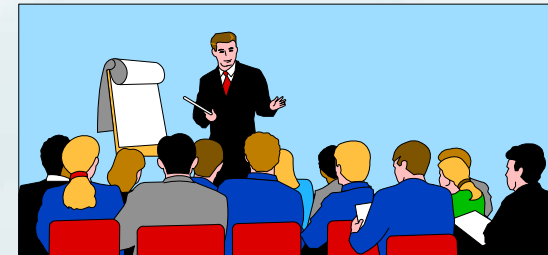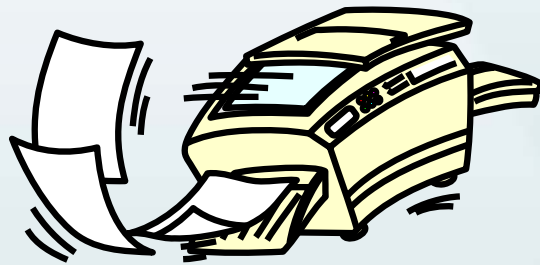# Firewall Issues Overview

Document update V2.06 and discussion

R.Niederberger@fz-juelich.de

Overview

- **Structure of current document
  Firewall Issues Overview - Vers.2.06**
- **Next steps**
- **Questions and discussion**

Document structure

- **Introduction**
- **Definitions**
- **Grid applications and their issues with firewalls**
- **Classification of firewall issues**
- **Future Directions**
- **Summary**
- **Appendix: Classification of firewall issues seen from the use cases side**

document structure(2)
Definitions

Definitions

- Firewall
- Classification of firewalls
    - network layer firewalls
    - application layer firewalls
    - application firewalls
    - stateful/stateless firewalls
- Firewall (global definition)
- Network Address translators
- Application level gateways
- VPN gateways

New structure of …

GRID APPLICATIONS AND THEIR ISSUES WITH FIREWALLS

- **Grid Middleware and Protocols**
  - Globus
  - UNICORE - The Seamless GRID Solution
  - Webservices Firewall Issues
- **Data Transfer and Storage**
  - GridFTP versus the Firewall
  - Impact of dCache deployment
  - Issues in enabling GPFS
- **Grid Network Architectures and Protocols** →**System Deployment**
  - The Issue with "Net of Trust" or the "bastion hosts" solution
  - The workflow management system TENT
  - **AccessGrid**
  - Firewalls and high bandwidth, long distance networks

Selection of applications

- Selection of some commonly deployed grid applications
- Description of issues applications face dealing with firewalls.
- No intention to include all possible application used in grid environments
- just to identify and describe a set of representative examples.
- Classification according to their communication behavior
- Leads to good description of the problems arising because of the existence of firewalls within the communication paths.

New structure of classification

Classification of Firewall issues by the fact that, …

- **The application is unaware of the network**
  - **Software (e.g. app does not know ports to use in advance)**
  - **Hardware (e.g. app does not know about FWs or # of FWs)**
  - **Network (e.g. app does not known location of partner (int, ext, DMZ))**
  - **Security policy (e.g. app does not provide enough info)**
- **The network is unaware of the application, which uses …**
  - **well known ports**
  - **Detectable dynamic data transfer ports**
  - **Obscured dynamic data transfer ports**
  - **Arbitrarily dynamic data transfer ports**

Next steps

- Get document public ➔ Time horizon: GGF18 √ **(done)**

  - End of Public Comments ➔ Oct 8th, 2006

- Improve current draft document ➔ any longer

- Add missing parts ➔ Are their any?

- Start a new document dealing with solutions
  ➔ Already started, we will hear later

!! Get involved !!

Questions and discussion

Questions
and
discussion