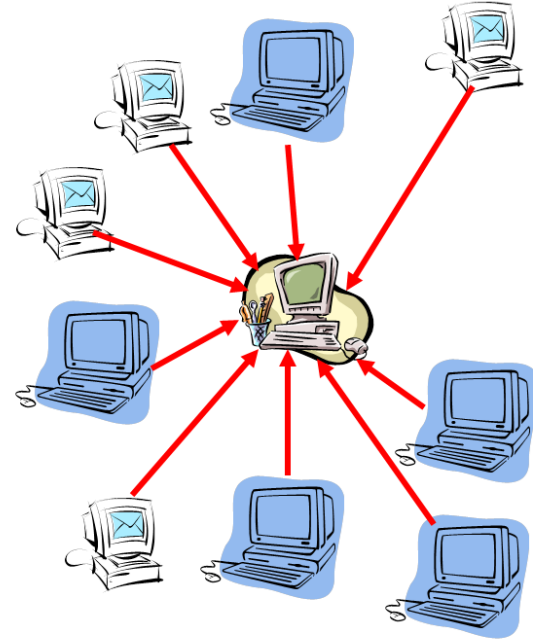


(Distributed) Denial-of-Service Attack

Background & Context:

- typical DoS attack:
 1. select target
 2. break into accounts around the world
 3. have these accounts send packet to target
- common: e.g., *Akamai*, *banks...* (extortion money)
- many other forms of attacks can be reduced to DoS attacks using *crypto*



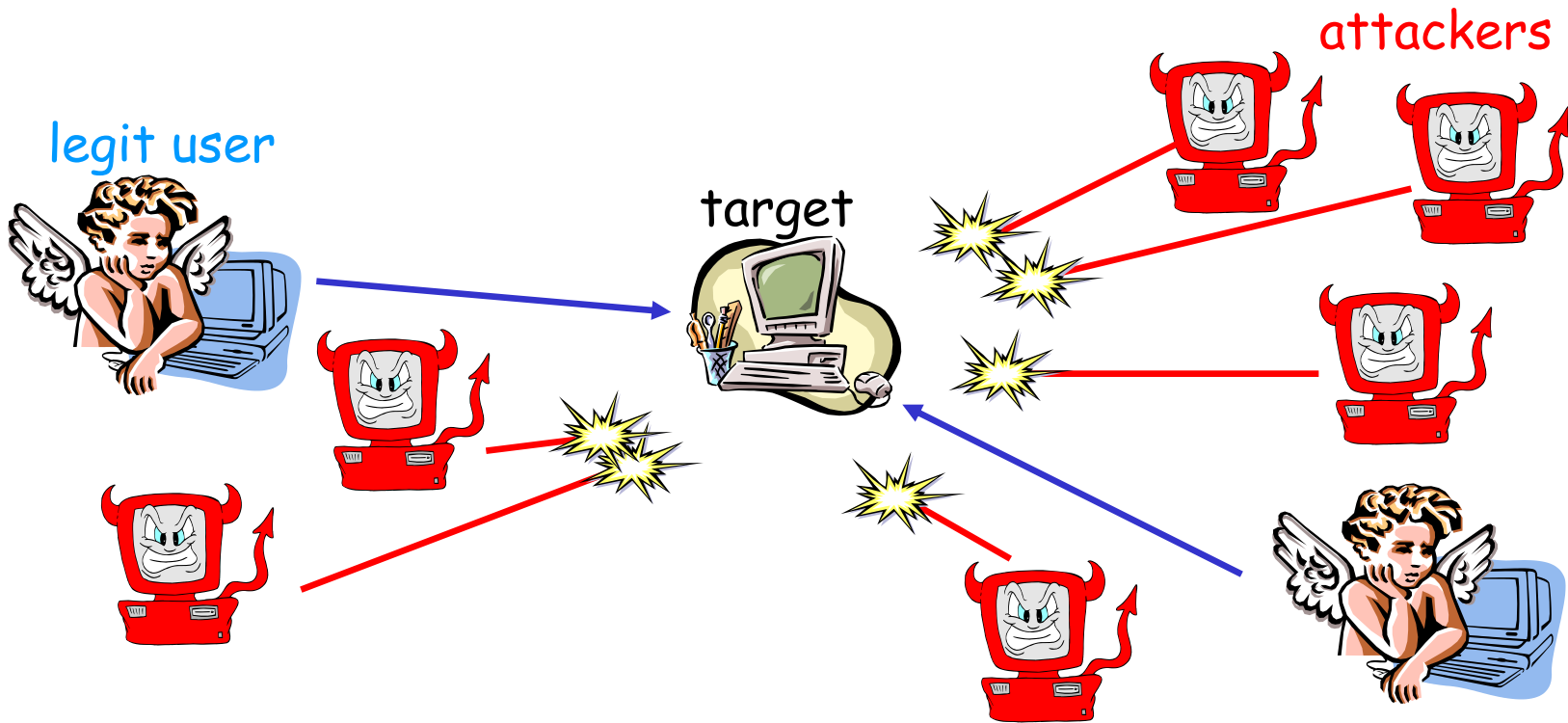
Goal today: **SOS (Secure Overlay Service)**

Published by Keromytis et al. at SIGCOMM 2002

Goal: Keep Service Available

"If you cannot prevent the attack, at least minimize its effects:
Service always **fully available** to *legit* users!"

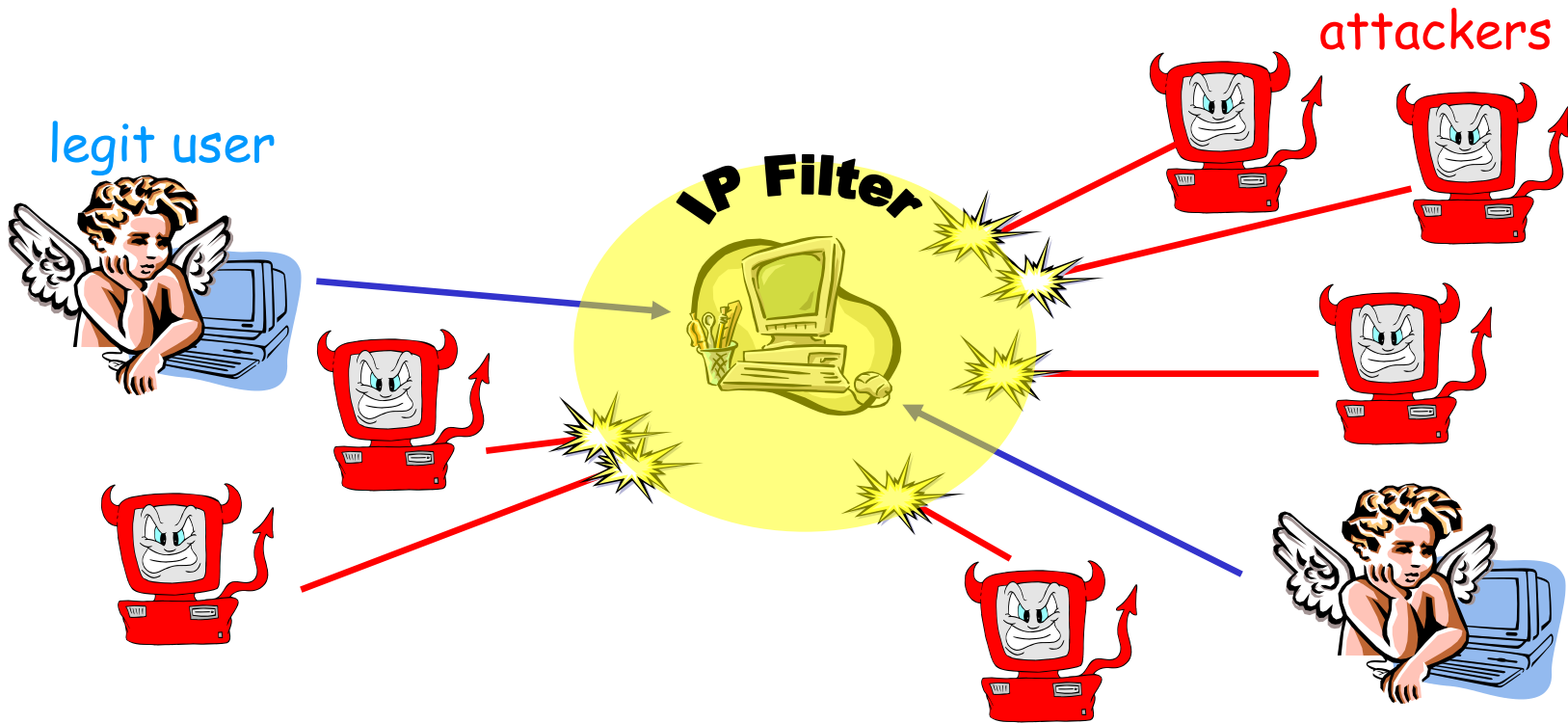
How to achieve?



Goal: Keep Service Available

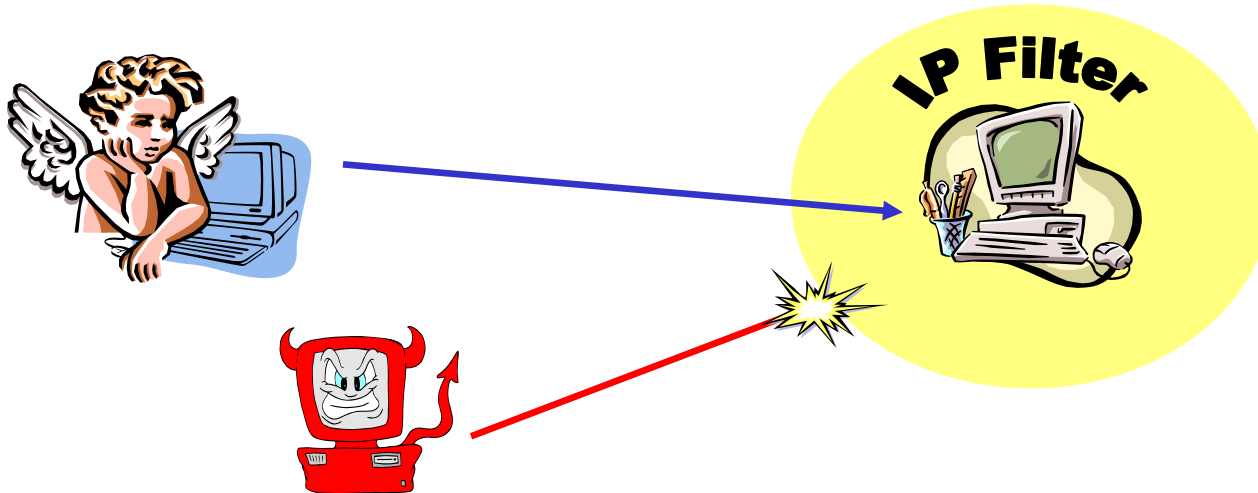
"If you cannot prevent the attack, at least minimize its effects:
Service always fully available to *legit* users!"

How to achieve?



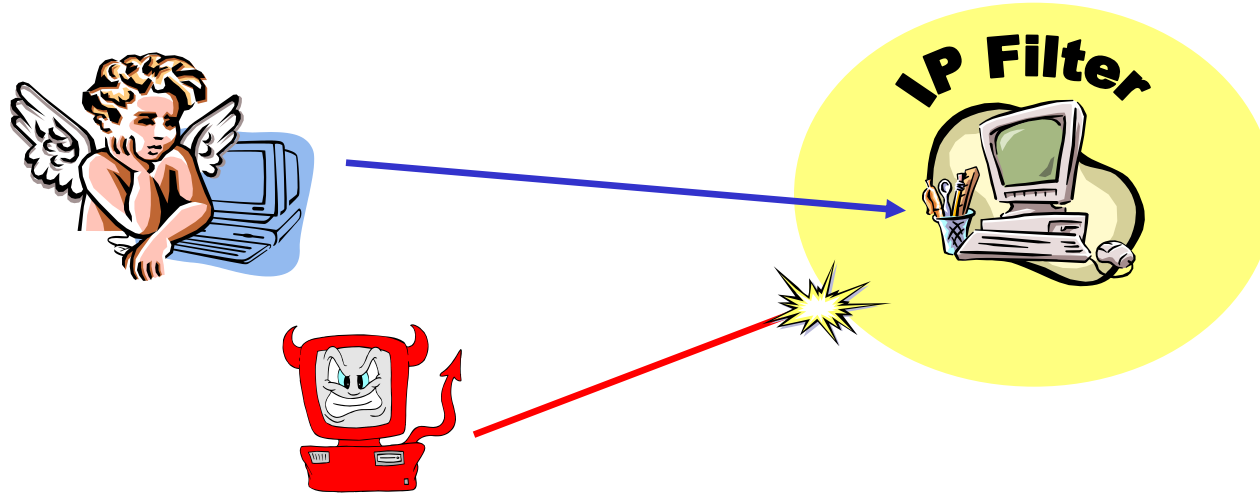
Step 1: IP Filter

- ❑ filter: on *target* itself, last *router* before target, or *separate* machine
- ❑ **classify traffic** in good and bad
- ❑ pre-approved **legitimate users** communicate with **target**
- ❑ un-approved (attackers') packets don't reach target



Advantage and disadvantage?

IP Filter: Discussion



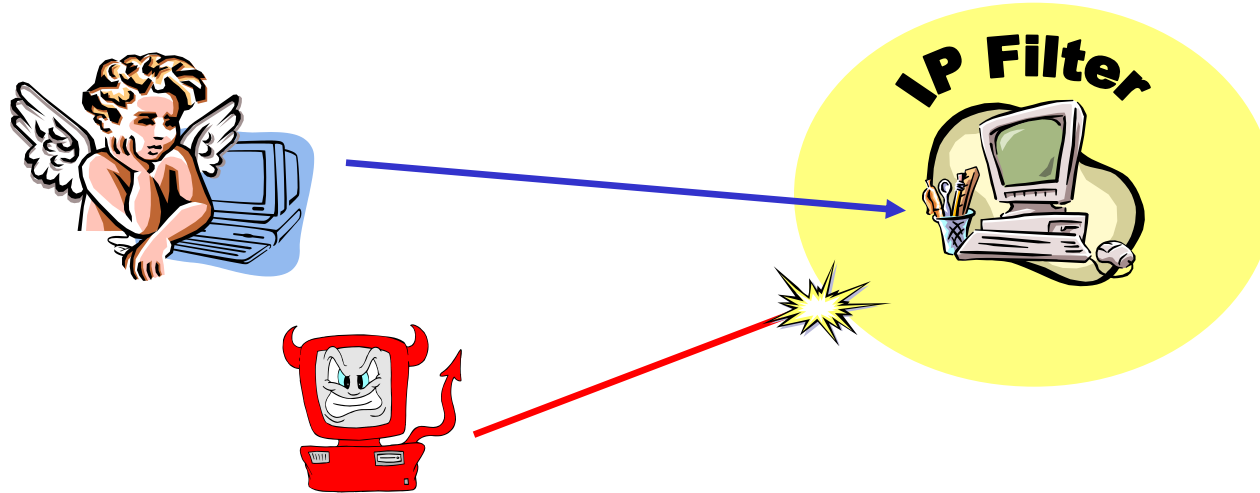
Advantage:

IP based filtering
is **simple & fast!**

Disadvantage:

- Which addresses are good?
- What if addresses change over time?
- Mobility, **dynamic** IP, ...?
- Address **spoofing**?

IP Filter: Discussion



Advantage:

Disadvantage:

IP based filtering

is s

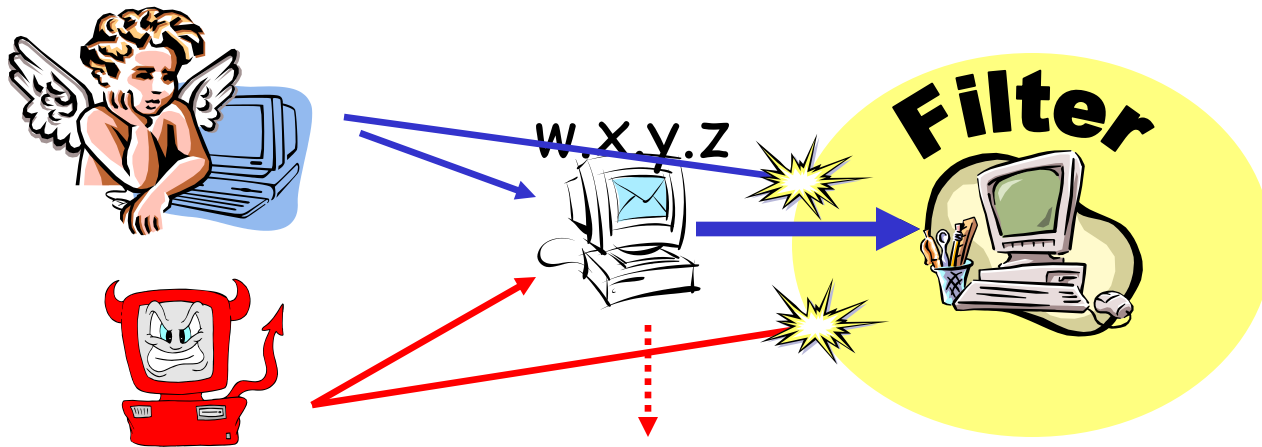
Filtering based on IP (only) not a good idea!
Better authentication scheme?

- Address spoofing? ...

Step 2: Add Indirection via a Proxy

Idea: use proxy (“firewall”), outside filtered region

- ❑ proxy, being a computer (rather than router) can perform **heavy-weight authentication**, access control
- ❑ only packets from proxy permitted through filter
- ❑ proxy only forwards **verified packets** from legitimate sources through filter

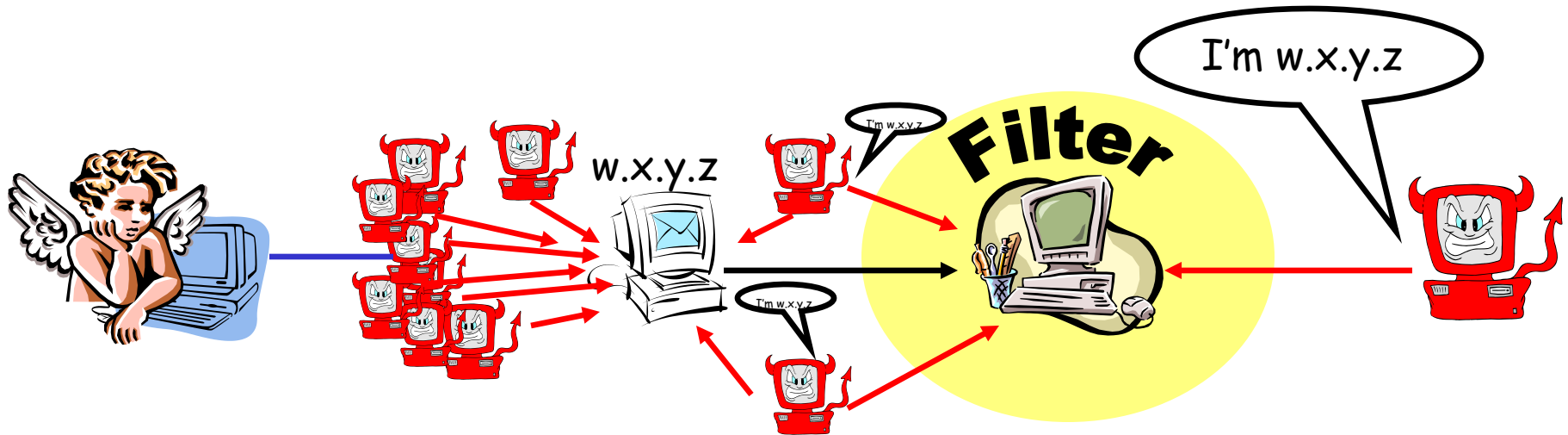


All problems solved?

Problems With a Known Proxy

Proxies introduce other problems:

- ❑ attacker may become proxy (can breach filter by attacking with **spoofed proxy address...**)
- ❑ attacker can **DoS attack proxy** (again preventing legitimate user communication)



Solution? How to make proxy robust?

Step 3: Use Redundant Proxies

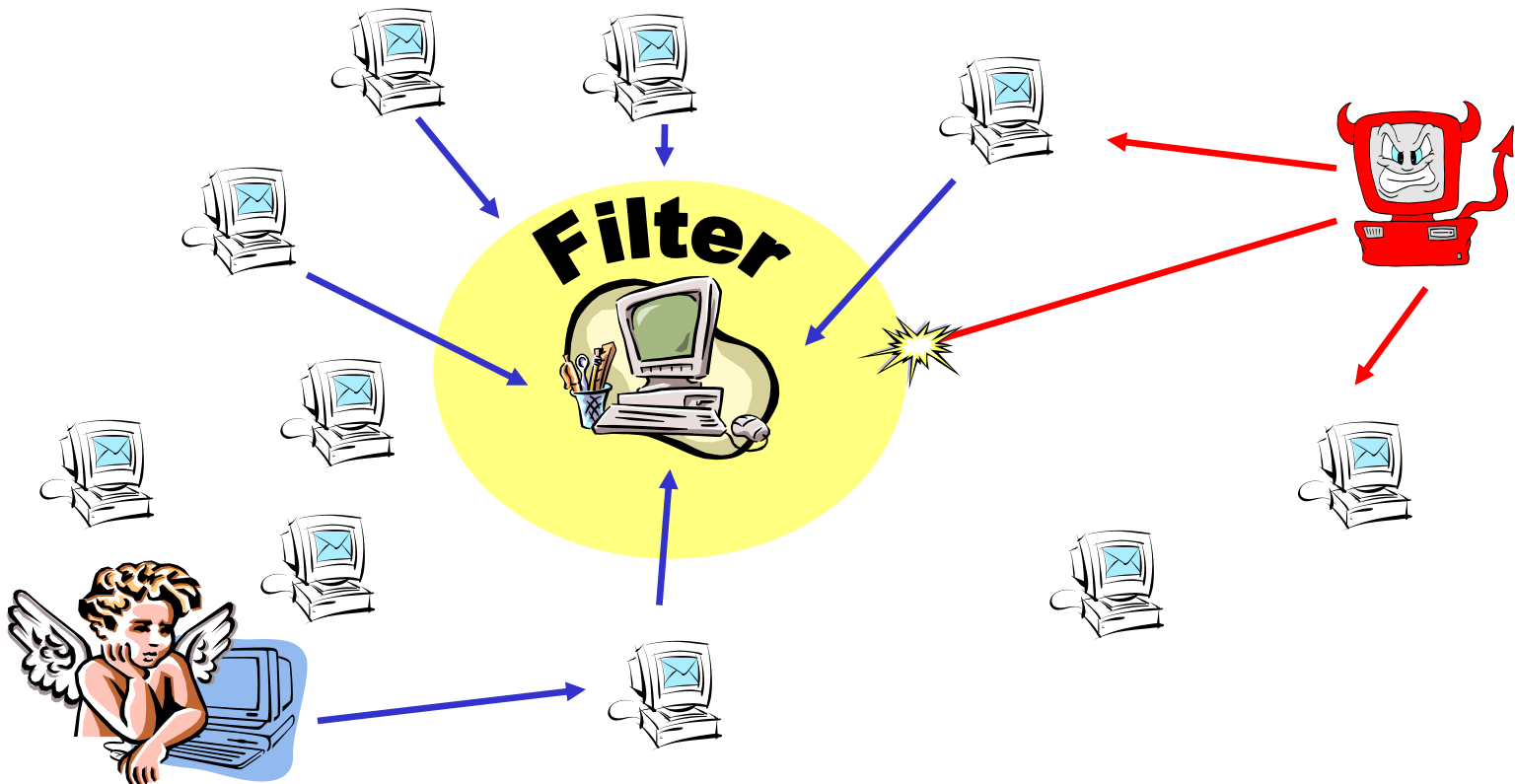
many proxies =
“distributed firewall”

Problems from Step 2:

- ❑ attacker may become proxy ?
- ❑ attacker can DoS attack proxy

But how to prevent
wrong identity?

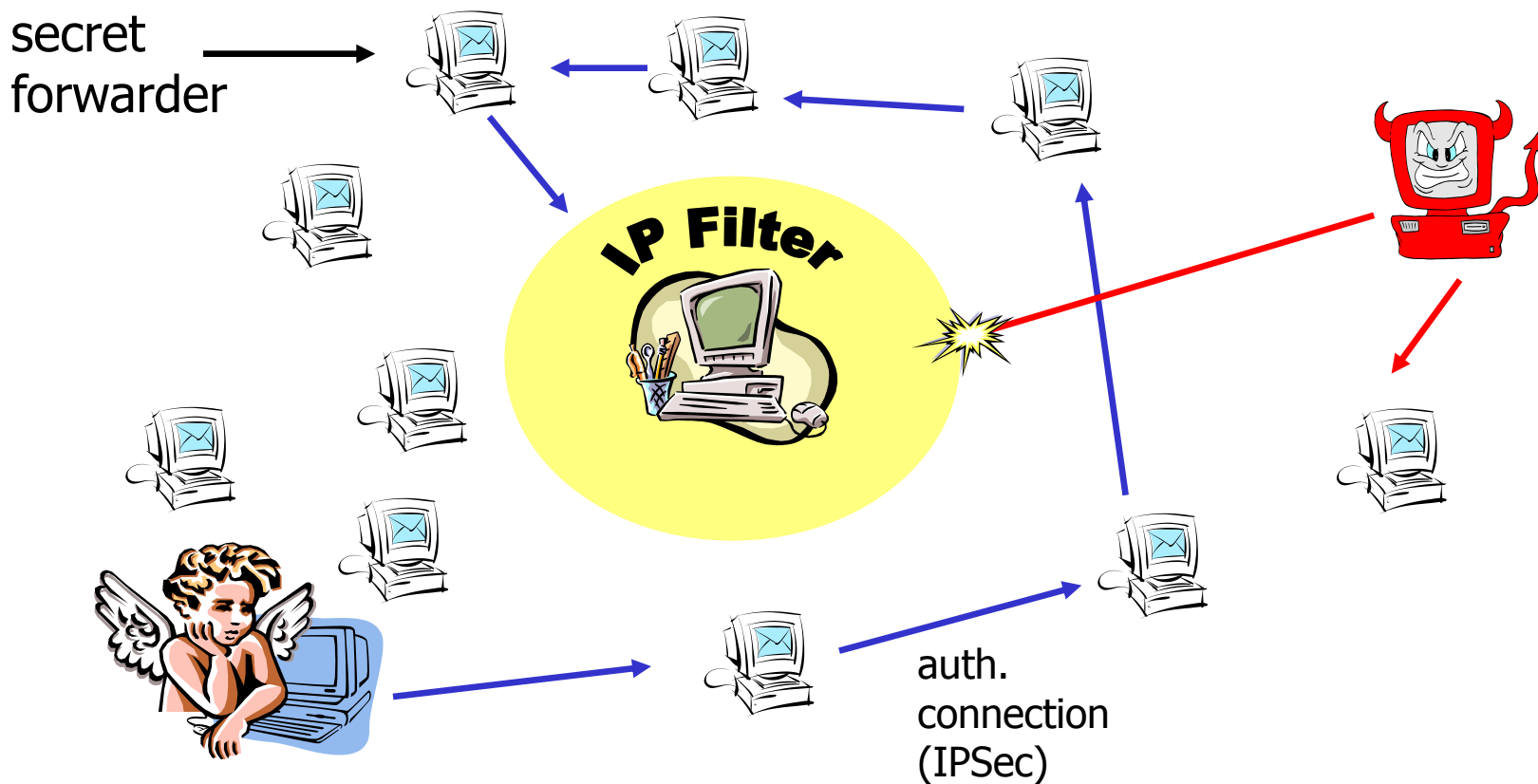
Good! Attacker cannot
take down all proxies!



Step 4: Use Secret Forwarders

Idea:

- ❑ only a **secret subset** of proxies forwards to target
- ❑ proxies forward requests using **random & robust routing** (IPSec)



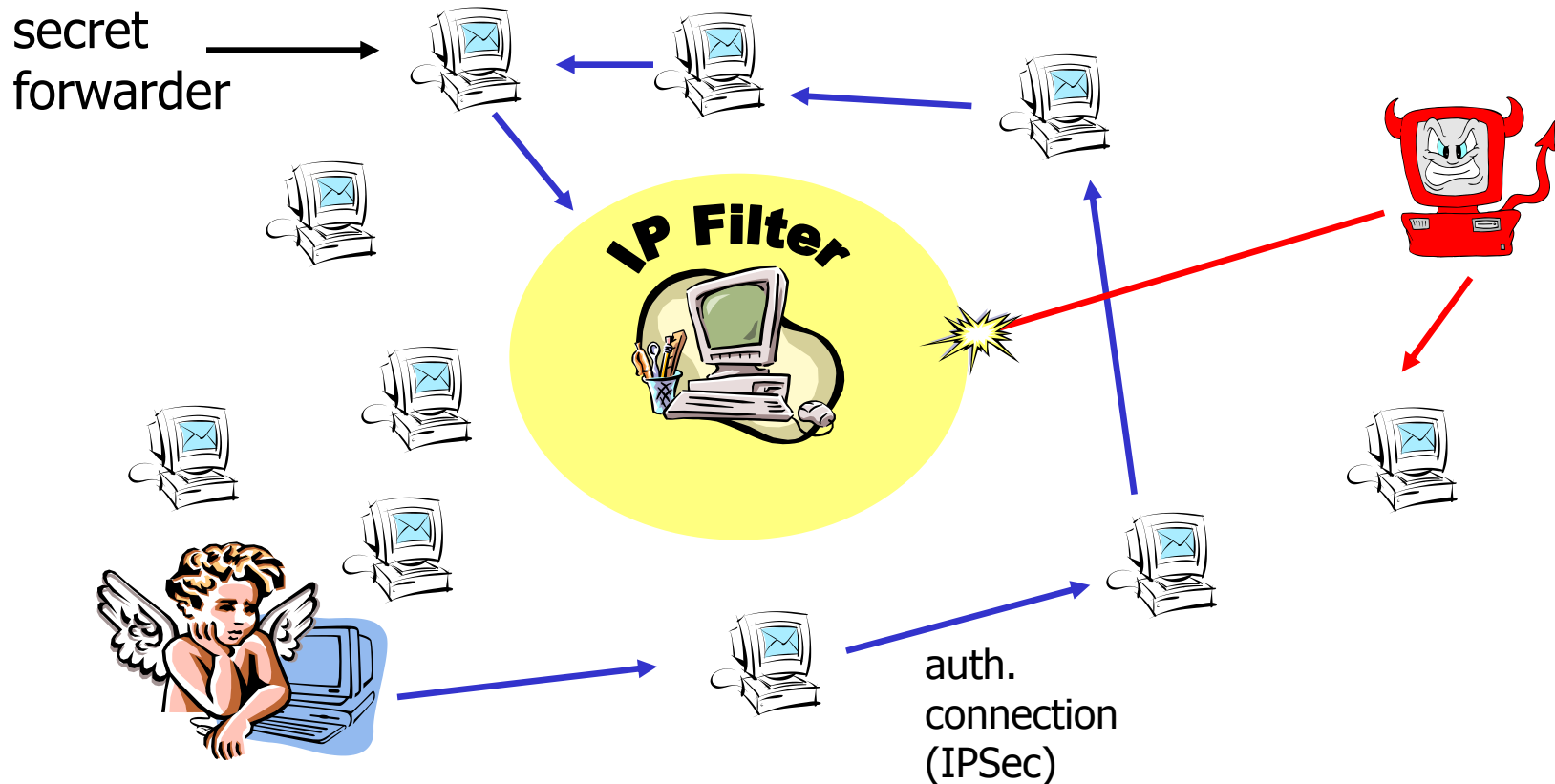
Step 4: Use Secret Forwarders

Problems from Step 2:

- ❑ attacker may become proxy ✓
- ❑ attacker can DoS attack proxy ✓

Good! Attacker cannot become all proxies!

Good! Attacker cannot take down all proxies!



SOS: Discussion

Concepts:

- ❑ many proxies for time-consuming authentication
- ❑ proxies can be replaced, target cannot!
- ❑ fast IP-filtering of proxy IPs only
- ❑ random routing between proxies (authenticated): no spoofing

Issues:

- ❑ How to organize proxies? Robust [peer-to-peer overlay](#)...
- ❑ Idea: put proxy into LAN? All traffic goes to proxy, only from proxy to target! But scalability?
- ❑ Really not possible to attack all proxies: maybe ok
- ❑ But really not possible to [become all proxies](#)? Success observable!
- ❑ What if attacker can make traffic statistics of proxies? Find forwarder?
- ❑ What if attacker can take control over [packet filter / router](#)?