A webservices based dynamic Firewall config approach? (or Firewall Virtualization for Grids)

R.Niederberger@fz-juelich.de
imonga@nortel.com

GGF 21 - FI-RG - 17.10.2007

What we have seen right now. Status of document #2 at FI-RG

r.niederberger@fz-juelich.de
imonga@nortel.com

The first gap

There is a gap between FW development and Grids apps usage.

FW vendors implement standard protocols, if they are widely used.

Grid application programmers use standards if they can be used across firewalls.

If there are (easy) bypasses available, they do not need to invent new standards

But who develops the standards making life easy and applications optimized?

r.niederberger@fz-juelich.de
imonga@nortel.com

The second gap

Some comments from industry:

"450 Mio. MS Office users are a market share.
How many do you have?"

"Implementing alternate or extended TCP standards in switches, routers and firewalls will be done, if there is a business case."

How much grid users (applications) do we have?

Should we count heads / nodes / CPUs?

Vendor attention is tough unless $$'s seen around the corner

r.niederberger@fz-juelich.de
imonga@nortel.com

A third gap arises

What, when there would be a protocol for dynamic firewall opening available?

Time for depreciation of FW equipment is about 5 years.

So what if I just got a new one without supporting standards coming up soon?

Should there be an intermediate solution available?

Should we look for just another circumvention?

How long does it last?

What about implementing a solution which fits both? If it would work right now, but it would leave time for adoption?

r.niederberger@fz-juelich.de
imonga@nortel.com

Next steps ?

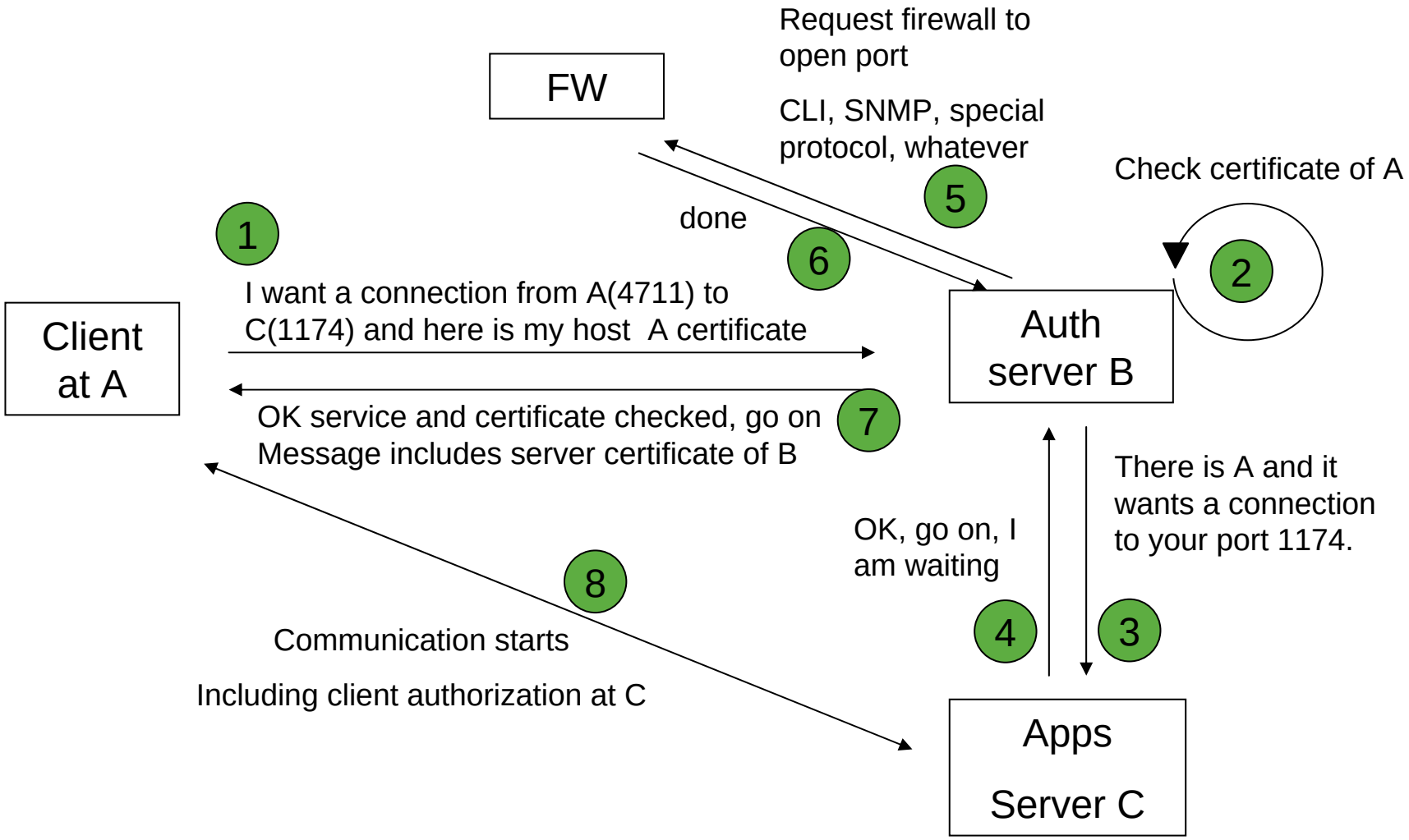
- Conclusions from FI-RG research
- No solution fits all, especially dynamics are not solved well

- Start on specification/work around the "virtualization" of firewall.
- a web-services interface that will be part of Grid middleware brokering between grid requests and firewall configuration to bypass traffic.
- This can be dynamic, offline or inline.

r.niederberger@fz-juelich.de
imonga@nortel.com

WebServices based FW opening

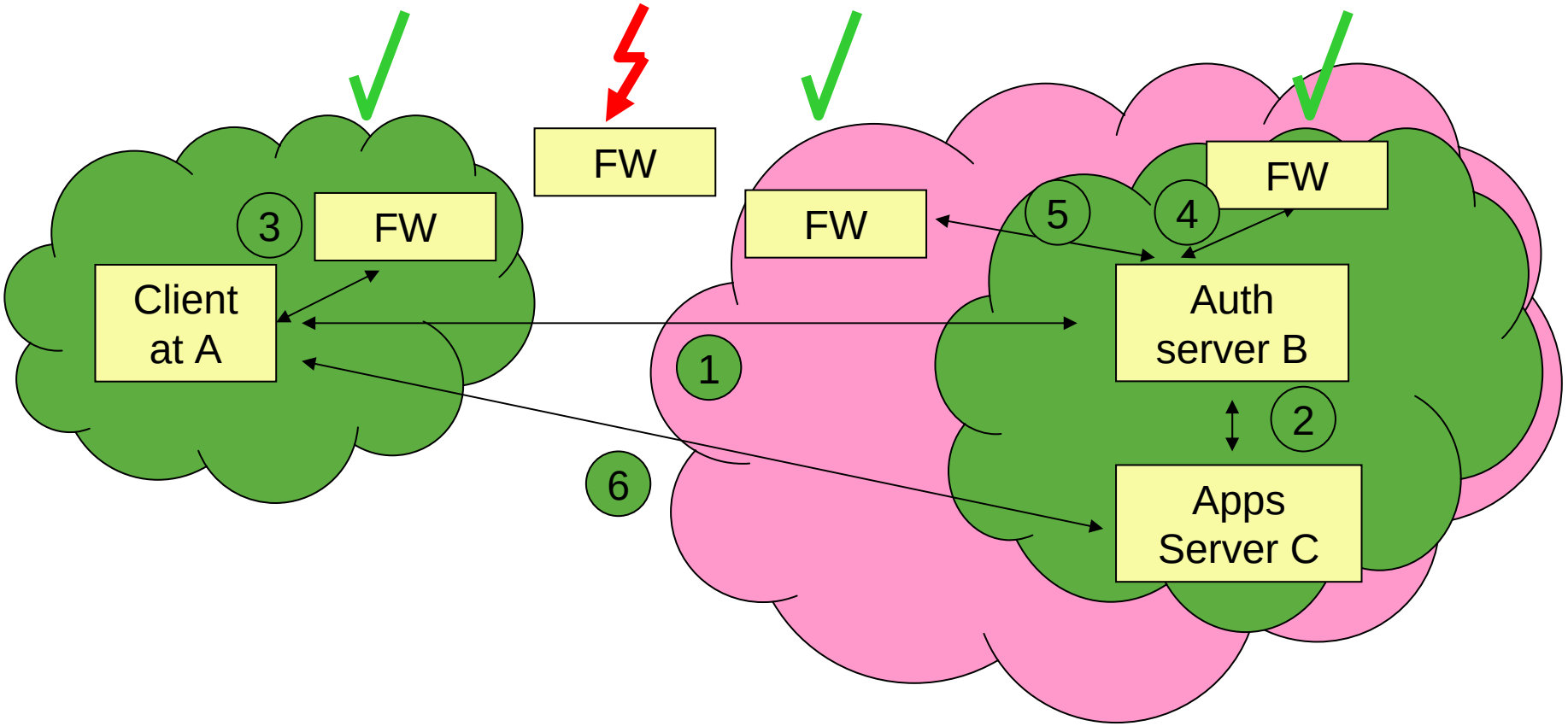
principle design



r.niederberger@fz-juelich.de
imonga@nortel.com

WebServices based FW opening

Multiple local, remote and external FWs



Pros of a Webservices based approach

- With CLI, dynamic opening can be done without new protocol definitions at Firewalls
- Nevertheless new FW software developments can introduce the new Web based protocol and look into packet. If Auth server acknowledges, port can be opened

r.niederberger@fz-juelich.de
imonga@nortel.com

Spawning of a FW-WG?

A discussion we had at last OGFs before:

- Should we provide this intermediate solution to overcome those gaps?
- Should we pave the way to a new standard by showing what‘s needed, what‘s possible, and how to do it?
- Should we evolve to become a FI-WG?
- Do we have the critical mass to start over?

- We think: Yes, we have.

r.niederberger@fz-juelich.de
imonga@nortel.com

A possible startup

- BoF at OGF 22 discussing this issue.
- Creating WG
  - Defining Protocol
  - Creating sample test app
  - Documentation

We have to make advertisement

- to get help and
- to get people involved.

We have to discuss our ideas with other OGF groups.

I think we have already our area directors convinced.

r.niederberger@fz-juelich.de
imonga@nortel.com

Questions and discussion

Questions
and
discussion

r.niederberger@fz-juelich.de
imonga@nortel.com