Firewall Issues Overview

-

Document update and discussion

R.Niederberger@fz-juelich.de

14.02.2006

Overview

- Structure of current document
- Classification of uses cases; some examples seen from application point of view
- Classification of use cases seen from a firewall perspective
- Next steps
- Questions and discussion

r.niederberger@fz-juelich.de

Structure of the document

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

INTRODUCTION
DEFINITIONS
- Firewall / Classification of firewalls / Firewall (global definition)
- Network Address translators
- Application level gateways
- VPN gateways

GRID APPLICATIONS AND THEIR ISSUES WITH FIREWALLS
- **Grid and Application Technology Deployments**
  - The Issue with “Net of Trust” or the “bastion hosts” solution
  - Impact of DCache deployment
  - Issues in enabling General Parallel File System
  - The workflow management system TENT
- **Grid Network Architectures and Protocols**
  - GridFTP versus the Firewall
  - UNICORE - The Seamless GRID Solution
  - Webservices Firewall Issues
  - Firewalls and high bandwidth, long distance networks

CLASSIFICATION OF FIREWALL ISSUES
SUMMARY
APPENDIX: CLASSIFICATION OF FIREWALL ISSUES SEEN FROM THE USE CASES SIDE

r.niederberger@fz-juelich.de

Classification of GPFS

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Name	GPFS				
Description	The General Parallel File System is a high-performance shared-disk file system. It provides fast, reliable data from all nodes in a homogenous or heterogeneous cluster running an AIX or LINUX operating system. GPFS allows parallel applications simultaneous access to one file or a set of files from any node that has the GPFS file system mounted using parallel streams for a single file transfer.				
Elements in communication path	**Software**		**Hardware**	**Network**	**Security Policy**
Severity	Low		Low	Low	Middle
Occurrence	NA		NA	NA	Management
Any kind of firewalls between the communicating entities.	**Own Software**	No. Software developed by IBM.	No hardware restrictions.	Communication is done via normal communication paths. (Site network – provider network – site network).	Protocol uses fixed configurable TCP port. Disadvantage: Communication including data is unencrypted.
	Ports used	GPFS TCP 1191. *Port is configurable*			
	Protocol used	*TCP*			

r.niederberger@fz-juelich.de

Classification of high bandwidth, long distance interconnects

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Name	Firewalls and high bandwidth, long distance networks				
Description	This use-case describes a setup that allows the creation of (optical) by-pass connections that span long distances which need to be connected via a FW				
Elements in comm path	**Software**		**Hardware**	**Network**	**Security Policy**
Severity	Low		High	Middle	High
Occurrence	NA		Performance	Management	Management
Enterprise and public firewalls at both ends of a connection. Enterprise firewall both connects to the DMZ and to an optical by-pass connection.	**Own SW**	Yes and No GridFTP or any other data mover may be used – requirements are independent	Switching performance and buffer space is critical for the enterprise side of the firewall. Buffers should be able to contain the bandwidth / delay product of a long haul connection. Performance should be in the multi-Gb/s range.	Enterprise firewall may be involved in driving the request of a by-pass connections when detecting private address space ARP requests or handling application specific signals using some protocol	1. Requests from an application to access the optical by-pass should be authorized. The firewall should call out to obtain such authorizations or be provisioned with information that recognises an access request. 2. Security policies should prevent hi-bandwidth / non TCP transmission protocol conformant traffic to be leaked into the regular Internet.
	Ports used	*Globus port range or others*			
	Proto-col used	*TCP and UDP in various flavours*			

r.niederberger@fz-juelich.de

Classification of firewall issues

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

- applications which use special single well known ports
- applications which use control streams to signalize the communication behavior
- applications with control stream for exchanging of control information. But not all info available
- Applications with unknown behavior (e.g. dynamic ports, multiple streams)
- applications which need high throughput data pipes

r.niederberger@fz-juelich.de

Firewall issues on applications seen from software perspective

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Software:

- Port numbers and amount of ports are unknown until the application starts
- Consequence: big holes (many ports) are required if amount and/or port numbers are unknown, single hole case (e.g. HTTP port 80) causes referral problems.
- Only specific, predetermined applications that use a low number
- only very well defined ports (well known ports) can be supported adequately.

r.niederberger@fz-juelich.de

Firewall issues on hardware

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Hardware:

- unknown number and kind of firewalls are located within the routing path
- High performance data streams across long connections need enough buffer space and switching capacity
- Firewalls which are able to deal with multiple wavelengths on a single fiber not developed until now.
- If these wavelengths have been divided into individual fibers by DWDM equipment, firewalls are not able to deal with 16, 32 or 64 links of 10 Gb/s each currently

r.niederberger@fz-juelich.de

Firewall issues on the network

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Network:

- Grid hardware resources running certain applications can not be placed inside the DMZ.
- Sometimes applications must past more than 2 DMZs.
- But putting Grid applications inside the DMZ may not be avoidable sometimes.
- Firewalls, when involved in bypass connections must perform elaborate routing functions

r.niederberger@fz-juelich.de

Firewall issues on Security Policies

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Security Policy:

- Firewalls may not be aware how many different applications may use the same port.
- Firewalls may not be aware of the amount of ports that are actually required v.s. configured.
- Firewalls may need to open up to 10.000 ports for certain applications
- Firewalls may not have enough information to authorize complex grid applications.
- Firewalls must not only protect from evil from the public network, but also prevent the public network from being abused.
- Firewalls may not be able to extend the security context between two applications.
- Firewalls may not be aware if a hosts connecting is actually trusted.

r.niederberger@fz-juelich.de

Next steps

- Improve current draft document
- Add missing parts
- Get document public
- Start a new document dealing with solutions

!! Get involved !!

r.niederberger@fz-juelich.de

Questions and discussion

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Questions / discussion

r.niederberger@fz-juelich.de