Firewall BOF

“Routing” Issues with WS/SOAP

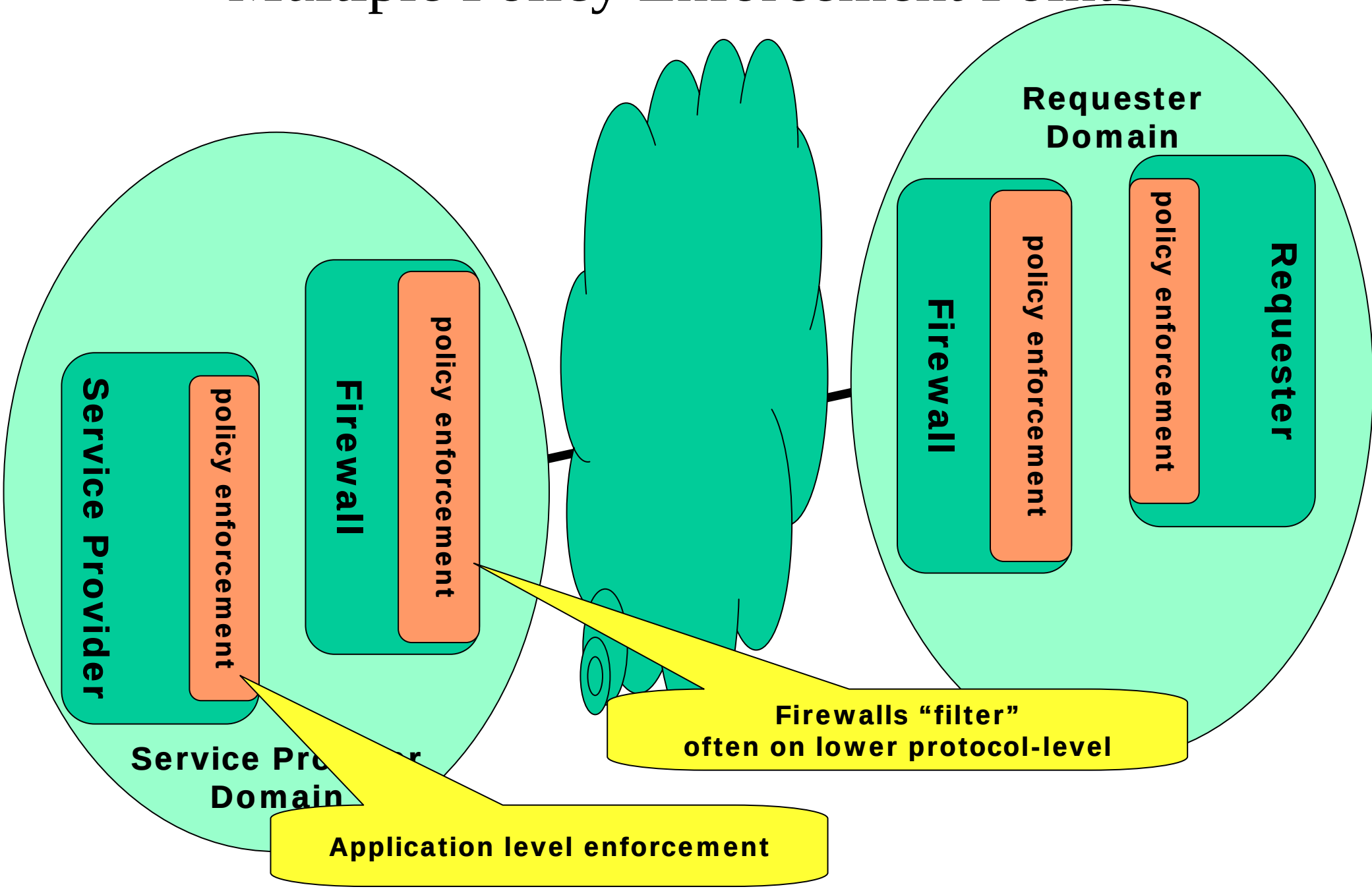
Mar. 14, 2005 (GGF13@Seoul)

Frank Siebenlist, ANL

Multiple Policy Enforcement Points

- Use firewall as course grained filter
  - Front door of apartment building analogy
  - Prevents some bad guys/bots to come through
- Still need for end-to-end policy enforcement
  - Ideally ws-endpoints on firewall and same authN mechanism!
- If firewall and resource policy language are equal, then consistency of policy easier checked
  - Easier to allow connections thru…(?)
- Requester-ServiceProvider context “tunneled” thru intermediates
  - Requester maintains a separate security context with each PEP
- Need for security protocol support, describing allowed routes and ability to express policy per PEP

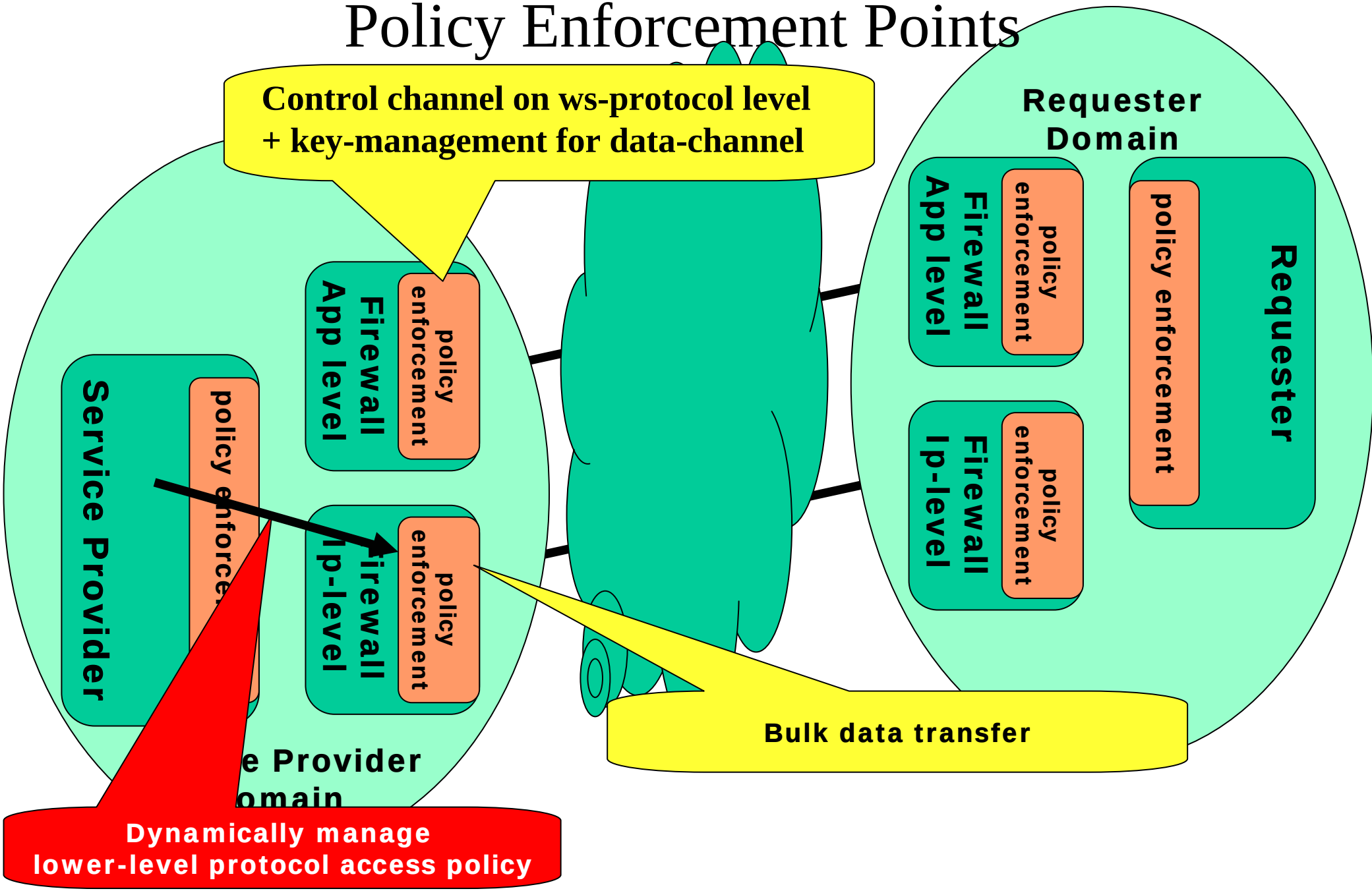
Multiple Policy Enforcement Points



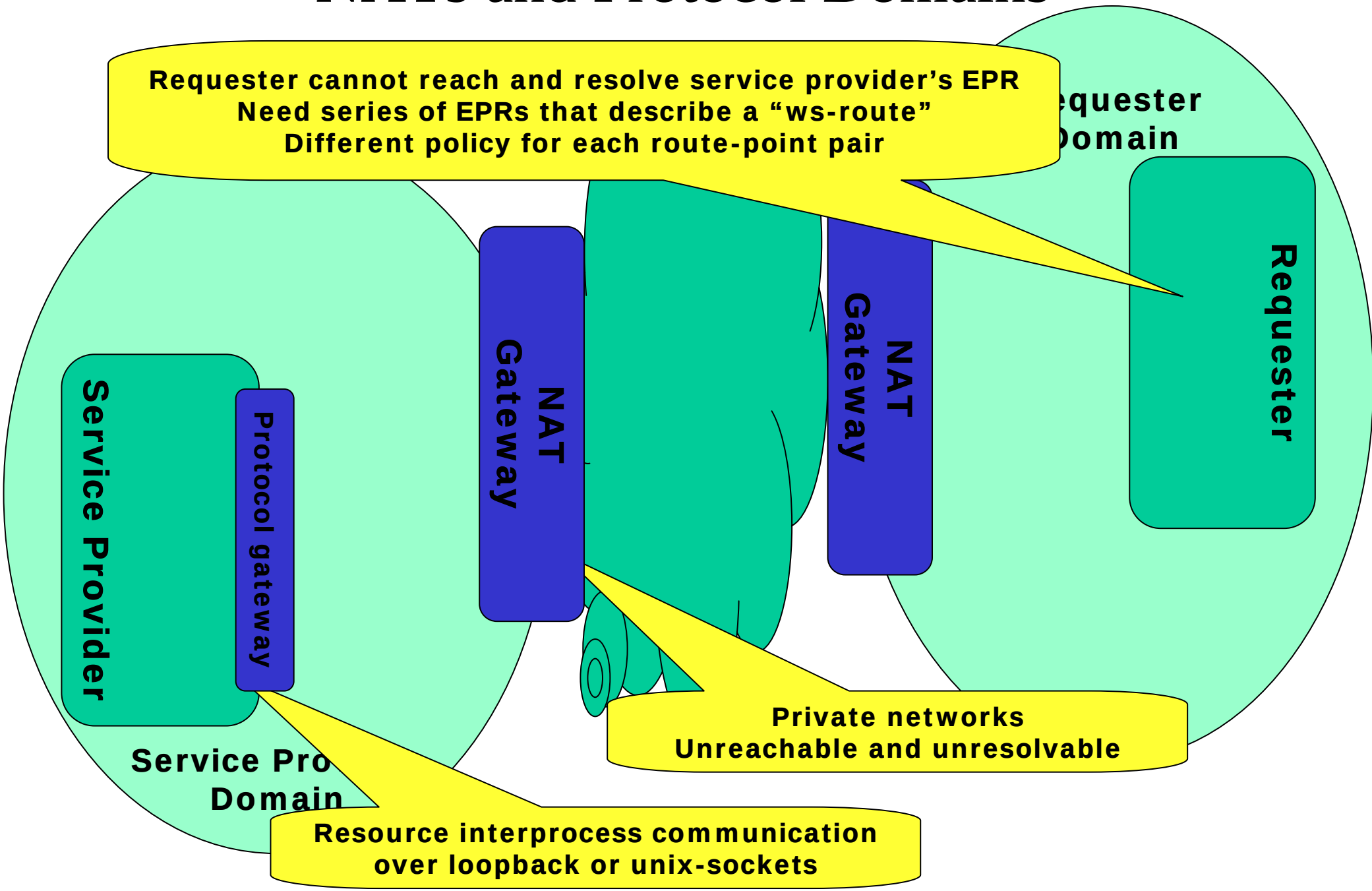
Requirements to blow real holes

- WS-SOAP may not be the “best” and most “efficient” protocol for all applications…
  - …hopefully this sounds cynically enough…
- Bulk data transfers have their own optimized low-level protocols
  - GridFTP, Lambda, SRB, etc.

Multiple Protocol Stack Policy Enforcement Points



NATs and Protocol Domains



Firewall BOF Input

- Need application-level firewall/routers/(reverse-)proxies
- Need Web-Service firewalls/routers
  - Also for NATs…
- Need ability to specify/discover the route
  - EPRs for separate legs
  - Publish and discovery of routes
  - Security context has to be tunneled thru intermediates
- No emerging standards in sight yet…
  - … but “they” must be working on this…
- Unclear whether we/GGF should try to solve this…

….but we can identify and articulate the requirements