the globus alliance
www.globus.org

Authenticating Firewalls

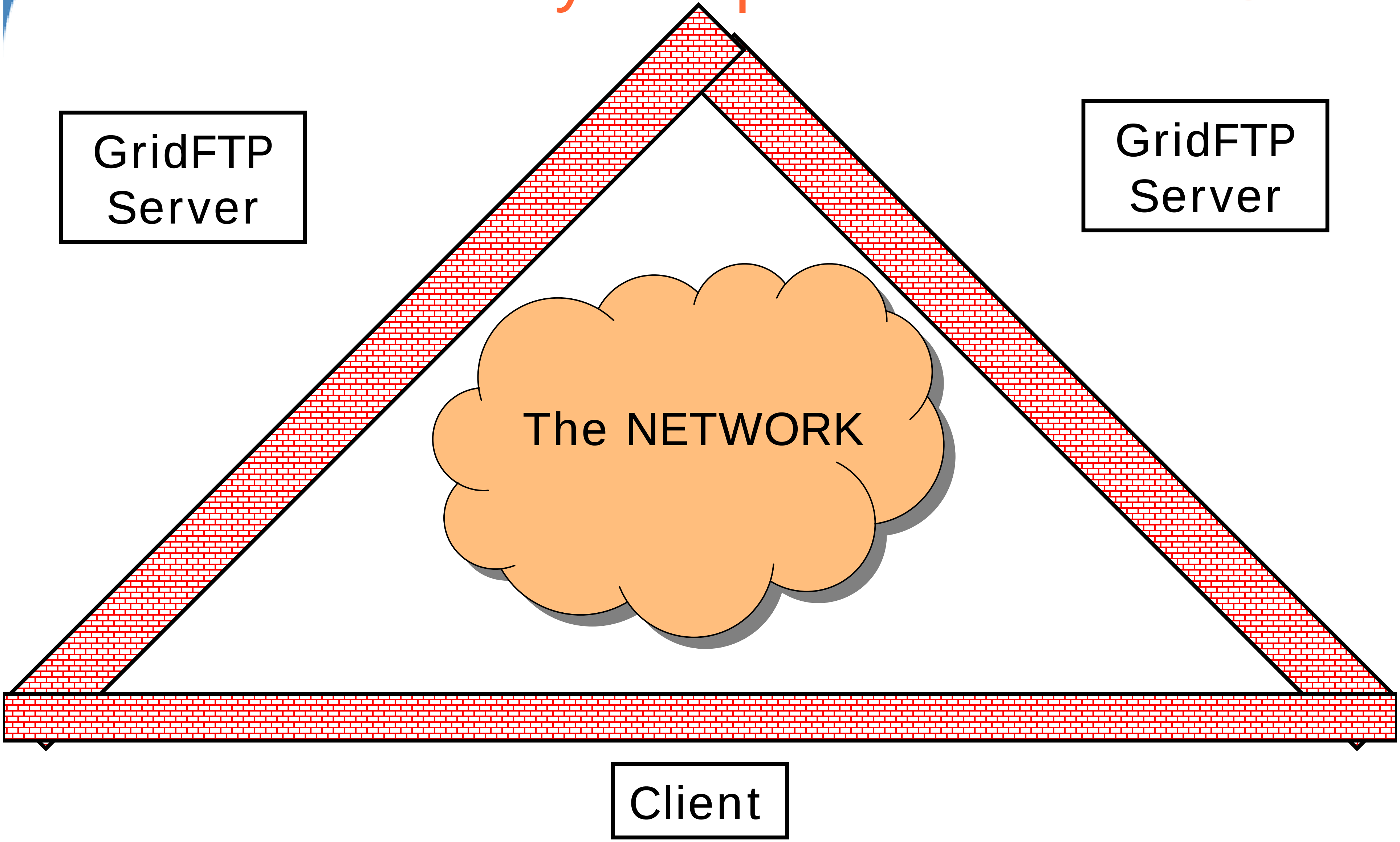
JET Workshop, 13-15 April, 2004

Jefferson Lab

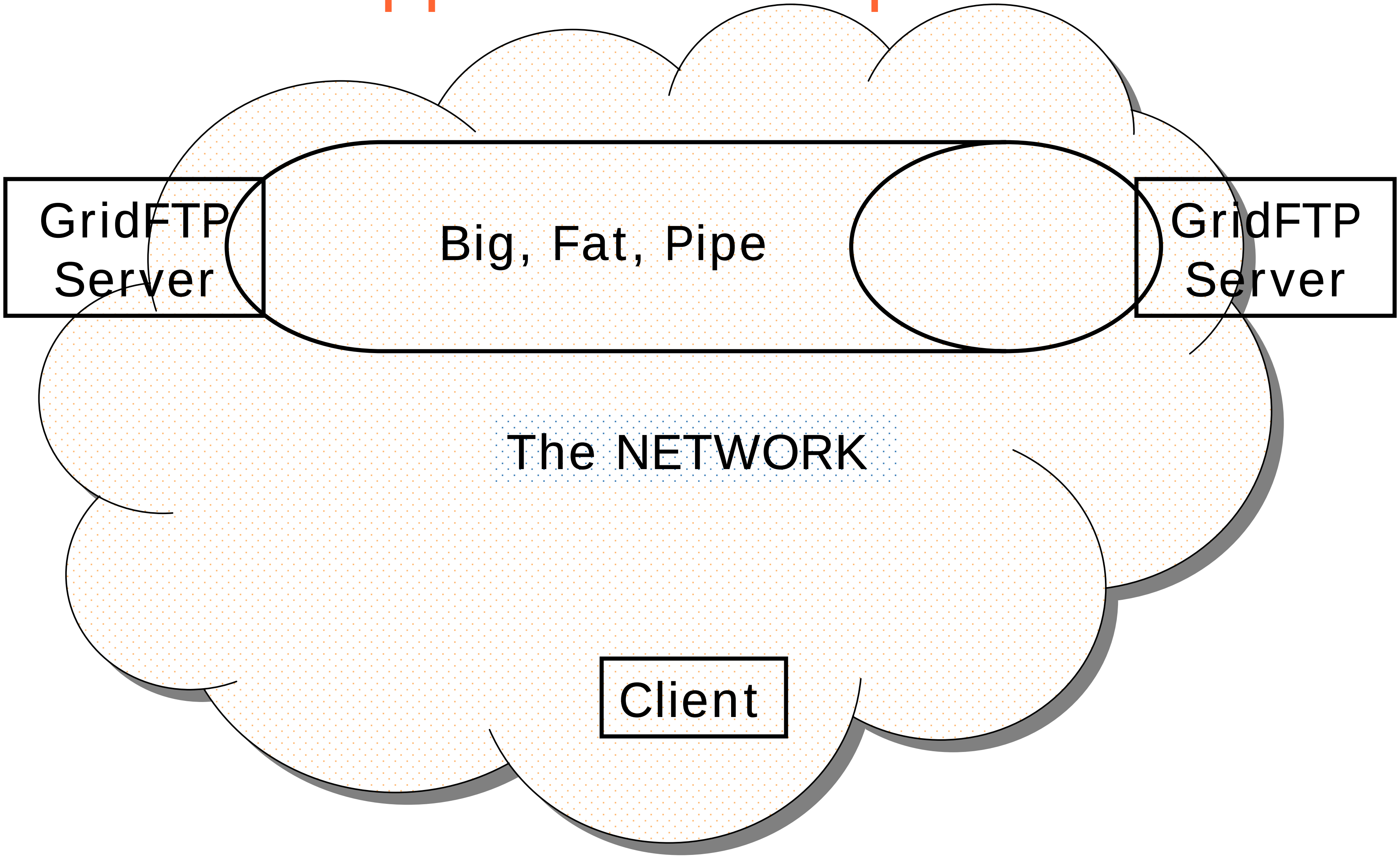
Bill Allcock

Argonne National Laboratory

What Security People Would like ☺



What application People Want ☺



Where are we at today?

- Applications often can’t run, and if they are high bandwidth apps, the firewall often limits performance.
- Today, it means negotiating (arguing, threatening?) with the security people and the admins to open holes, but then they stay open too long, and anyone can exploit them.
- We need something better…

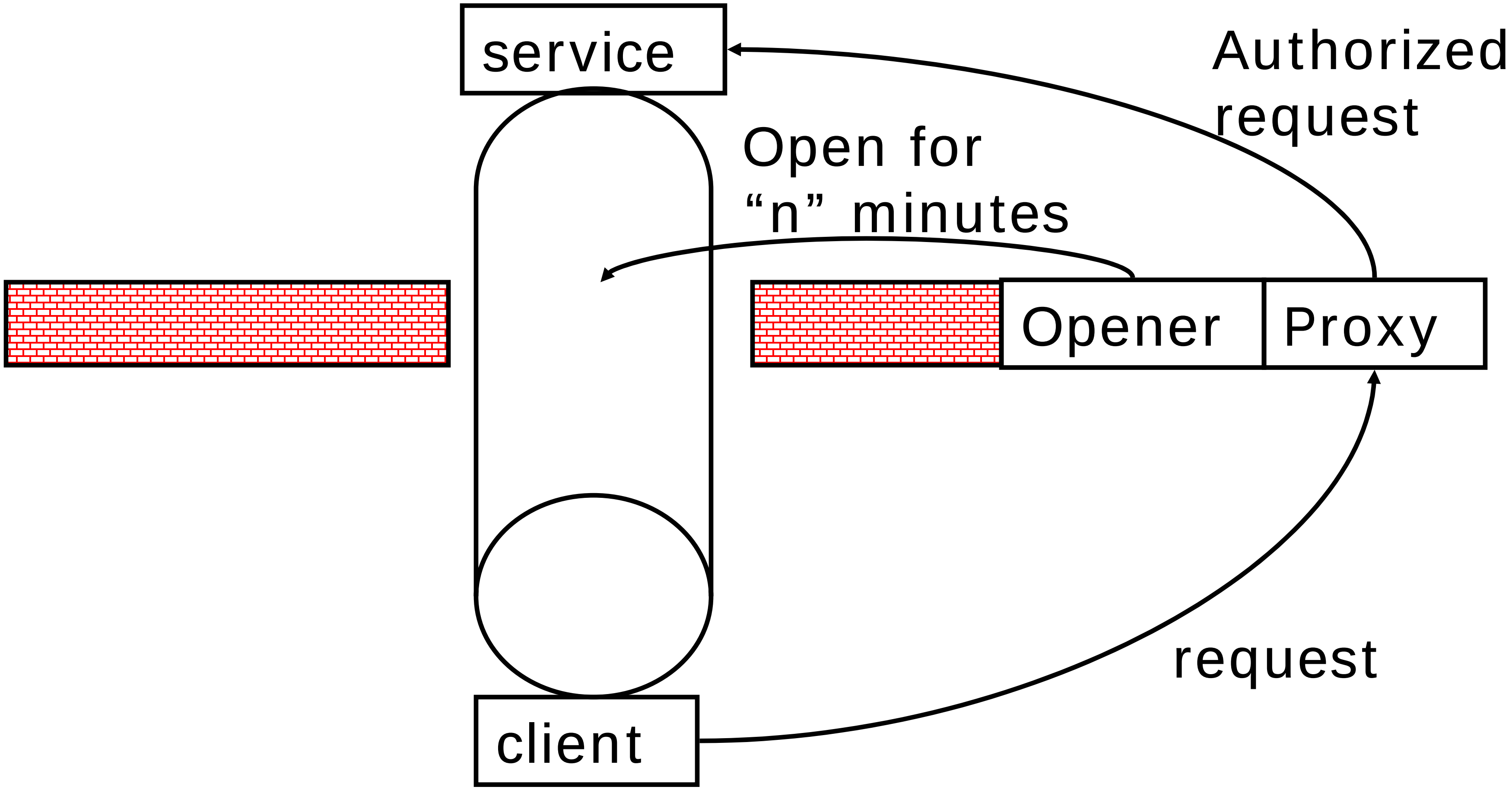
An Idea

- First, this is an idea, and we don’t have all the angles figured out, so please throw stones... well, not really, but you get the idea.
- We need
    - To open holes in the firewall
        - Only when absolutely necessary
        - For a specific party
        - With confidence that the use of that port falls within authorized behavior

How can we do that?

- We envision two services
  - A service proxy
    - Intercepts incoming service requests (SOAP in Web Services)
    - Validates / Authorizes the request
    - Pluggable framework so it can be easily extended
    - Once authorized forwards it to the service
  - A secure, dynamic firewall “automatic garage door opener”
    - Temporarily opens holes through the firewall
    - Uses lifetime management to ensure the holes close
    - Ideally can specify exact host and service that will contact
    - Possibly have no monitoring of packets after that?
    - But could work with IDS, if it were fast enough.
  - Could, in theory, use these separately

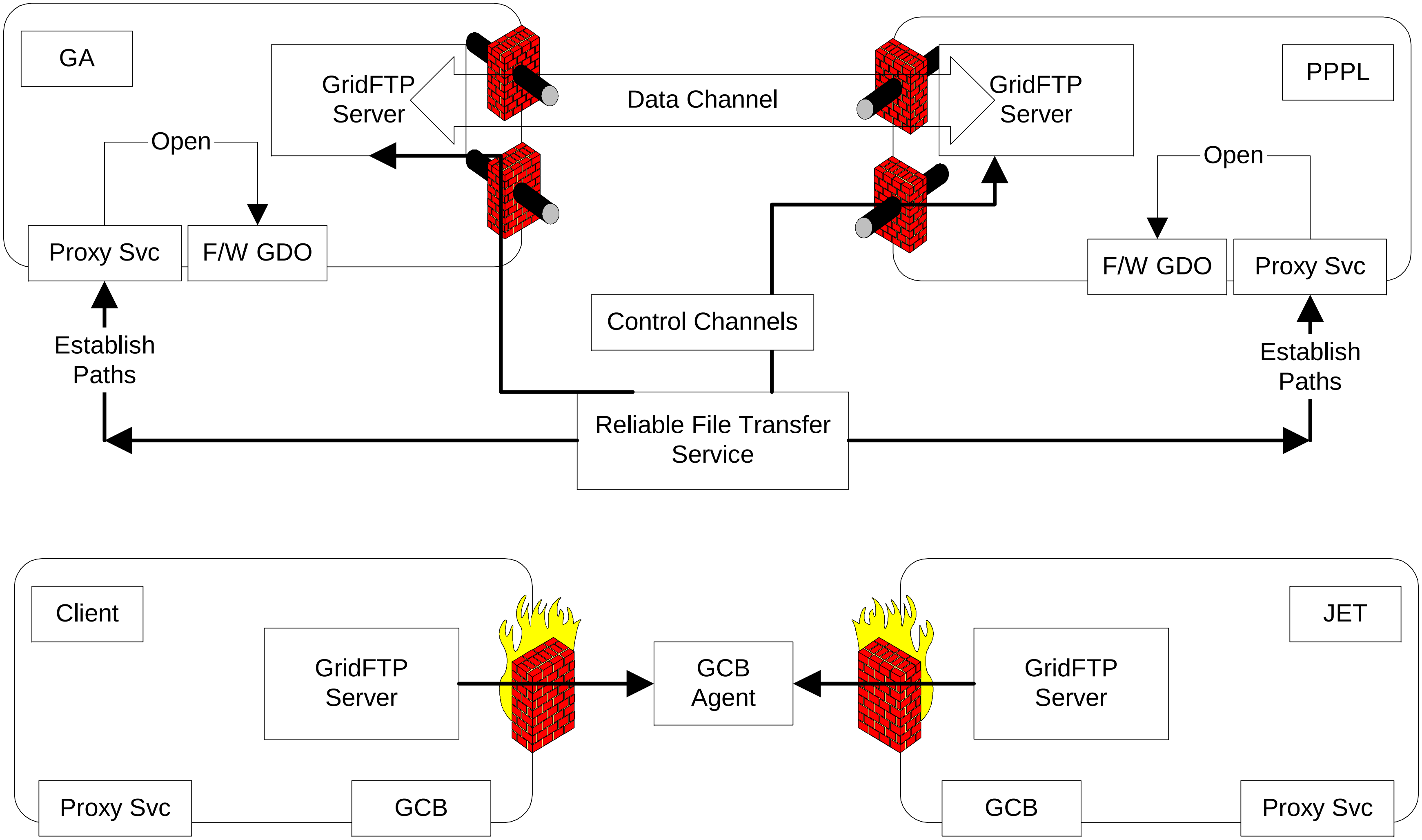
A picture


service
Authorized
request
Open for
“n” minutes
Opener
Proxy
request
client

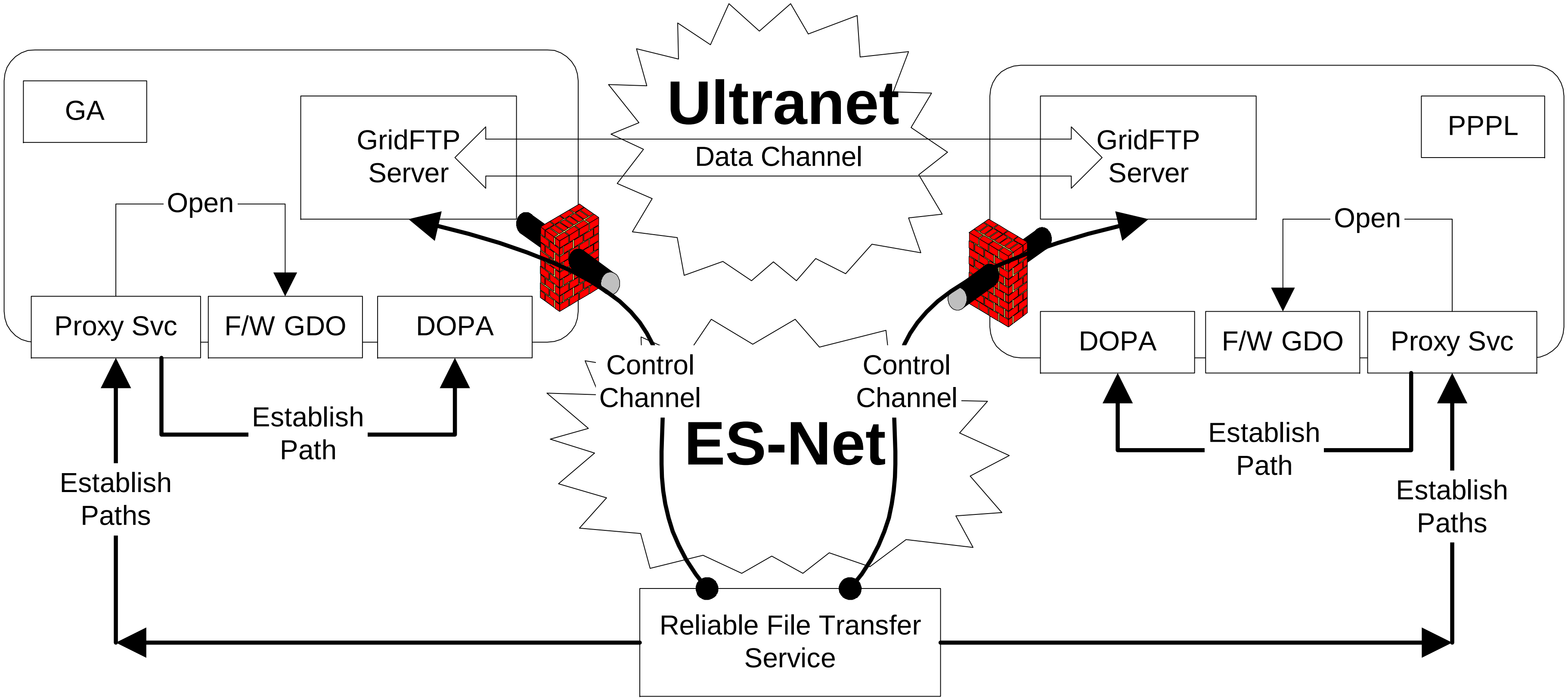
Issues

- You might notice the picture does not show who talks to the opener, this has significant security and effort impacts
  - The Proxy?
  - The Service?
  - The Client?
- Stability / Security of plug-ins
- What about non-SOAP requests?
- Would this be secure enough to let the fat pipe run un-monitored?

Fusion Collaboratory



Even with Optical Paths...


GA
GridFTP Server
Ultranet
Data Channel
GridFTP Server
PPPL
Open
Open
Proxy Svc
F/W GDO
DOPA
DOPA
F/W GDO
Proxy Svc
Control Channel
Control Channel
ES-Net
Establish Path
Establish Path
Establish Paths
Establish Paths
Reliable File Transfer Service