

# UK GRID FIREWALL WORKSHOP

A meeting held at the National e-Science Centre on 5 November 2002

Organised by Paul Jeffreys (Oxford University) and David Boyd (CLRC)

---

## 1. CONCLUSIONS OF THE WORKSHOP

The conclusions of the meeting are given in sections 7 and 8.

### **In summary:-**

- There must be a clear assignment of responsibility for resources attached to the Grid to system administrators.
- There is a distinction between network firewalls protecting a site (strategically important and relatively static) and host-based firewalls running on Grid resources.
- **The trusted host server solution is acceptable to most sites as a short term (but not scalable) mechanism for configuring host-based firewalls, but it must be securely managed and accessed and must be maintained up-to-date.**
- **An initial step will be to download to each site participating in the Level 2 Grid a file containing a list of IP addresses and port ranges in order to make rapid progress towards the implementation of the trusted host solution.**
- The dynamic firewall may be of interest as a more scalable and potentially more secure host-based firewall mechanism in some situations.
- A hybrid host (with static IP addresses) and dynamic firewall solution may be useful for getting operational quickly.

## 2. OUTLINE OF THE WORKSHOP

Following the meeting held on 1 May 2002, 'Making the Grid Work in a Computing Services Environment', a series of workshops was planned to address specific issues.

The first of these considered the use and maintenance of firewalls within a Grid environment.

The purposes of the meeting were:-

- *To bring together developers of the UK e-Science Grid and computing service providers;*
- *To enable the technical support community and e-Science/Grid community to exchange ideas and networking/firewall information;*
- *To produce a coherent set of recommendations for firewall configuration and maintenance for the U.K. Level 2 Grid, and to identify practical workable solutions for use with the Grid.*

The main aim of the workshop was to focus on implementations suitable for Globus within a Level 2 Grid (L2G) framework, but also considered issues related to Web Services.

There was an open invitation to the UK e-Science community, network administrators and firewall administrators, and more than 50 people attended.

In the morning there were a number of scene-setting presentations (available from <http://umbriel.dcs.gla.ac.uk/NeSC/action/esi/contribution.cfm?Title=121>):-

*Introduction to part of GLOBUS relating to use of firewalls - Andrew McNab*

*Introduction to Web Services as they relate to use of firewalls - Matthew Dovey*

*A 'Dynamic' Firewall - Jon Hillier*

*A 'Clique/Trust' Firewall - Jon Hillier*

*Firewall Configurations - Jon Hillier*

*GRID and VPNs - Matthew Dovey*

These were followed in the afternoon by 4 parallel break-out groups which were asked to discuss the suitability and applicability of the various solutions discussed during the morning namely:-

- "Clique GRID" – Trust based
- Dynamic Firewall

- VPN (IPSec) Tunnelling

The aim was not towards a prescriptive firewall solution, but to appraise a set of possible solutions, in order that attendees would be in a position at the end of the workshop to leave with the best possible information and understanding in order to deploy the Level 2 Grid in their own academic environments.

For each solution the break-out groups were asked to address the following questions:-

1. Does the solution offer the required security for the GRID projects?
2. Are there inherent security weaknesses of the solution which would make it less suitable?
3. How effective would the solution be for a level 2 GRID?
4. Is the solution scalable beyond a level 2 GRID?
5. Would the solution still be valid in protecting a GRID based on GridServices or WebServices?
6. Would the solution still be required for a GRID based on GridServices or WebServices?
7. Are there technical problems with the solution which would affect its use in GRID projects?
8. Are there technical problems with the solution which would affect its adoption at an institution?
9. Is the solution consistent with current security policies in place at institutions or in GRID project?
10. Will the solution remain consistent with future security policies?

The following sections summarise the recommendations for future action which emerged from these break-out groups, and in the subsequent feedback and open discussion session which ended the meeting. The variations reported across the break-out groups represent the range of opinion in the meeting.

### **3. WORK GROUP A**

3.1 The assumptions made by the group were:-

- Necessary to consider application specific firewall
- Ephemeral ports are allowed to be open – for Gatekeeper only
- Delegate responsibility to gatekeeper administrator (well specified)

3.2 Suggestions made by the group were:-

- Need a uniform procedure
- Standard L2 Gatekeeper on all sites recommended (separate hardware item)
- Support (on site) required for Rpm, documentation, training.

### 3.3 Conclusions re. firewall models:-

- VPN: Not viable in near future (eg lack of interoperability)
- Dynamic/Clique hybrid: go for hybrid with static addresses initially, scope for dynamic firewall later as offers scalability

## 4. WORK GROUP B

### 4.1 The assumptions made by the group were:-

- Focus on a Level 2 grid.
- Quick 'n' dirty solution.

### 4.2 The following questions were asked:-

- What are we protecting?, from whom? and why?
- Should grid machines (resources, gatekeepers, clients) be kept on a separate subnet or vlan?
- Whose regulations will govern use of the facilities?
- Is separating grid machines from the rest of the LAN a good idea?
- Why is there a limited port range?

### 4.3 Conclusions re. firewall models:-

- Grid clients should be placed on a separate subnet.
- For firewall access, limit GridFTP usage to single, non-PASV mode so that no servers have to be started on the client.
- VPN idea possibly too complex to enable in time.
- Dynamic firewall idea needs more investigation but shows promise, only for software firewalls though.
- Host database solution too complex?

## 5. WORK GROUP C

### 5.1 Opinions offered by the group were:-

- Each potential solution would work if resources were fenced into their own security sub-domains. Concentrating on this, practical and implementable security domains may be more important than firewall rules. These would not necessarily prevent a serious security breach of GRID resources bringing the institution into ill-repute.
- A clique GRID based on DNS lookups may be implementable within the L2G timeframe but there are issues over replication delays for roaming IP addresses.

- A robust implementation of a dynamic firewall may not be possible within the L2G timeframe, especially as ideally a dynamic firewall would need multiple back ends to interact with different firewall platforms.
- Timescales must also allow time for institutions to integrate any solution with the local policies.

## 5.2 Conclusions re. firewall models:-

- The VPN solution has the advantages of being available off the shelf and more viable in the longer term, but there are interoperability issues between the current VPN solutions.

## 6. WORK GROUP D

### 6.1 Opinions offered by the group were:-

- Important that underlying *operating system* on Grid clients and servers is made secure - this is mainly a case of following good practice.
- Focus should be on keeping Grid resources secure rather than trying to prevent access.
- Where possible Grid accessible resources should be kept separate from other sensitive resources.
- A host database server must be very secure and will need a backup server for redundancy.

### 6.2 Conclusions re. firewall models:-

- Role for dynamic firewall may be as application firewall on gatekeeper.

## 7. CLOSING DISCUSSION

In the closing plenary discussion session, the following points were re-emphasised:

7.1 There must be a clear assignment of responsibility to, and acceptance of responsibility, by system administrators of resources attached to the Grid and they must be made aware of the issues and risks associated with the Grid.

7.2 There is a distinction between network firewalls protecting a site (strategically important and relatively static) and host-based firewalls running on Grid resources (potentially more dynamic).

7.3 A question which needs to be addressed is whether each site should aim to provide a dedicated gatekeeper system?

7.4 The DNS system should be examined as a possible basis for implementing a trusted source of Grid IP addresses.

7.5 There must be very clear and documented guidelines developed for how a secure Grid IP address host operates.

7.6 Clients are seen as a weak link in the Grid security framework and sites may be unwilling to provide access for them without knowledge of their security credentials.

## 8. GENERAL RECOMMENDATIONS

After a wide ranging discussion, the following recommendations were made:-

**8.1 The trusted host (clique) server is acceptable to most sites as a short term (but not scalable) mechanism for configuring host-based firewalls, but it must be securely managed and accessed, and must be maintained up to date.**

**8.2 An initial step will be to download to each site participating in the Level 2 Grid a file containing a list of IP addresses and port ranges in order to make rapid progress towards the implementation of the trusted host solution; this will separate two components of the task: the deployment of the firewall within Institutions from the development of the remote database from which the information is downloaded.**

**8.3 The dynamic firewall may be of interest as a more scalable and potentially more secure host-based firewall mechanism in some situations.**

**8.4 The hybrid host (with static IP addresses) and dynamic firewall solution may be useful for getting operational quickly.**

**8.5 The VPN firewall is a longer term possibility building on off-the-shelf technology, but is not a widely acceptable solution at the present time mainly because of interoperability issues between the current VPN solutions.**

## 9. ACKNOWLEDGEMENTS

The organisers wish to thank:

- those who gave presentations at the meeting;
- those who led the discussion groups and recorded the discussions;
- those who participated in the meeting and thereby helped to move forwards our understanding of how build a successful UK e-Science Grid;
- the team at the National e-Science Centre for hosting the event and for providing excellent support for the organisers and nourishment for the participants.