JÜLICH
FORSCHUNGSZENTRUM

OpenGridForum
OPEN FORUM | OPEN STANDARDS

# Firewall Virtualization for Grid Applications
# -
# Work Group

r.niederberger@fz-juelich.de
thijs.metsch@sun.com
imonga@es.net

# OGF IPR Policies Apply

- "I acknowledge that participation in this meeting is subject to the OGF Intellectual Property Policy."
- Intellectual Property Notices Note Well: All statements related to the activities of the OGF and addressed to the OGF are subject to all provisions of Appendix B of GFD-C.1, which grants to the OGF and its participants certain licenses and rights in such statements. Such statements include verbal statements in OGF meetings, as well as written and electronic communications made at any time or place, which are addressed to:
    - the OGF plenary session,
    - any OGF working group or portion thereof,
    - the OGF Board of Directors, the GFSG, or any member thereof on behalf of the OGF,
    - the ADCOM, or any member thereof on behalf of the ADCOM,
    - any OGF mailing list, including any group list, or any other list functioning under OGF auspices,
    - the OGF Editor or the document authoring and review process
- Statements made outside of a OGF meeting, mailing list or other function, that are clearly not intended to be input to an OGF activity, group or function, are not subject to these provisions.
- Excerpt from Appendix B of GFD-C.1: "Where the OGF knows of rights, or claimed rights, the OGF secretariat shall attempt to obtain from the claimant of such rights, a written assurance that upon approval by the GFSG of the relevant OGF document(s), any party will be able to obtain the right to implement, use and distribute the technology or works when implementing, using or distributing technology based upon the specific specification(s) under openly specified, reasonable, non-discriminatory terms. The working group or research group proposing the use of the technology with respect to which the proprietary rights are claimed may assist the OGF secretariat in this effort. The results of this procedure shall not affect advancement of document, except that the GFSG may defer approval where a delay may facilitate the obtaining of such assurances. The results will, however, be recorded by the OGF Secretariat, and made available. The GFSG may also direct that a summary of the results be included in any GFD published containing the specification."
- OGF Intellectual Property Policies are adapted from the IETF Intellectual Property Policies that support the Internet Standards Process.

# Agenda

0.) Agenda, note-taker, IPR statement, Charter discussion

1.) Introduction and status of FVGA-WG

2.) Group discussions

# Introduction and status of FVGA-WG

# FVGA-WG
# Administrative Issues

**Group Name:** Firewall Virtualization for Grid Applications - Working Group (FVGA-WG)

**Area:** Infrastructure

**Mailing list:** fvga-wg@ogf.org

**Projects page:**
https://forge.gridforum.org/sf/projects/fvga-wg

**Protocol draft:**
http://forge.gridforum.org/sf/docman/do/downloadDocument/projects.fvga-wg/docman.root.drafts/doc15527/1

**Contacts**:

- Ralph Niederberger: r.niederberger@fz-juelich.de
- Thijs Metsch: thijs.metsch@sun.com
- Inder Monga: imonga@es.net

# Group Summary

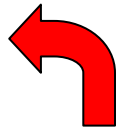
- Grid Computing
  - vision of applications having on-demand, ubiquitous access to distributed services running on diverse, managed resources like computation, storage, instruments, and networks among others, that are owned by multiple administrators.
- fi-rg has documented use cases & issues that Grid applications face (GFD.83) with firewalls and has documented which cases need additional attention (GFD.142)
- fvga-wg
  - will leverage the application requirements from FI-RG
  - standardize a set of service definitions for a virtualized control interface into firewalls and other midboxes allowing grid applications to securely and dynamically request application/workflow-specific services

# Goals/Deliverables

- Produce a standardized protocol for an authorized grid application to specify its data-path traversal requirements:
  - Port opening/closing service
  - Requests from within and outside the security domain
- A set of security recommendations surrounding the application interacting with the Firewall service at the control and data plane including AAA of the service requests
- A best practices document for the network-administrator and a grid-administrator to understand the architecture and security implications of this deployment including:
  - Deployment scenarios and use-cases
  - Interactions between various Grid components
  - Examples of successful prototype deployments
- The resulting standard, the security recommendations and the best practices document developed by the working-group will enable Grid-Middleware services developers to include a dynamic firewall service into their Grid applications.

# Group Milestones

| | |
|---|---|
| OGF23: | Charter discussion and group volunteers |
| OGF24: | Discussion on requirements to define the standardized service interface for virtualized Firewalls |
| OGF25: | Draft on Firewall-Virtualization-Service |
| | Discussion on Security, AAA and Grid-Security aspects |
| OGF26: | Firewall Virtualization-Service draft version 2 |
| | First draft on Security recommendations (v1) for FVGA |
| OGF27: | Finalized Firewall Virtualization-Service draft |
| | Security Recommendations v2 |
| | Two implementations and demonstration |
| | Discussion on Best Practices draft |
| OGF28: | WG-Last-Call for Firewall Virtualization-Service |
| | Final version of Security Recommendations |
| | First draft on Best Practices |
| OGF 29: | WG-Last-Call Security Recommendations |
| | Finalize Best Practices draft |
| OGF 30: | WG-Last-Call Best Practices Draft. |



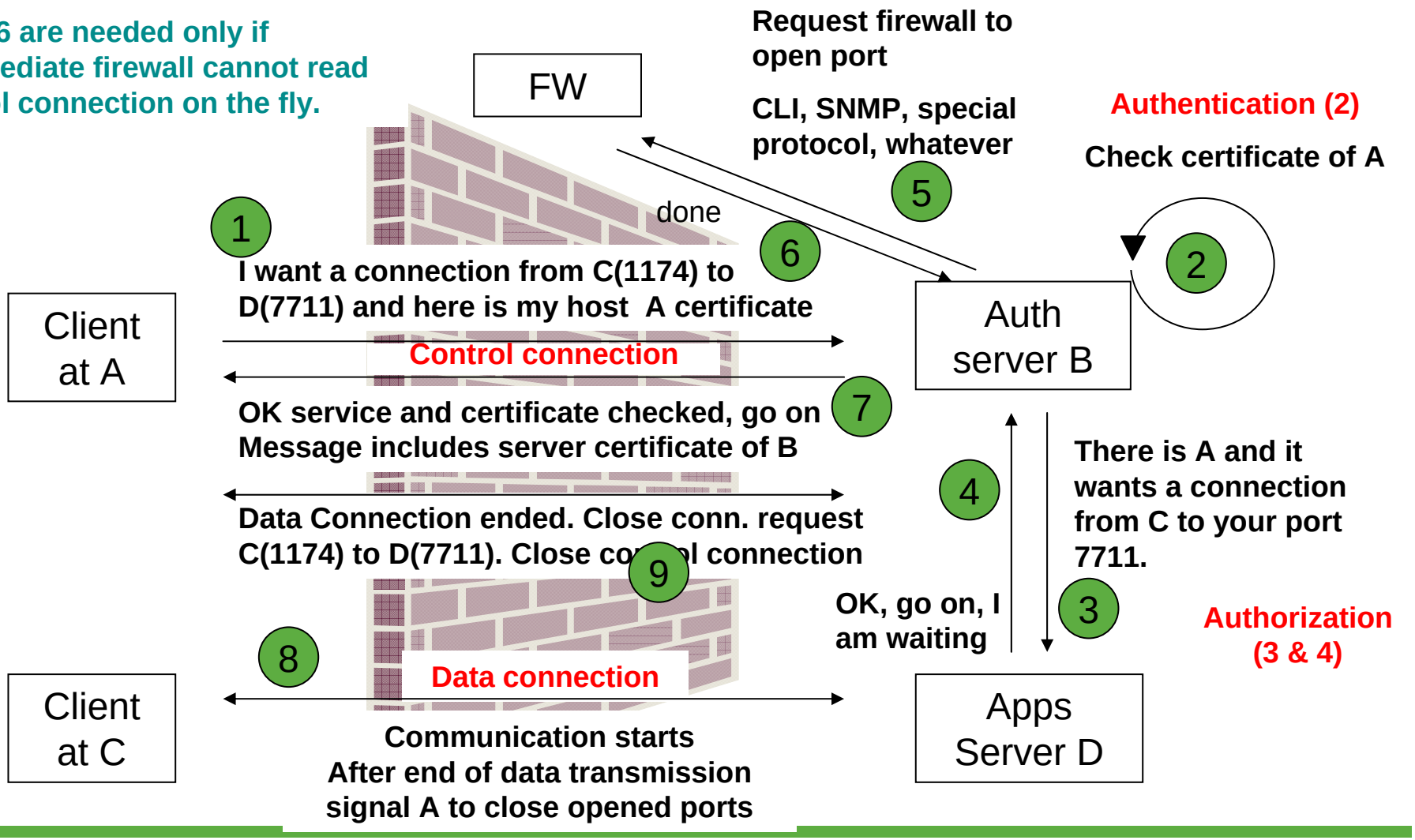
**We are still here**

# Proposed Solution

- Make middleware and network resources known to each other
  - Grid middlewares should know, but must not know about communication path
  - network resources should be opened dynamically
- End-to-end applicability
- Local authorization/authentication
- Independence of the FW vendor/implementation
  - Capabilities may be different

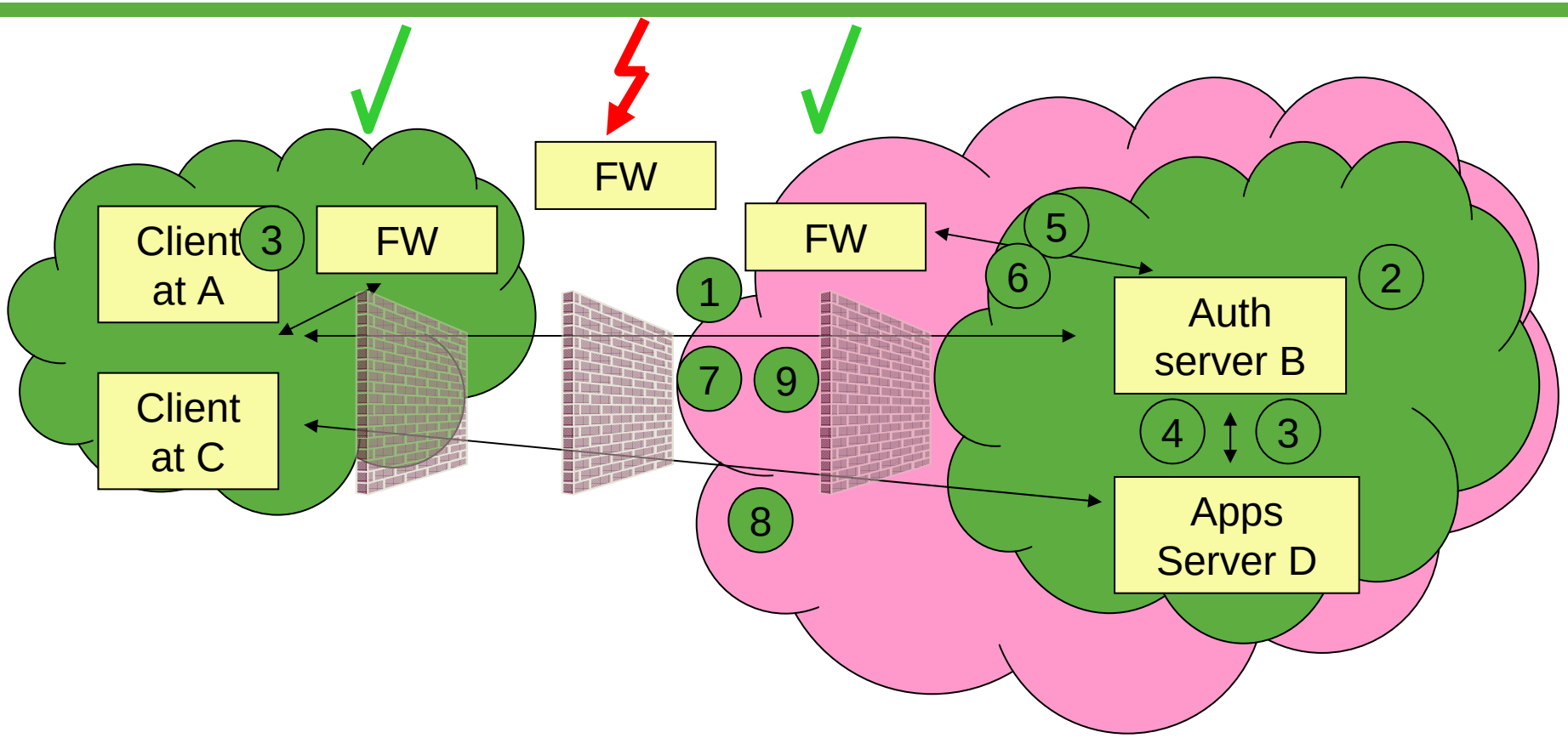
# principle design for FW opening

5 and 6 are needed only if intermediate firewall cannot read control connection on the fly.



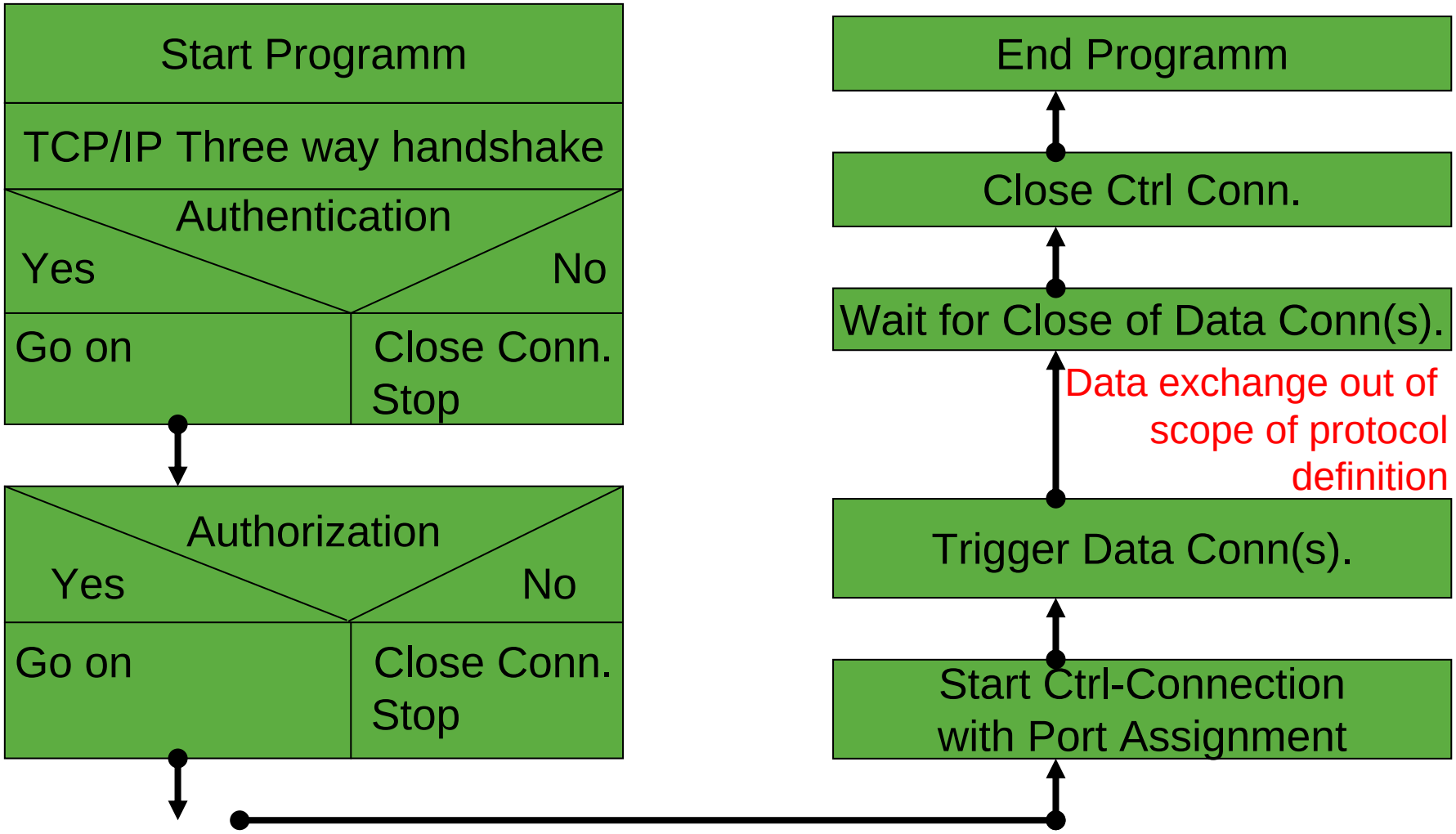
# WebServices based FW opening

## Multiple local, remote and external FWs




This part can be solved only, if control connection is unencrypted, i.e. intermediate firewalls can read datastream of control connection.

# Program flow chart



# Status of working group

- A Firewall Traversal Protocol (FiTP) has been defined which allows opening of ports on intermediate firewalls.
- In principle this protocol defines the control connection discussed in the previous slides.
- Protocol draft is still under discussion (first discussion in OGF 25, second time in OGF 26)
- Protocol has been forwarded to IETF members for feedback.
- No comments received until now.

- Next steps:
- Further discussion on draft in OGF 27
- Including feedback from IETF into protocol draft (**no feedback yet**)
- Providing two independent implementations (client and server)
- After refinements: standardization at OGF and IETF
- Timeline: one to two OGFs behind milestones

JÜLICH
FORSCHUNGSZENTRUM

OpenGridForum
OPEN FORUM | OPEN STANDARDS

# Questions and discussion