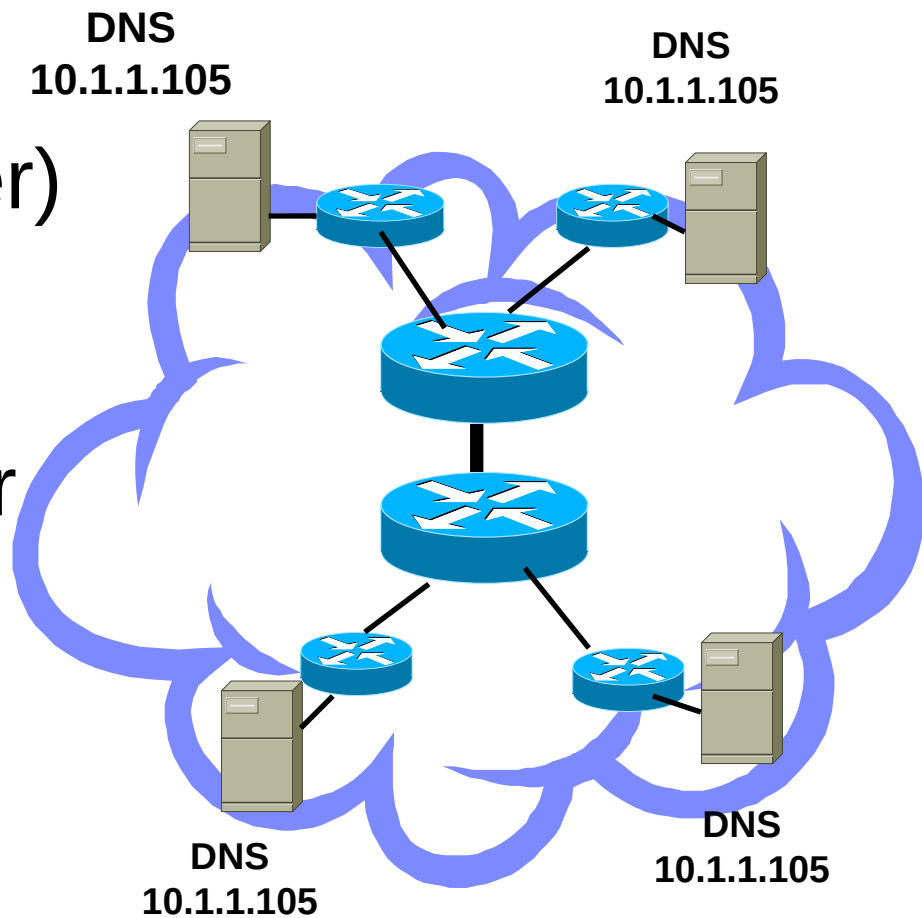
Skydda Routing

- MD5-autensiering
  (vem talar jag med)
- Filtrera routing information
  vilka nät ?
  hur många nät ?



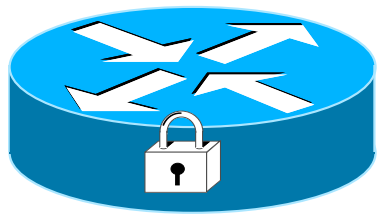
Skydda DNS

- Mot Falsk Information
  - Säker (patchad server)
  - DNS-sec
- Mot Belastningsattacker
  - Många DNS servrar
  - Lastbalansering
  - DNS anycast
  - DDOS-tvätt



Generell Router/Switch Säkerhet

- Bugfixar, CERT alerts
- Krypterad management (SSH)
- Autensierade Routing protokoll
- Engångslösenord för inloggning...
- NTP för exakta tidsstämplar i loggar



- ...tillåt endast management från vissa ip adresser ....

Varning : Säkra Management/kontrollplanet

- **Core-routrar kan switcha flera miljoner paket per sekund genom routern genom optimerad hårdvara**

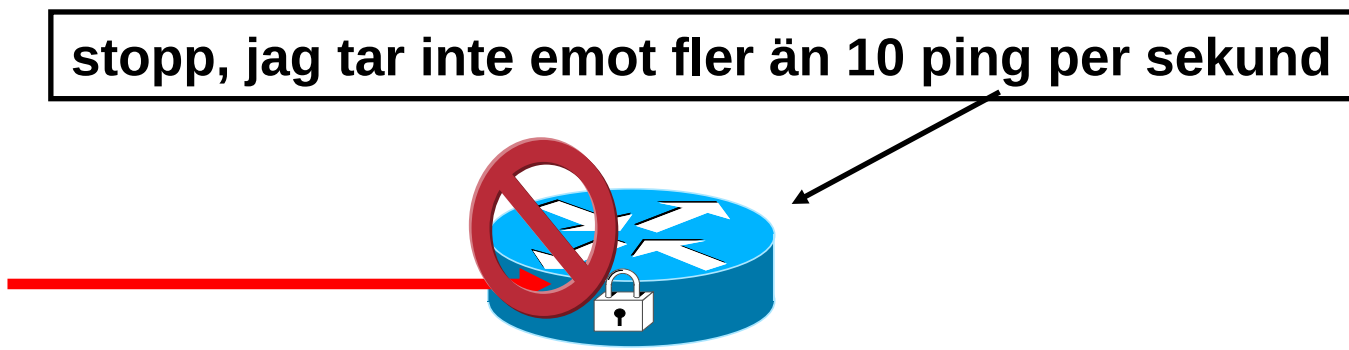
men

- **Routern kan få problem om den får för många paket till sig själv (CPU, ej hårdvara)**

Säkra Management/kontrollplanet (2)

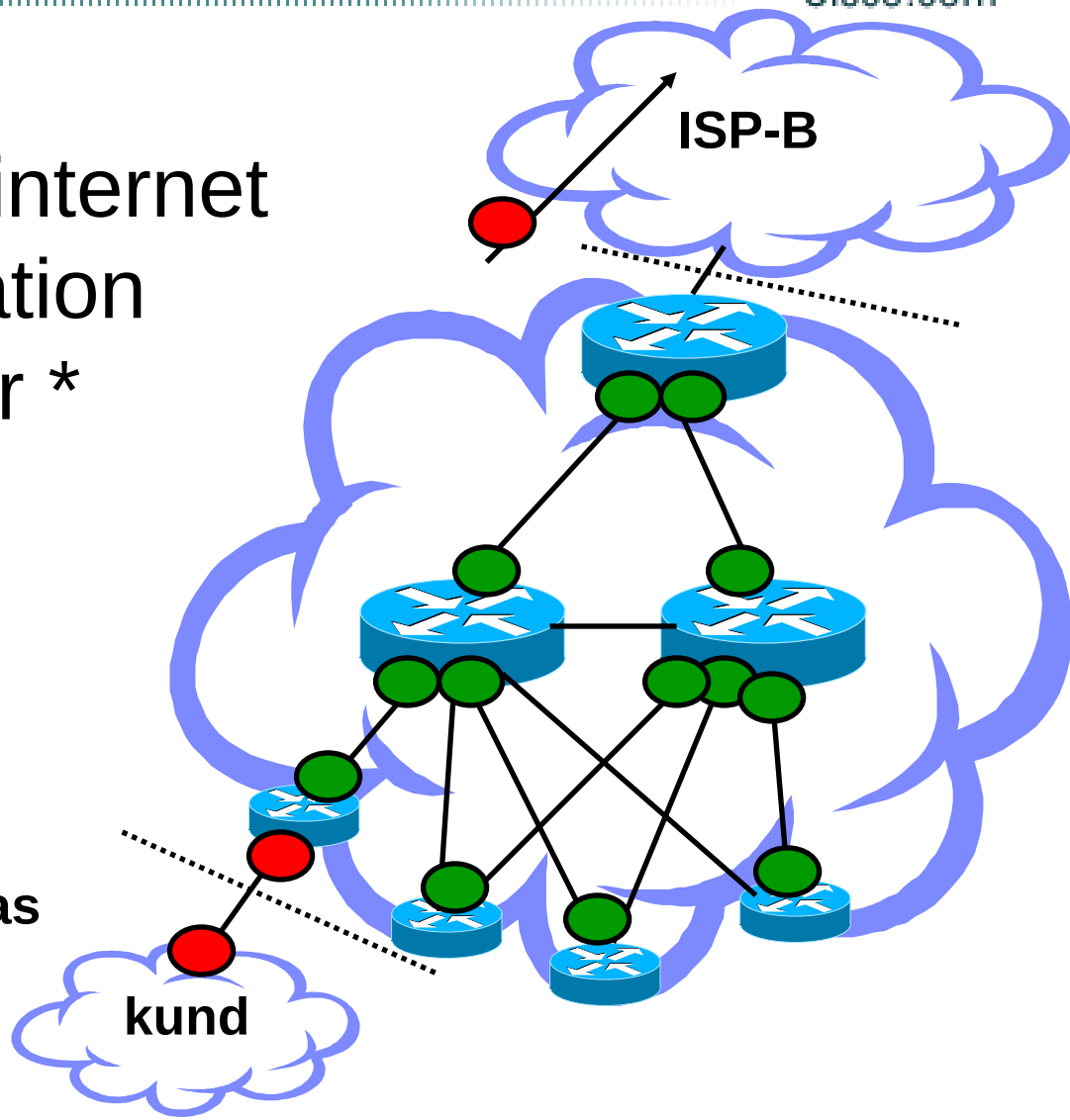
- **Begränsa paket till routern, t.e.x**
  bara från 10.1.1.0/24 (vårt managementnät)
  routing updates från grannar
  max 10 paket per sekund

Control Plane Policing



Skydda Core Routrar

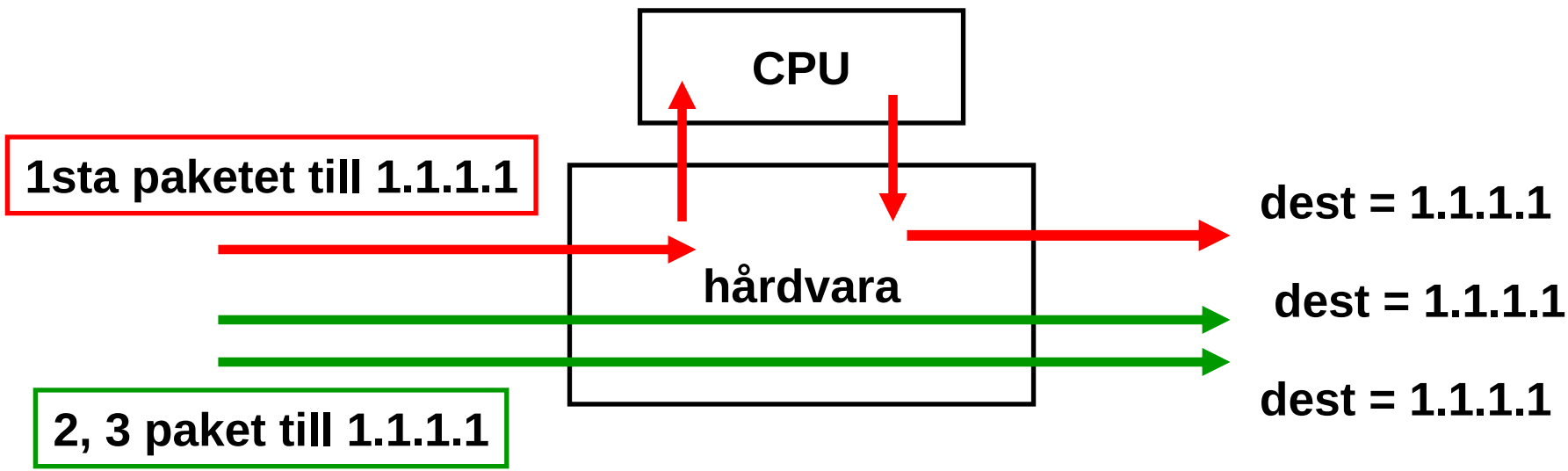
- behöver ej nås från internet
- filter, routing information
- privata länk adresser *



*** ping och traceroute kan störas**

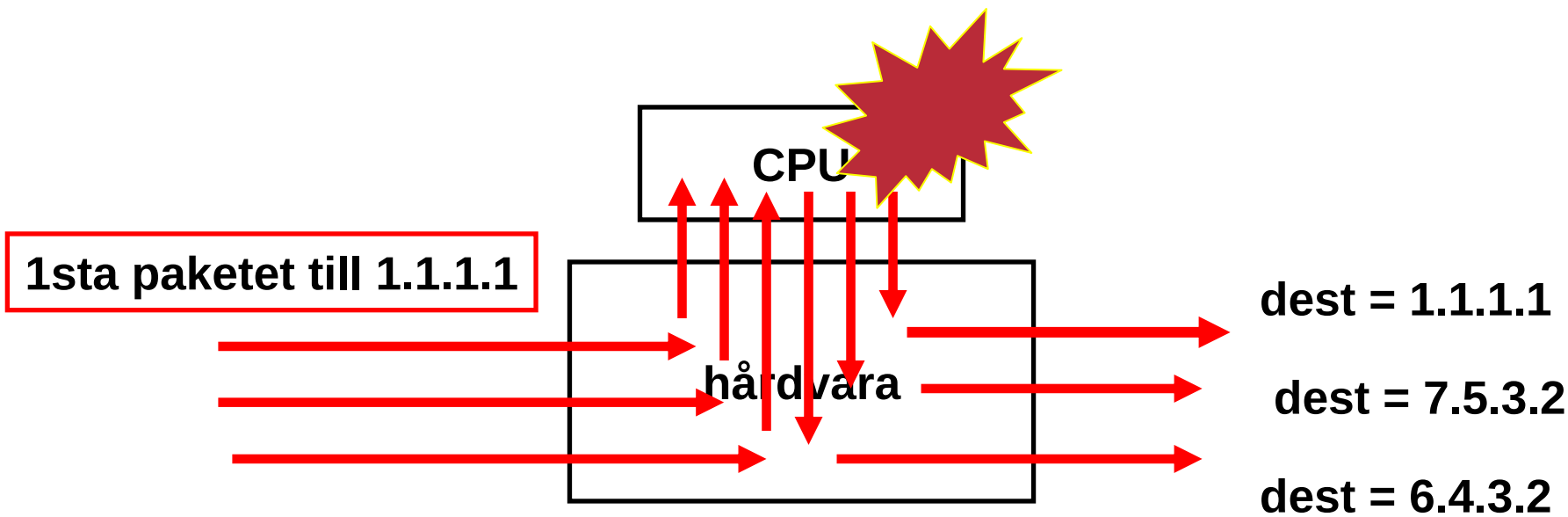
Abnorma trafikmönster och cache baserad forwarding

- Vissa router-arkitekturer byggar på caching.
- Första paketet till en destination går till CPU
- CPU uppdaterar hårdvara med routing info
- Efterföljande paket switchas i hårdvara



Abnorma trafikmönster och cache baserad forwarding (2)

Maskar och vissa DDOS attacker leder till abnorma trafikflöden med oändligt antal destination

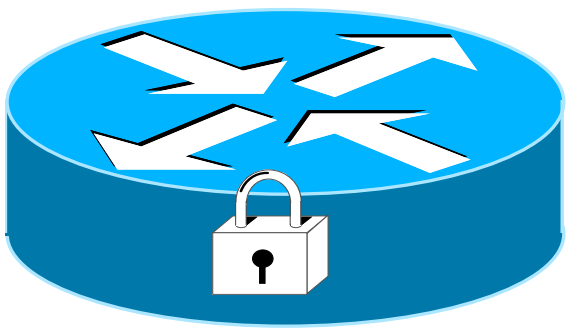


Abnorma trafikmönster och cache baserad forwarding (2)

En robust routers prestanda påverkas inte av antalet flöden/antalet destinations adresser.

Punkt.

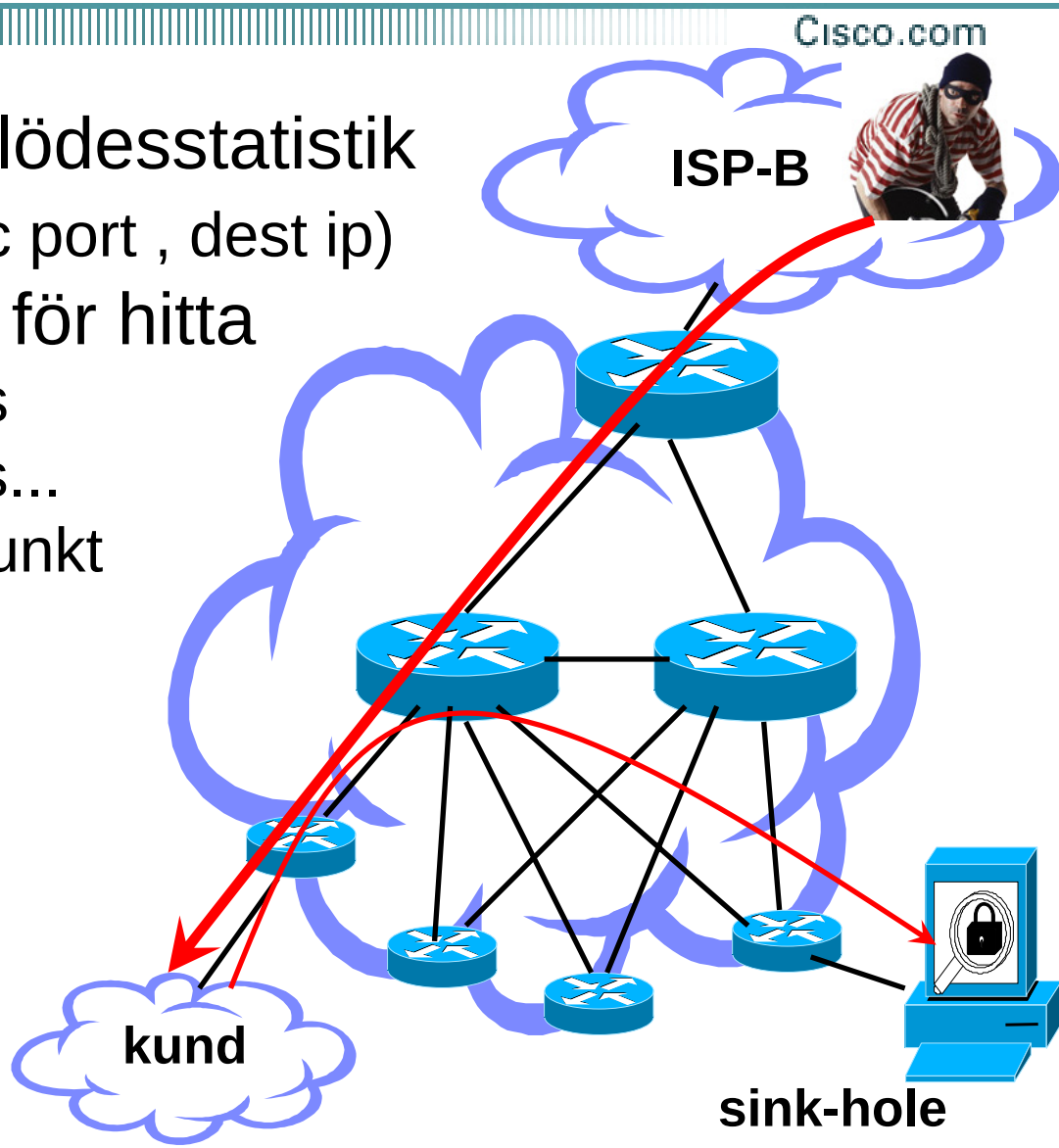
 # ip cef



Flödesanalys (t.e.x Netflow)

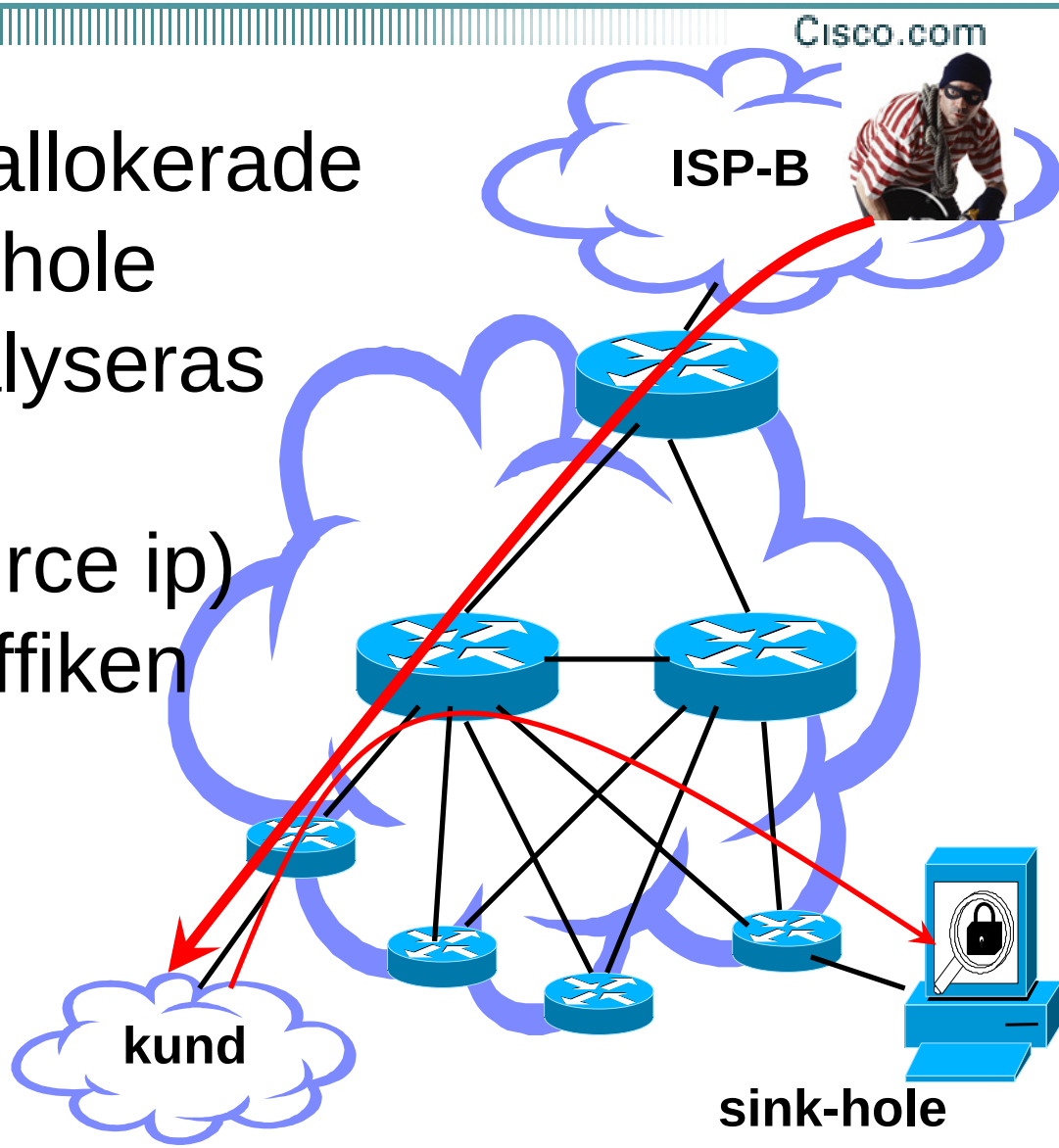
- Routrar kan exportera flödesstatistik

  flöde = (src ip , dest ip, src port , dest ip)
- Flöden kan analyseras för hitta
  - vilka siter som attackeras
  - typ av attack, volym , pps...
  - attack source / ingress punkt



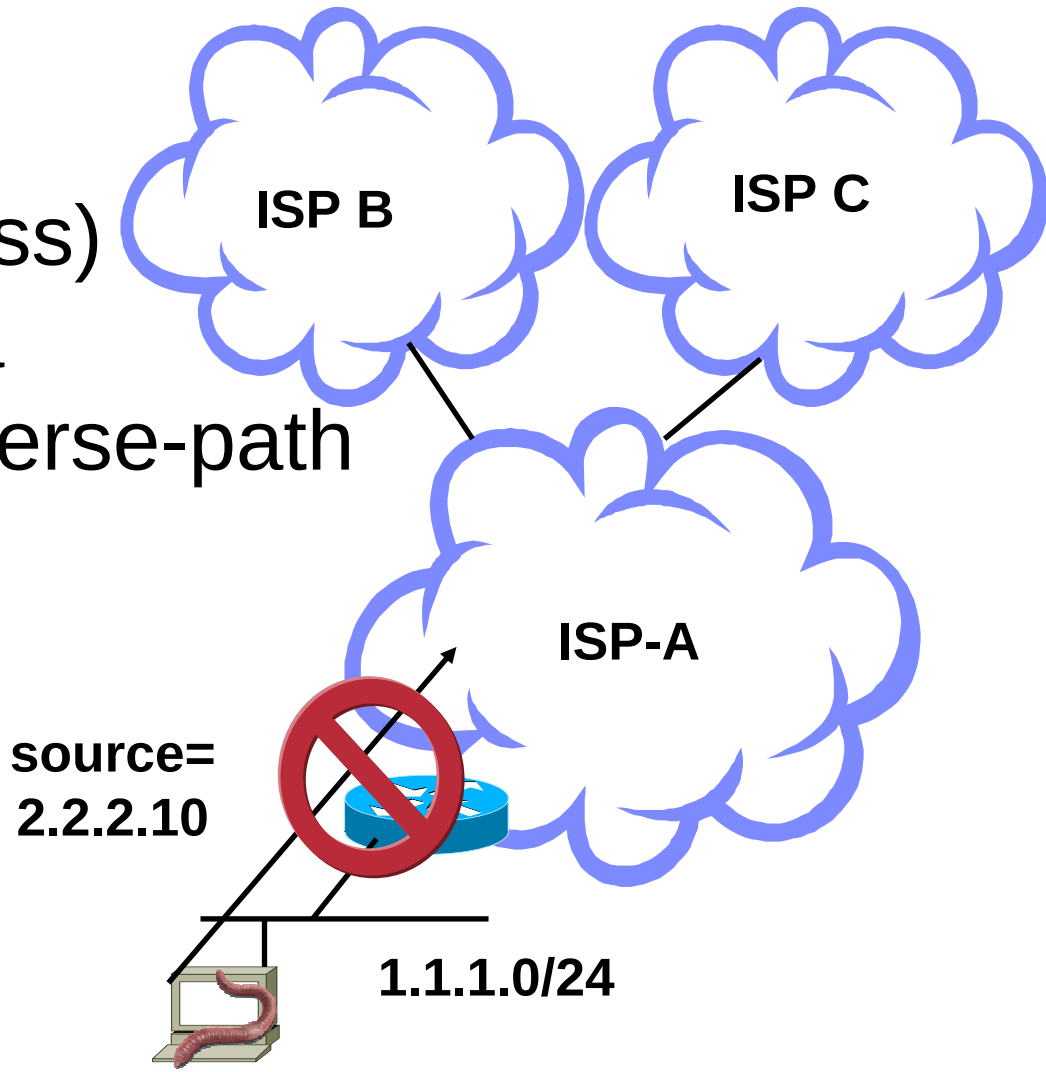
Sink-holes

- Routa all traffik till oallokerade adresser till s.k sink-hole
- Där kan trafiken analyseras
  vem attackeras
  vem attackerar (source ip)
  varifrån kommer traffiken
    (vilken ISP)



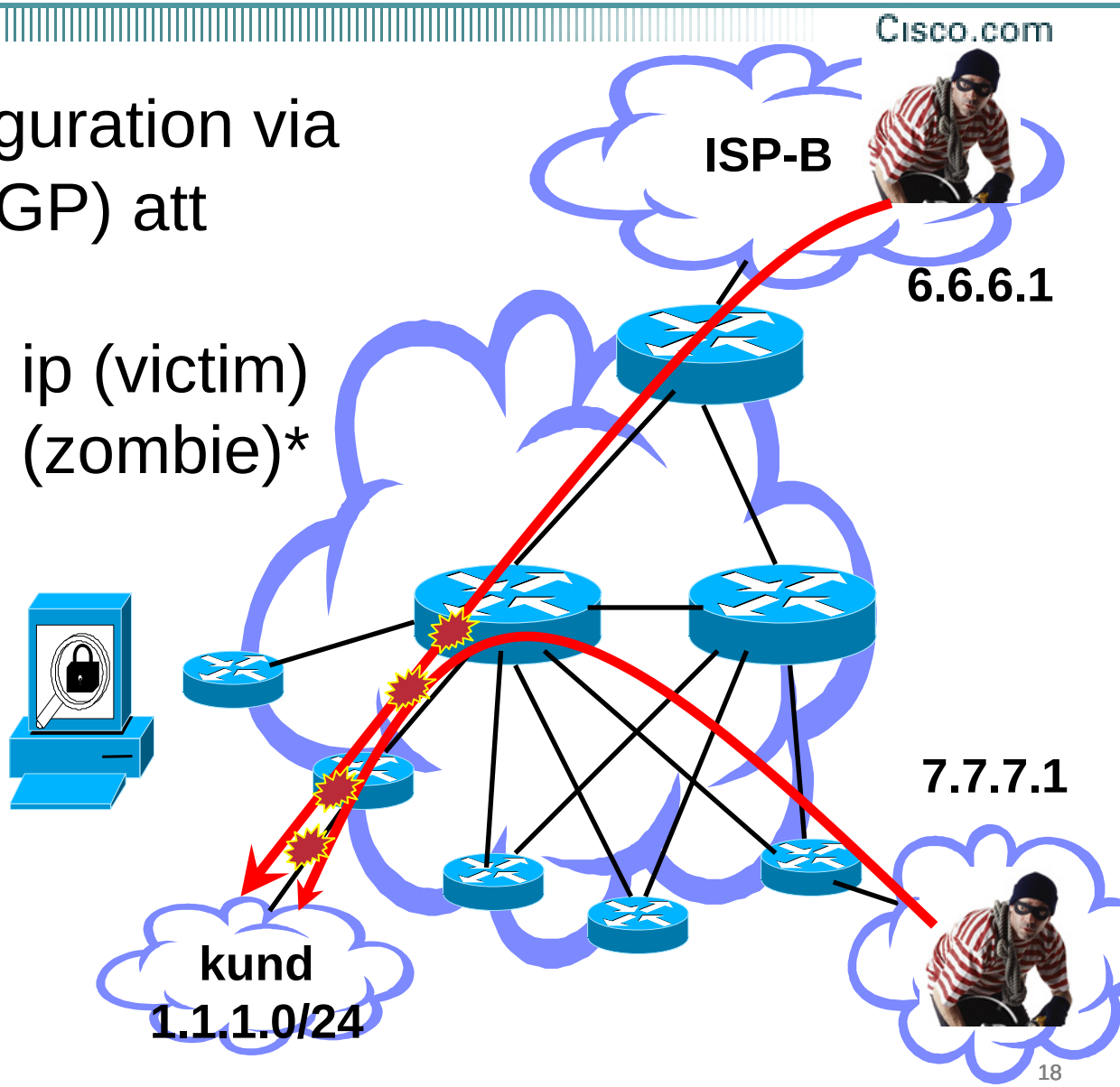
Anti-spoofing

- Stoppar Spoofing (falsk avsändaraddress)
- Enkelt att konfigurera
  ip verify unicast reverse-path



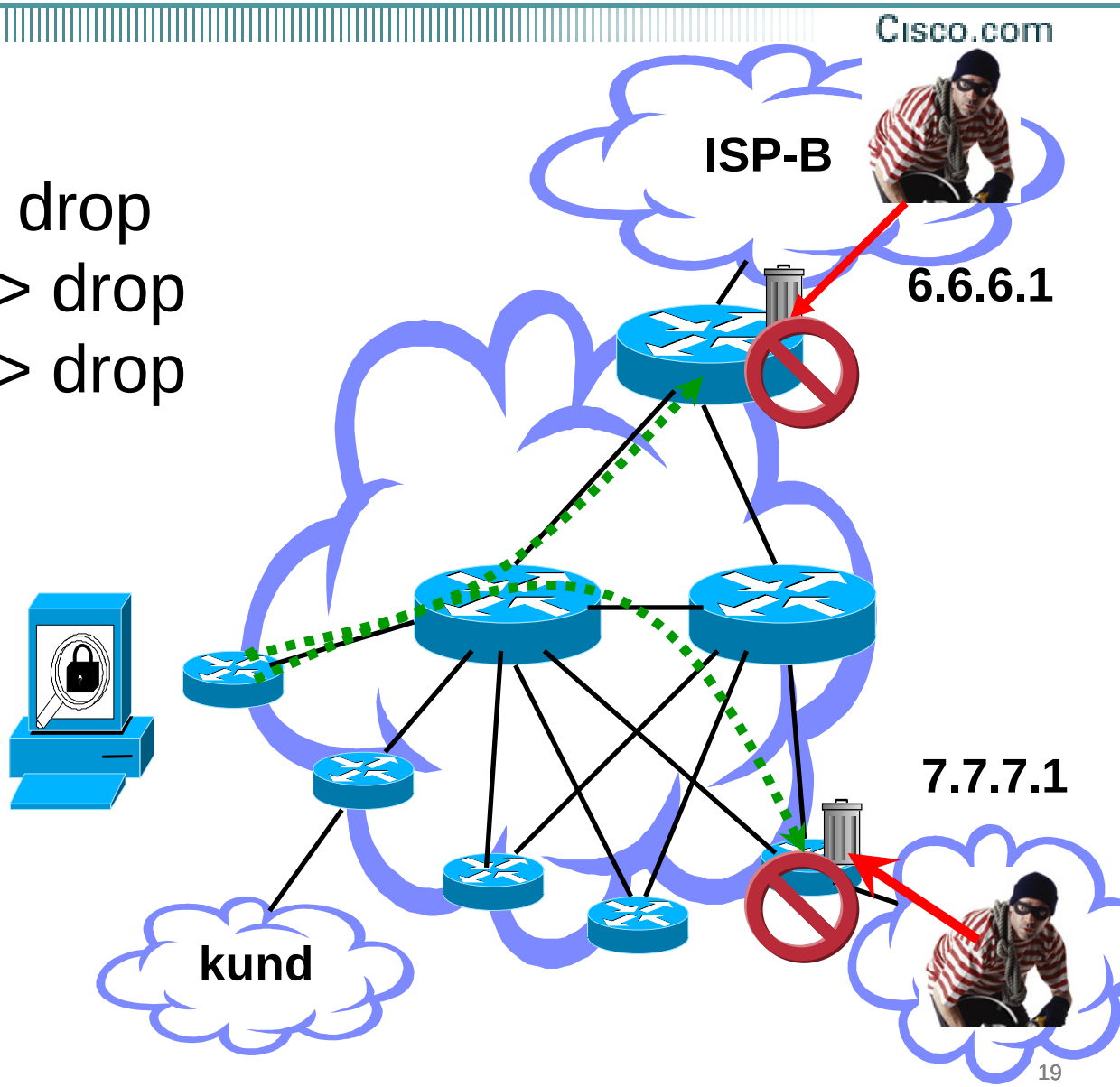
Black-holing

- Dynamisk omkonfiguration via routing protokoll (BGP) att stoppa all traffik
  - till destination ip (victim)
  - från source ip (zombie)*



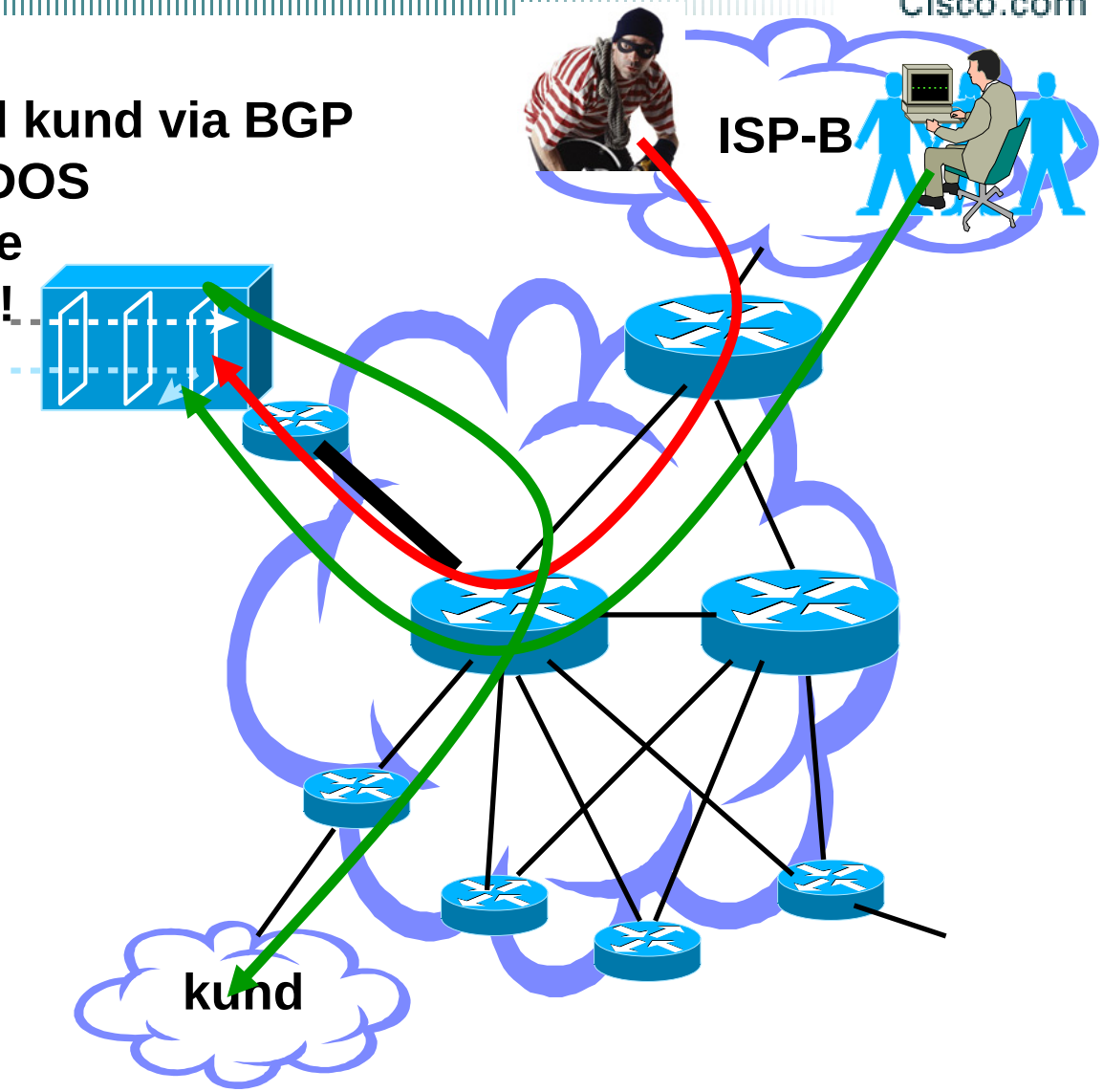
Black-holing

- BGP Update ->
  - trafik till 1.1.1.0 -> drop
  - trafik från 6.6.6.1-> drop
  - trafik från 7.7.7.1-> drop

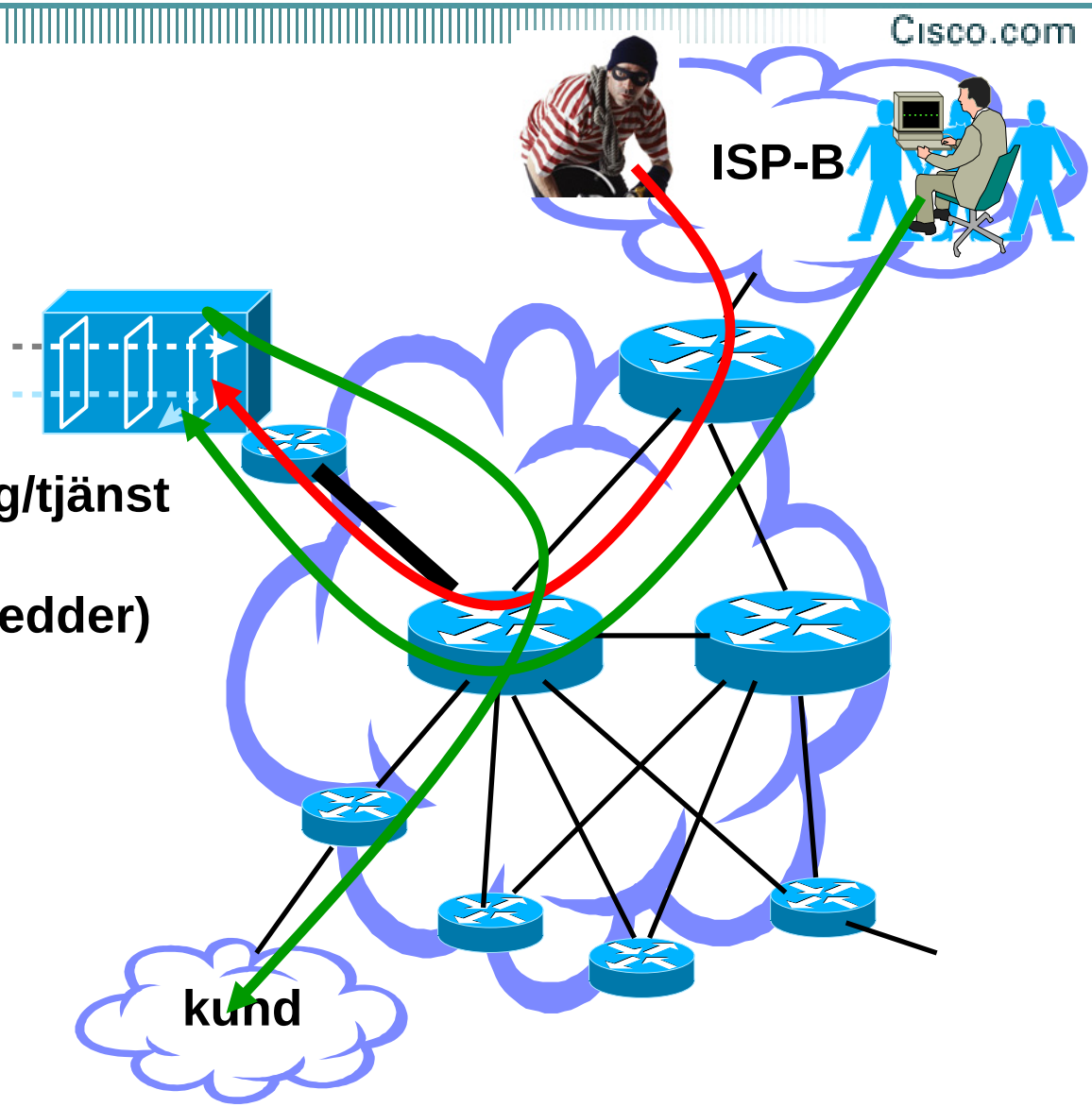


DDOS tvättmaskiner

Avleder trafik till attackerad kund via BGP
Tvätta trafik, filtrera bort DDOS
Legitim trafik skickas vidare
Kunden site stannar uppe !!



DDOS tvättmaskiner(2)



Operatörsplacerad lösning/tjänst
-mest kostnadseffektiv
-bäst skydd (höga bandbredder)

Sammanfattning

Internet blir robust genom operatörers OPSEC team, deras förberedelser, kontakter, processer, policys (och vissa tekniska knep).

Om Internet är viktigt för din organisation, välj en operatör som förstår och satsar på säkerhet