JÜLICH FORSCHUNGSZENTRUM

OpenGridForum
OPEN FORUM | OPEN STANDARDS

Firewall Virtualization for Grid Applications
-
Work Group

r.niederberger@fz-juelich.de
imonga@nortel.com
thijs.metsch@dlr.de

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

1. Update, status and future of FI-RG
2. Introduction and status of FVGA-WG
3. First thoughts for a dynamic firewall configuration
4. Group discussions

Update, status and future of FI-RG

- After more than 3 years FI-RG has been „hibernated“ at last OGF
- Can be reactivated, if any new issues arise
- #2 document is in public comment „Requirements on operating Grids in Firewalled Environments“

- Work will be taken over by FVGA-WG, which will try to define a protocol standard for dynamic opening of ports

Introduction and status of FVGA-WG

Administrative Issues

Group Abbreviation:

- fvga-wg

Group Name:

- Firewall Virtualization for Grid Applications - Working Group

Area:

- Infrastructure

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.
  - dynamic, seamless Virtual Organizations (VOs) using distributed resources
  - application driven transport privileges from the network
  - pre-existing security policies within the network (firewalls, NAT, ALG, VPN-GW)
  - administrator/manual intervention to work.
- fi-rg has documented use cases & issues that Grid applications face (GFD.83)

- 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 standard set of service definitions that provide an abstract interface for an authorized grid application to specify its data-path traversal requirements:
  - Port opening/closing service
  - Data Plane and Service Plane interactions
  - 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 standards from the working-group will enable Grid-Middleware/Network services developers to implement a virtualized firewall service, integrate with Grid-middleware security and provide a dynamic firewall service to the Grid applications.
- The working group will ensure that it is compatible with the OGSA architecture and leverages the security infrastructure and standards for 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.

Future contributions

- **Mailing list:** fvga-wg@ogf.org
- **Projects page:** https://forge.gridforum.org/sf/projects/fvga-wg
- Contacts:
  - Inder Monga: imonga@nortel.com
  - Ralph Niederberger: r.niederberger@fz-juelich.de
  - Thijs Metsch: thijs.metsch@dlr.de

The Problems?

- Control Plane (ex. Web Services) vs. the Data Plane
  - CP using port 80 works seamlessly but Data Plane gets blocked
- Manual vs. Automated
  - Document the ports per middleware, grid protocol deployed or authorize the CP to provide a level of automation
- Static vs. Transient
  - Related issues as above

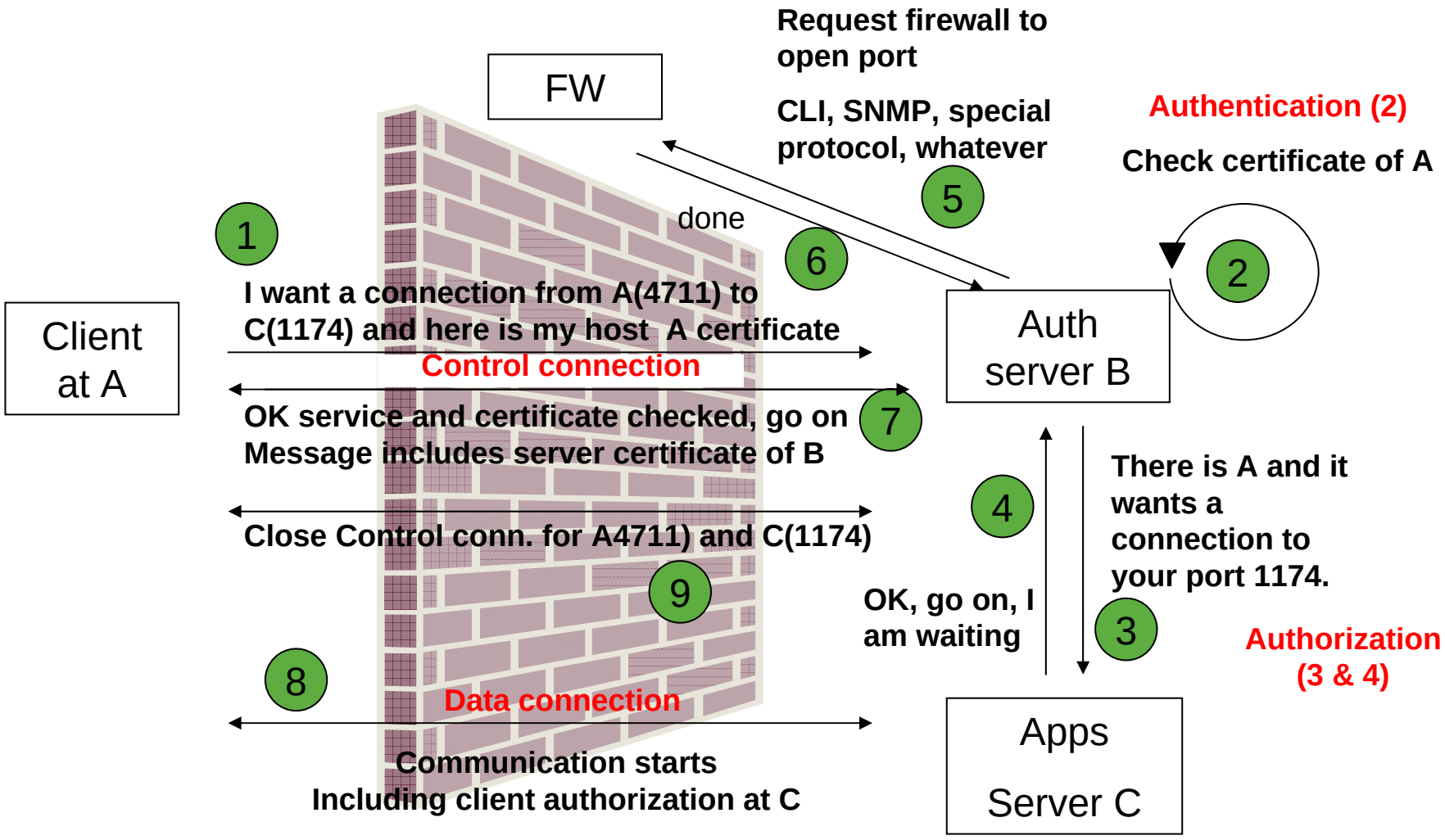
Proposed Solution

- Make middleware and network resources known to each other
  - Grid middlewares should 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

First thoughts for a dynamic firewall configuration

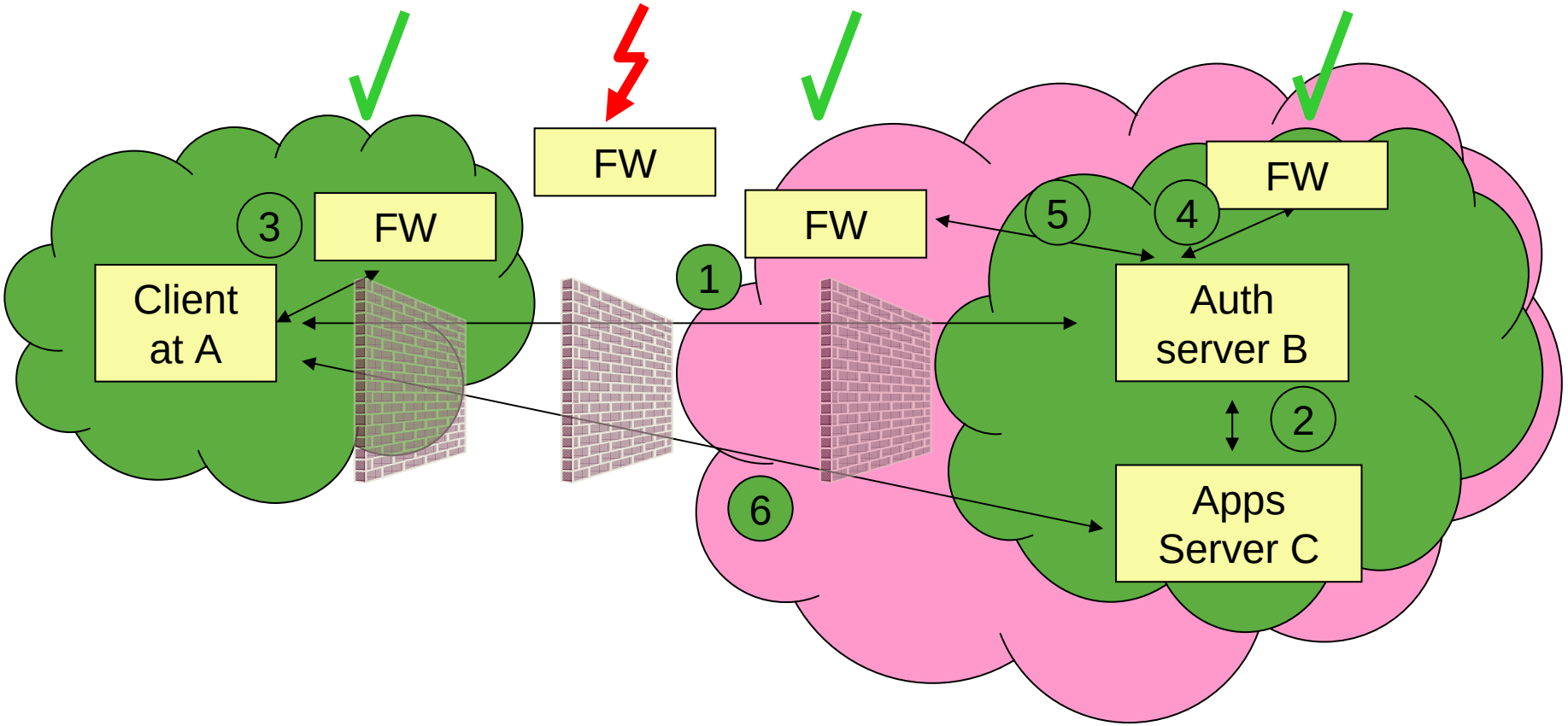
WebServices based FW opening

principle design



WebServices based FW opening

Multiple local, remote and external FWs



Open questions (1)

Which parts should be standardized?

- Control connection
- Authentication
- Authorization
- Data connection

Open questions (2)

What kind of connections should be allowed? Let be:

- A (Control-Connection-Client)
- B (Control-Connection-Server)
- C (Authentication-Server)
- D (Authorization-Server)
- E (Data-Client)
- F (Data-Server)

A=E &/v A≠E

B=C=D=F v B≠C≠D≠F v „any combination“

Open questions (3a)

Number of connection allowed?

a) Port A to Port B

b) Port [A1…An] to Port [B1…Bm]

c) Port * to Port *

d) „any combination“

If multiple streams allowed, define a standard format for specifications.

Example: Interpretation of [A1…An],[B1…Bn]?

a) [A1-B1],[A2-B2],…[An-Bn]

b) [A1-B1],[A1-B2],…[A1-Bn], [A2-B1],[A2-B2],…,[A2-Bn],…,[An-Bn]

Open questions (3b)

How does the exchange of used (to be used) ports take place?

a) Client says which one to use
b) Server responds which one to use
c) Client fixes client port and waits for server port
d) Any other recommendations?

Open questions (4)

It has to be checked, if

- FTP
- SIP
- H.323
- …..

control structures/protocols can be used.

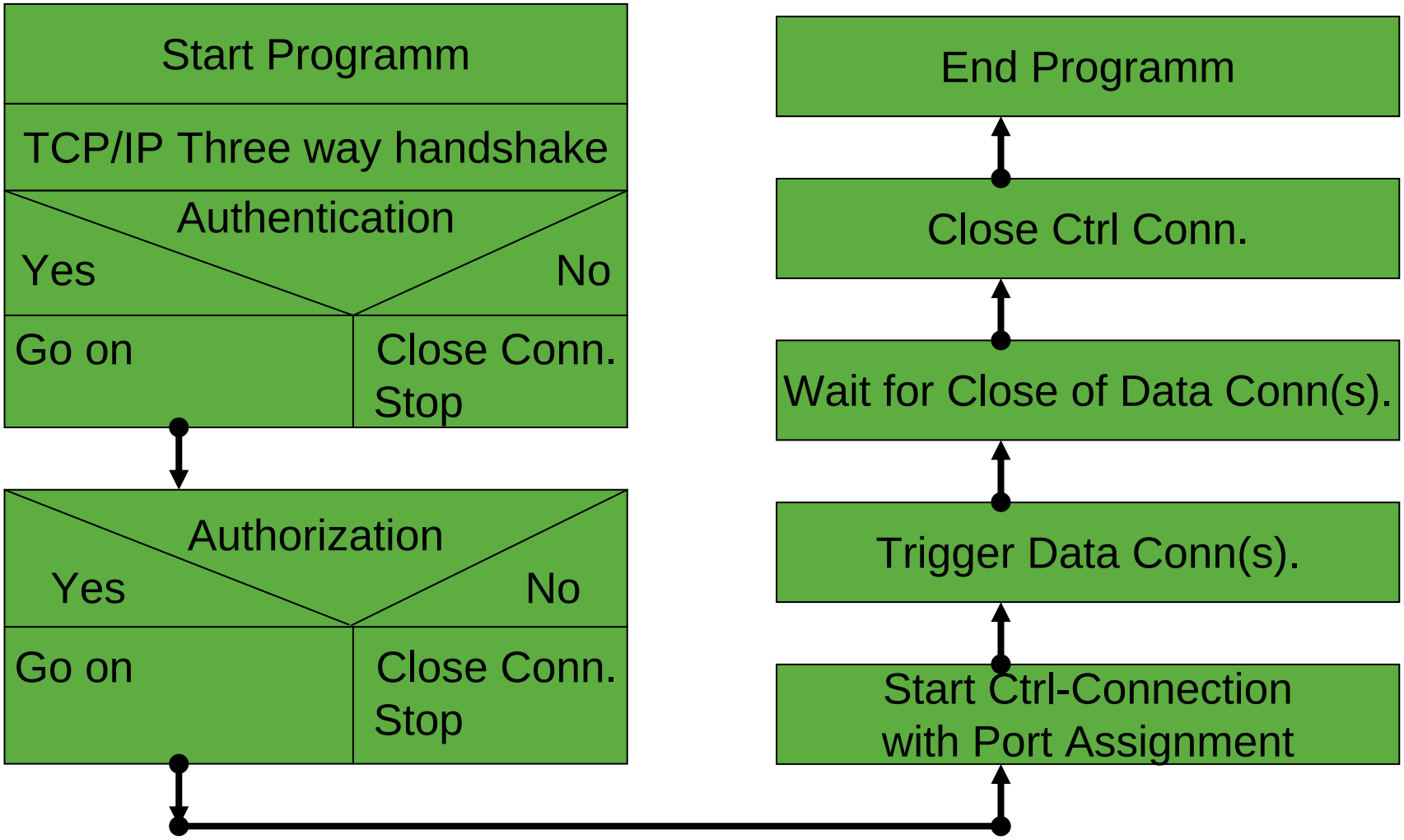
Using as opener as a whole or using parts of those protocols

Simple state machine

- three way handshake
- Authenticating
- authorizing
- control connection established
- agreement on dynamic port(s) to be opened including starting of session with data server (getting ports to be used)
- data exchange (done between client and data server)
- closing session with data server
- closing control connection with client
- finish connection

Of course there are additional states needed. The listing above is a first draft only.

Program flow chart



JÜLICH
FORSCHUNGSZENTRUM

OpenGridForum
OPEN FORUM | OPEN STANDARDS

Questions and discussion