“The software formerly known as the Site Proxy”

Oscar Koeroo
JRA3

Content

- What's the problem?
- What do we need?
- How do we want to solve it
- Our prototype
  - and how does it work

What's the problem?

- **Most to all WNs (in LCG-2) can make outbound connection to almost any machine on the Internet**
  - No Firewalls that limits a user
    - A few possibilities are:
      - *WN publicly addressable*
      - *Inbound is prohibited and outbound is still free to use*
        - NAT box
        - Firewall rules
      - *WNs are locked up for any Internet traffic*
  - VOs request ability for their users to connect to there own servers
    - Pulling VO specific data on a WN
      - *Packages*
      - *Data*
    - Push result on to VO specific machines
    - Interactive
      - *Database access*

- **This means that every (rogue) user can do harmful things like:**
  - Launch DDoS - Grid Jobs can aid or start a DDoS on a (web-)server
  - Share Warez - Compromised machines can serve as Warez servers
  - Make a pass-through for Worms & Viruses

What we need…

- **Network containment**
  - We need to keep a user primarily in the fabric
  - If users have a connectivity wish they can request it at the (concerning) resource centers
  - RCs need to be in full control of their (network) domain

How do we want to solve it

- **Lockup a site tight**
  - Let the Grid services be connectable and let them connect to others
  - Grid services mutual authenticate themselves to other services with some kind of access control so they can be regarded as safe(r) connections
  - For the WNs and the jobs:
    - No (direct) inbound connectivity
      - *Achieved by setting up a router, NAT box or Firewall (or some combination) prohibiting these connections*
    - No outbound connectivity
      - *The router, NAT box or firewall (or a combi.) prohibit these connections*

- **Only when needed open-up a port to make a (controlled) connection available**

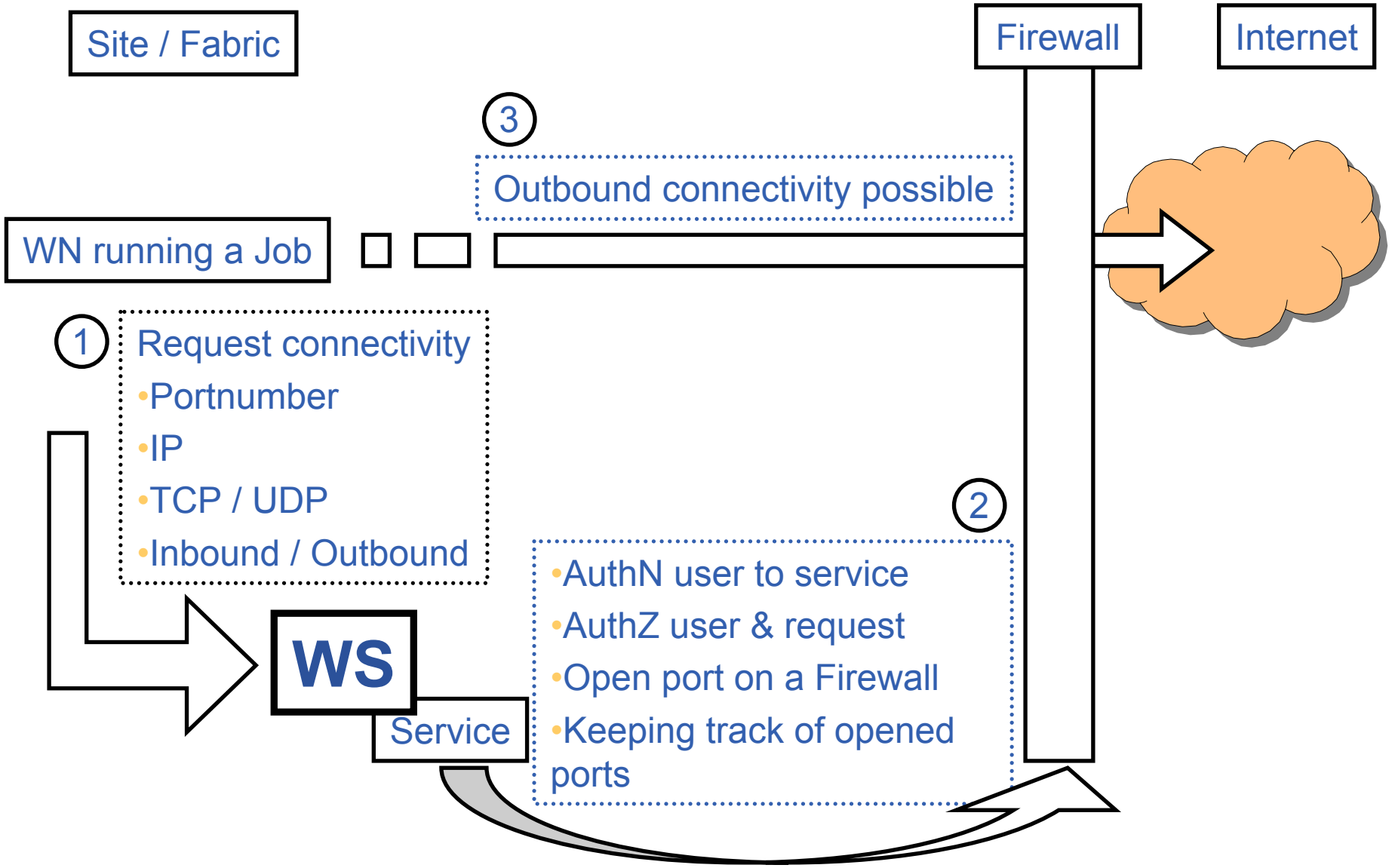
The prototype called: “Lasa”

- **“Proxy” has a (overloaded) meaning in:**
  - The database world
    - *A kind of cache for queries*
  - The networking world
    - *HTTP*
    - *FTP*
  - The security world
    - *X509 – RFC 3820*
    - *Radius*

- **Can we throw ‘Site Proxy’ to /dev/null and use ‘Dynamic Connectivity Service’ ?**

- **The name of the prototype will be ‘Lasa’**

How does it work



Present & Future

- **Current prototype implementation (Nov 2004)**
  - Design finished
  - No AuthN and AuthZ security elements
  - Only portnumber requests
  - Current supported setup:
    - NAT box with IPTables
- **Future**
  - AuthN & AuthZ
  - Fine & coarse grained connectivity policy description
  - Connectivity can be requested on DNS
  - Support for other setups:
    - Telnet/SNMP controlled routers
    - Different firewalls