Deployment of firewalls at Resource Providers: status and future directions

Gian Luca Volpato
RRZN - Leibniz Universität Hannover
volpato@rrzn.uni-hannover.de

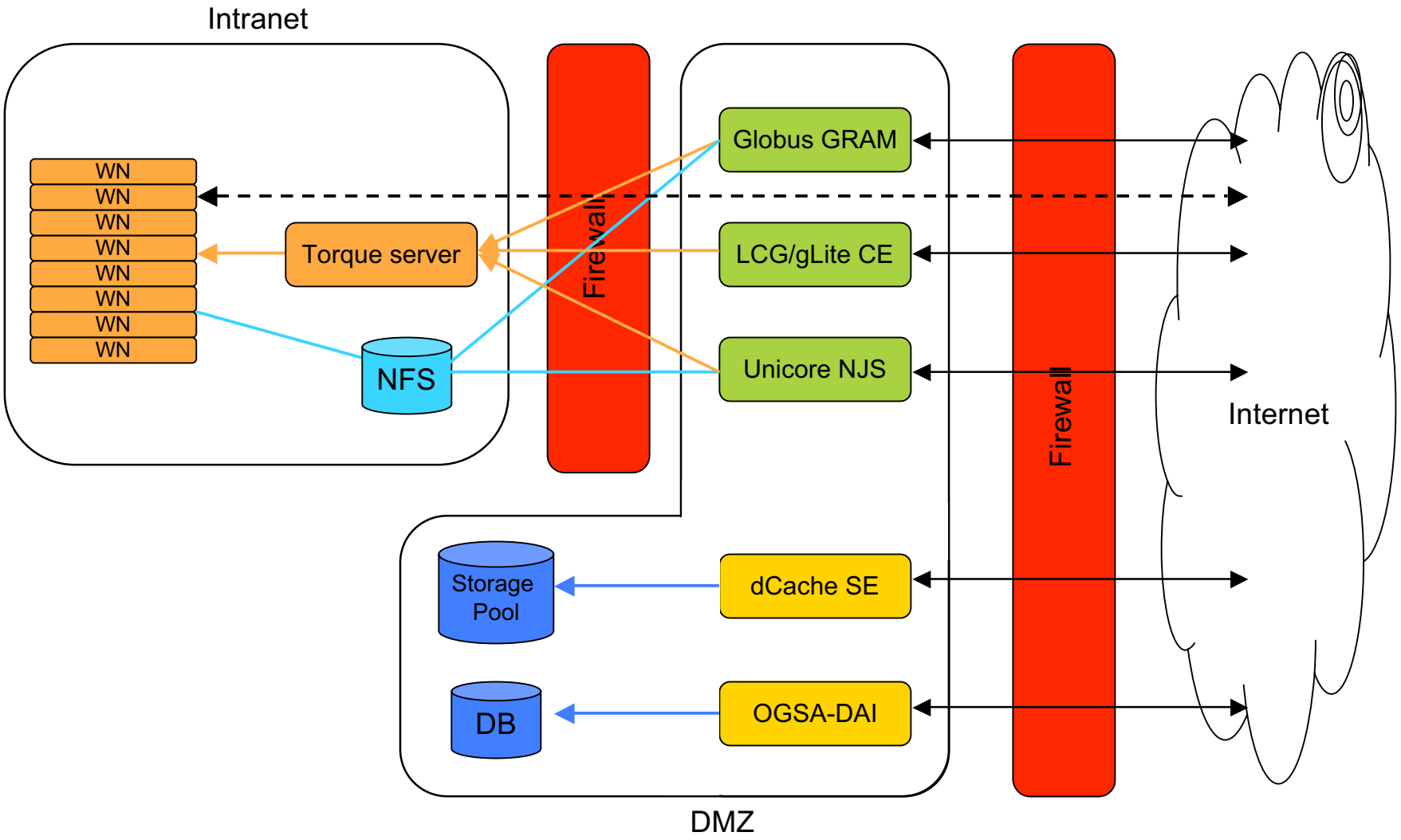
GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Overview

R|R|Z|N

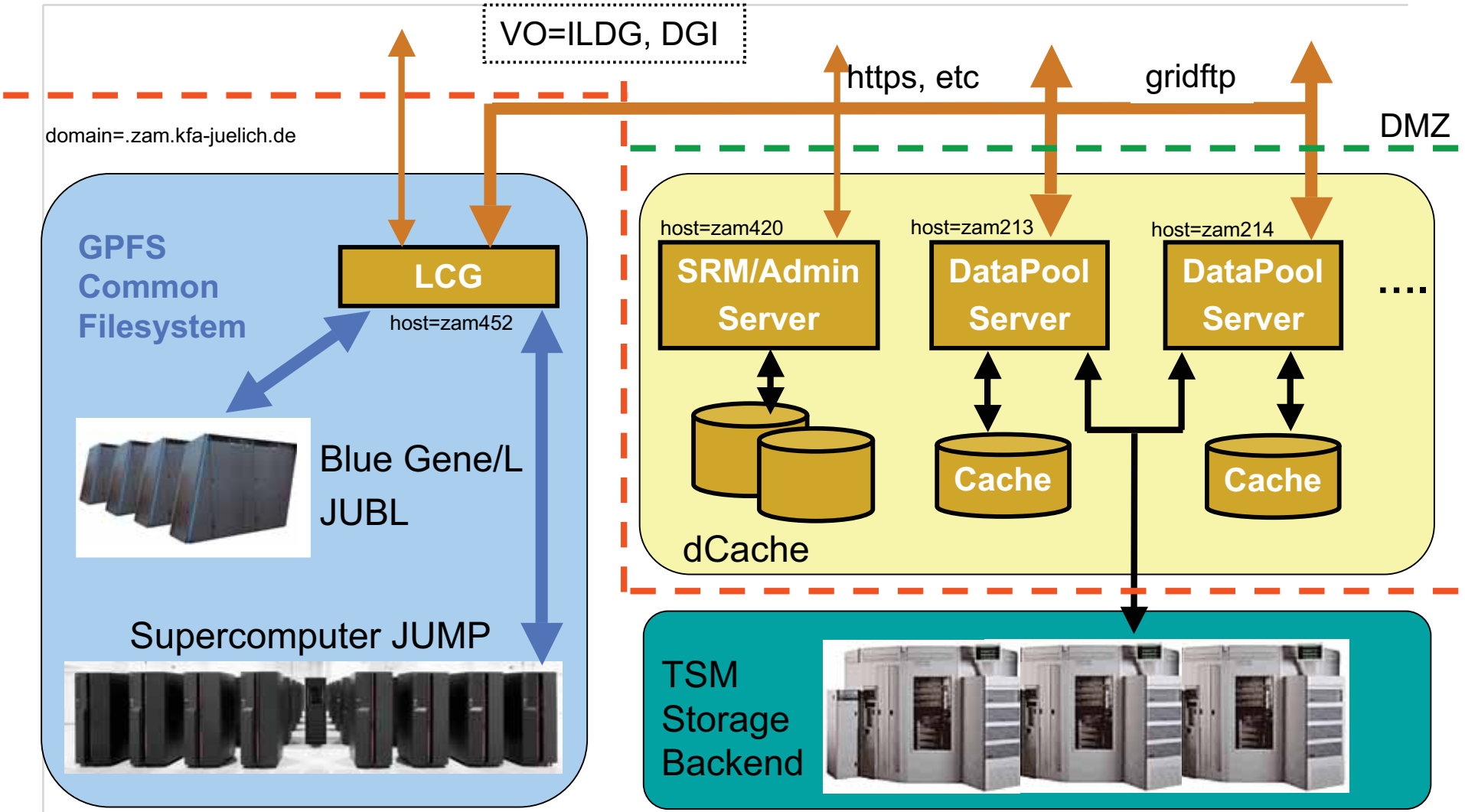
- Resource Providers configuration
- Recommendations for firewall deployment
- GridFTP issues and suggestions
- High-performance firewalls
  - Requirements
  - Operation
  - Experiences

Resource Providers configuration



Resource Providers configuration

R|R|Z|N

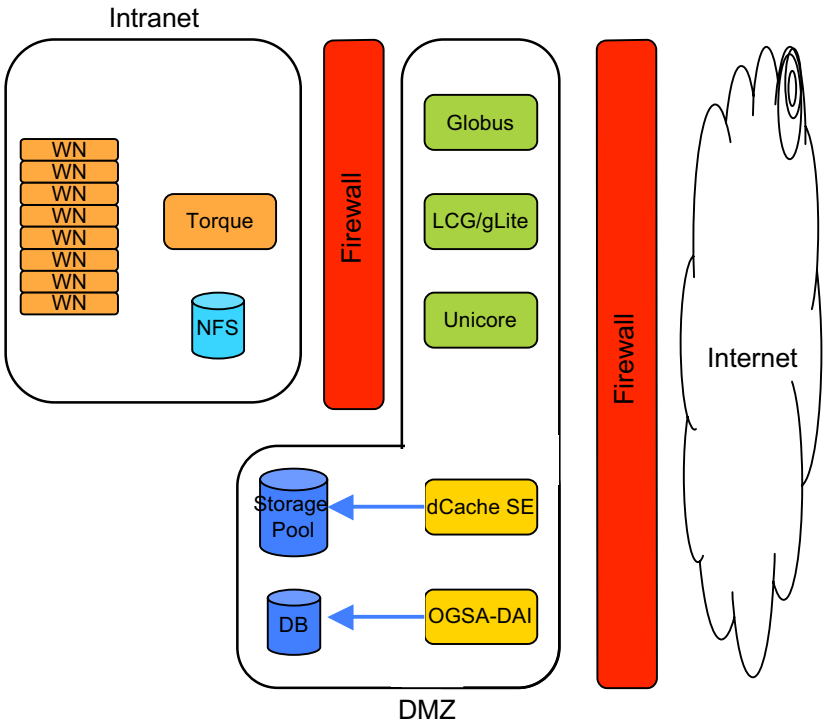


Recommendations for Firewall configuration

R | R | Z | N

List of ports to be opened in the firewall for:

- Globus
- LCG/gLite
- Unicore
- dCache SE
- OGSA-DAI
- Worker Nodes



Assumptions:

- Outgoing connections are always allowed
- Incoming connections are allowed only to the above-listed hosts

Report: “Recommendation for Static Firewall Configuration in D-Grid”

Issues with Firewall configuration

R | R | Z | N

GridFTP servers need a range of open TCP ports (incoming-outgoing)

- Globus GRAM
- LCG/gLite CE
- dCache SE

Use of advanced features provided by GridFTP clients or API in the data transfer tools installed in the WN

- Multiple-streams capability of

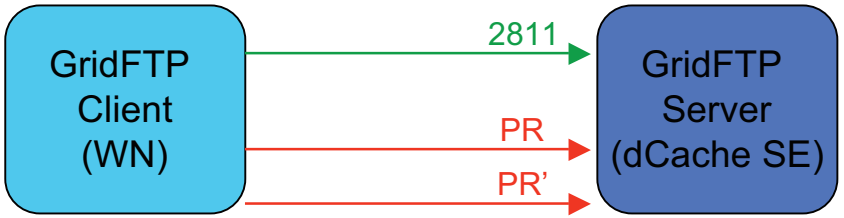
  globus-url-copy

  lcg-cp, lcg-cr

  srmcp

GridFTP behavior

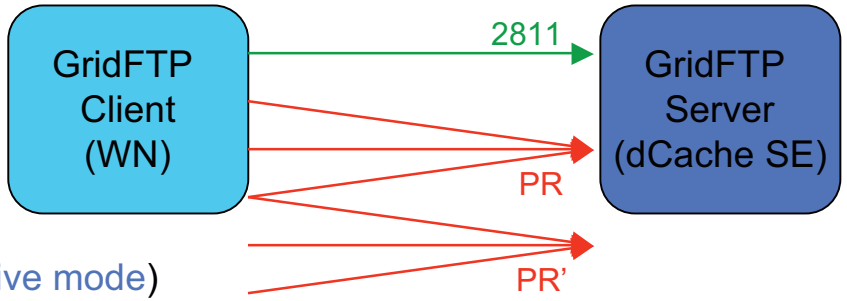
R | R | Z | N



PR = 20000-25000

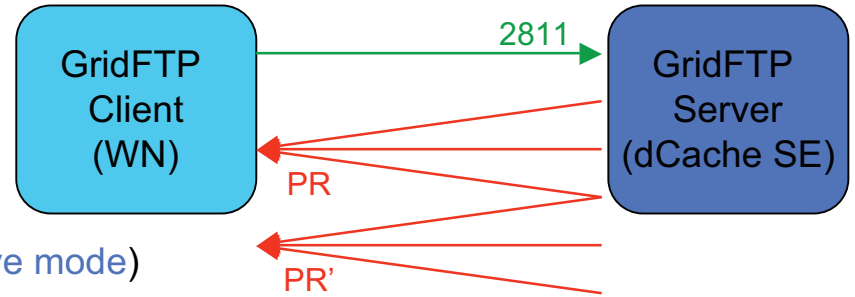
OK

Single-stream GET and PUT (Passive mode)



OK

Multi-streams PUT (Passive mode)



Danger

Multi-streams GET (Active mode)

GridFTP suggestion

R|R|Z|N

- Disable multi-streams (GET) transfers
  &
- Adopt TCP-BIC instead of TCP-Reno

Measurements from FG3-3 “Alternative Transport Protocols”
Hannover - Aachen

	TCP-Reno Mbit/sec	TCP-BIC Mbit/sec
Standard parameters single-stream	61	60
Custom parameters single-stream	151	401
Standard parameters multiple-streams	244	240
Custom parameters multiple-streams	339	511

TCP-BIC is supported by SLC 4.4 and SLES 10.2
TCP-BIC is the standard algorithm for SLC 4.4 (WNs and dCache SE)

Multiple-streams is impossible in most cases because Resource Providers do not allow incoming connections directed to the WNs

Selective filtering

R|R|Z|N

Restrict incoming connections:

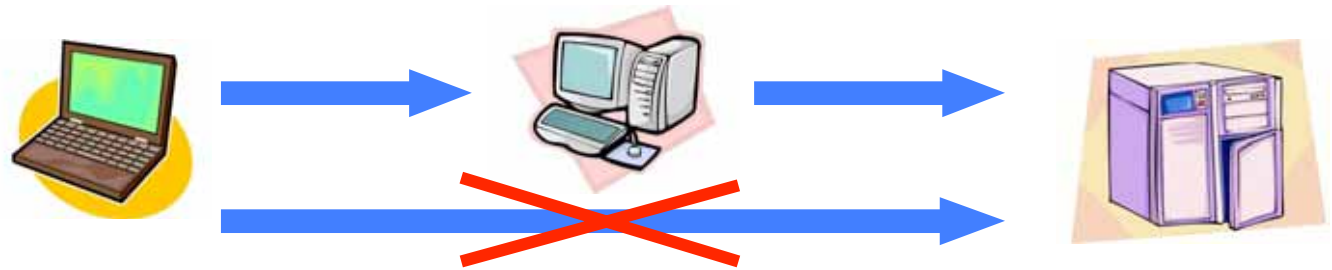
- Source IP address is known
- Destination IP address matches an internal host
- Destination port is in the list of Grid services

How can we know all IP addresses used in D-Grid?

- Central directory where all D-Grid hosts/subnets are registered - Almost impossible!

How can we deal with the mobility of the “Laptop-UI”?

- Use laptop to connect to a “stationary UI” (registered in the directory)
- Only this UI needs to accept connections from any IP address



Einsatz von Highspeed-Firewalls

R|R|Z|N

Einsatzspektrum:

- GRID-Communities sind diversifiziert:
  - von klein, aber hochperformant
  - bis räumlich und organisatorisch weitverteilt
  - oft übergeordnete Sicherheitsrichtlinien
- Unterschiedliche Anforderungen:
  - Leistungsdaten, Skalierbarkeit
  - Ressourcen, Know-how
- HighSpeed-Firewalls müssen den Anforderungen der Ressourcen-Anbieter und Nutzer genügen
  - Anforderungserhebungen
  - einheitliche Testverfahren für Firewall-Systeme notwendig

Leistungsparameter von Firewall-Systemen

R|R|Z|N

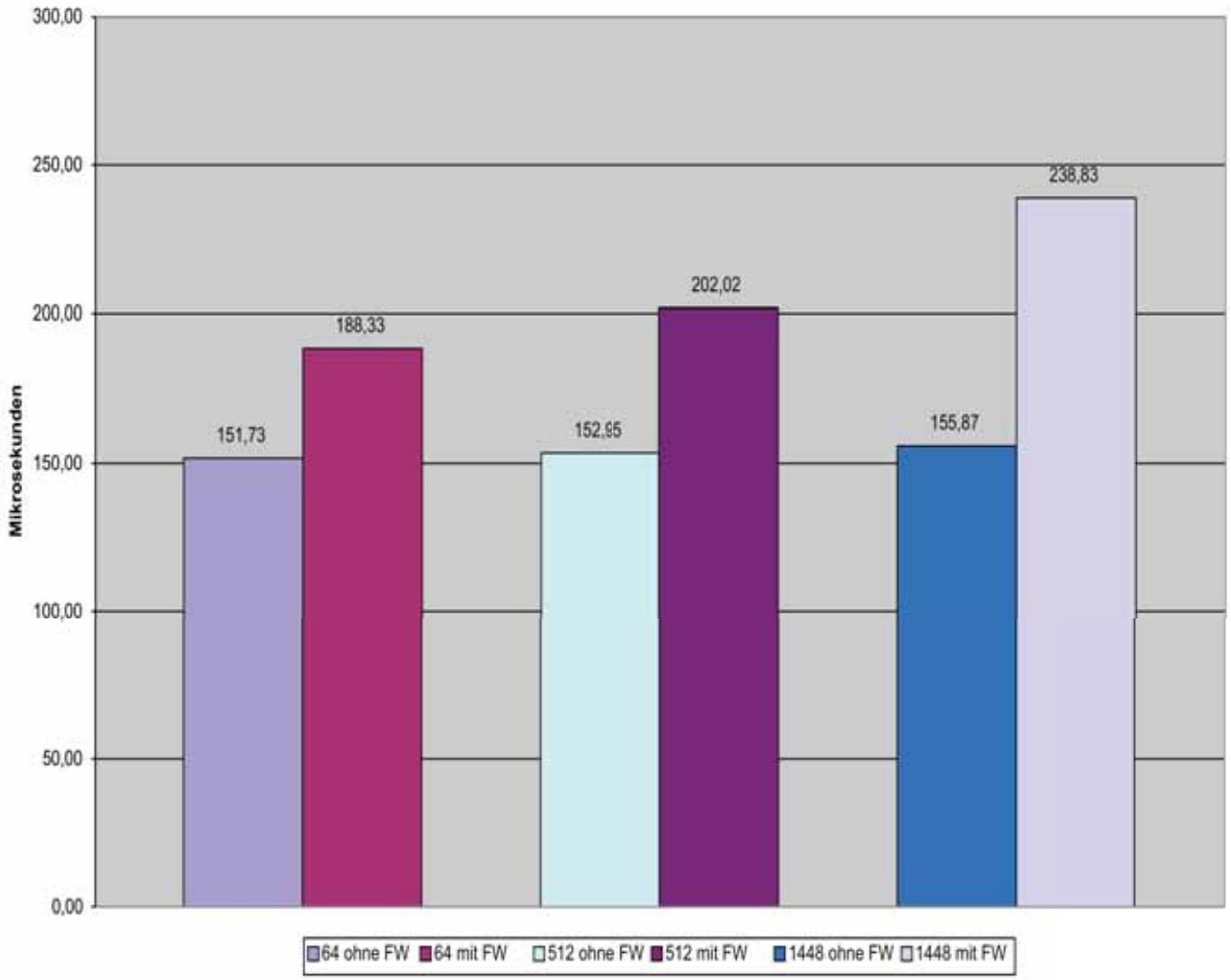
- Verzögerung
  - beim Aufbau von Verbindungen
  - bei aufgebauten Verbindungen
- Durchsatz
- Anzahl der Pakete pro Sekunde
- Anzahl paralleler Verbindungen
  - paralleler Verbindungsaufbau
  - max. Anzahl paralleler Verbindungen
- Bericht: „Firewall-Testszenarien Methoden, Ausführungen und Auswertungen”

Erfahrungen während der Firewall-Tests

R|R|Z|N

Verzögerung:

- Cisco Firewall Services Module im Cisco Catalyst
- Ziel: Messung der Verzögerung im Hinblick auf Latenz sensitive Anwendungen
- unterschiedliche Paketgrößen erzeugen unterschiedliche Verzögerungen



Erfahrungen während der Firewall-Tests

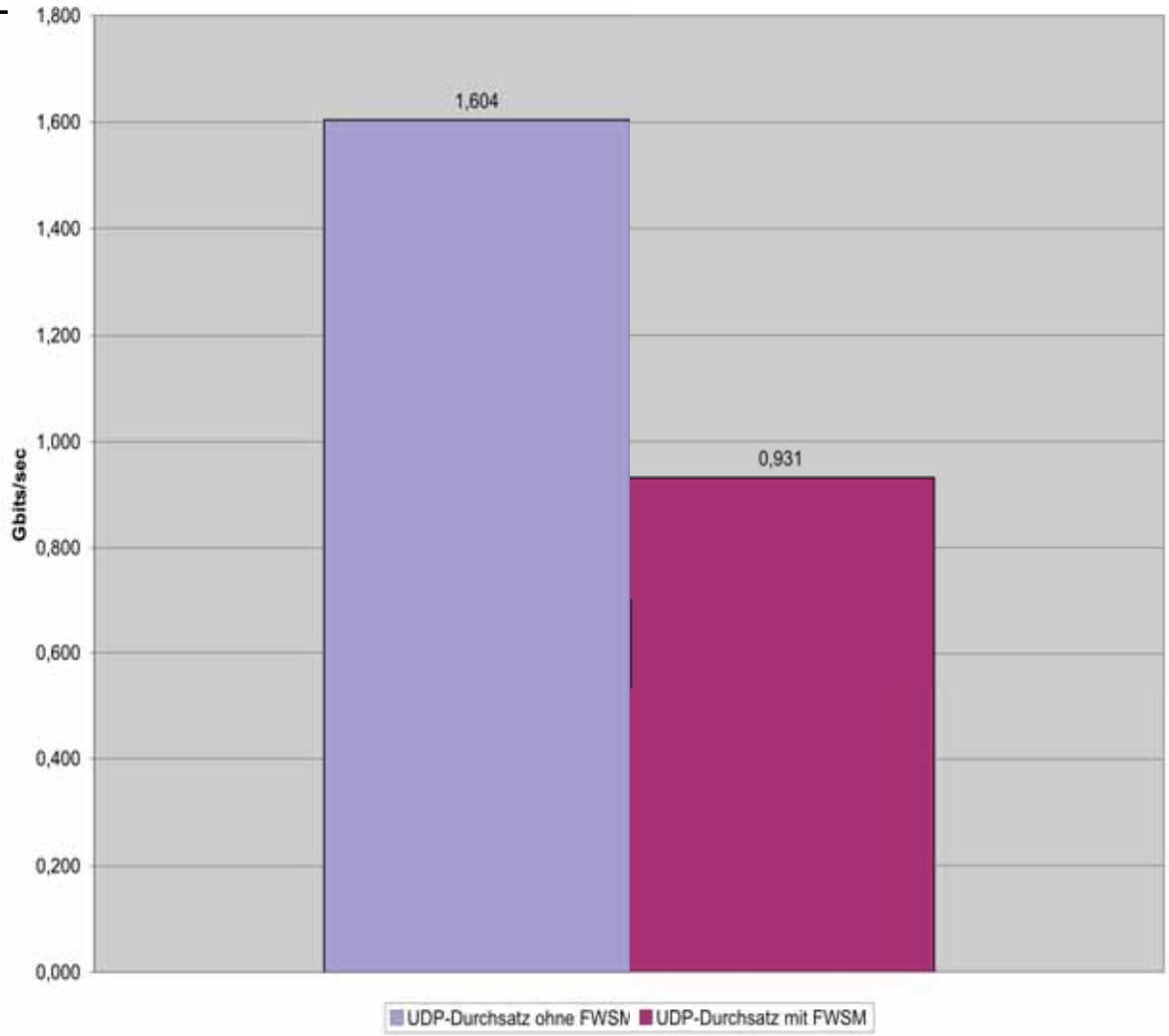
R|R|Z|N

UDP-Single-Stream-Durchsatz

- internes Load-balancing im Cisco Catalyst erlaubt max 1 Gbit/s Single Stream

Weitere Erfahrungen

- UDP-Multi-Streams erzielen höheren Durchsatz
- Testverfahren müssen angepasst werden

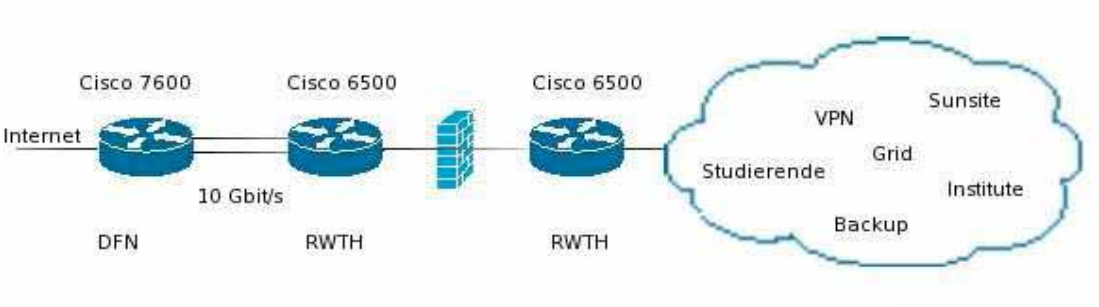


Einsatzszenario RWTH-Aachen

R|R|Z|N

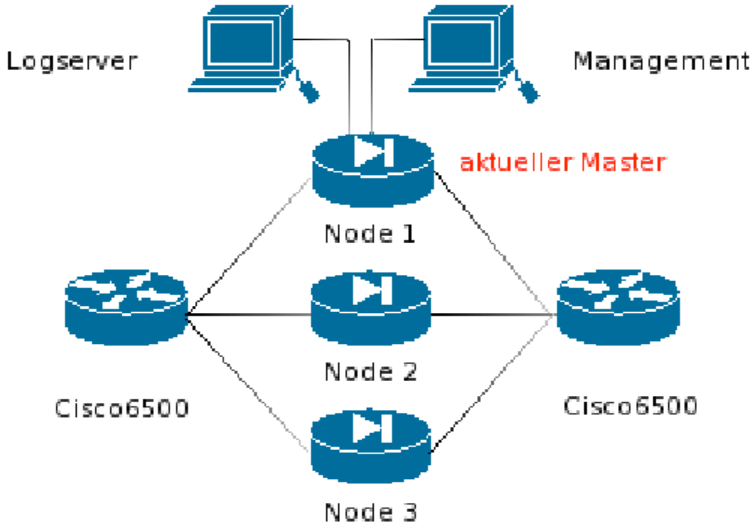
Anbindung an DFN 10 Gbit/s

- Netzwerk Switched Gbit Ethernet, 10 Gbit/s im Core
- Traffic-Mix: Studierende, VPN, Backup, Sunsite, Institute, Grid



Firewall-Konfiguration

- 3 Nodes mit 10 GbE-NICs
- 1 Node als Master
- Load-balancing via Redirect



Overview

R|R|Z|N

- Resource Providers configuration
- Recommendations for firewall deployment
- GridFTP issues and suggestions
- High-performance firewalls
  - Requirements
  - Operation
  - Experiences