Charter for FVGA-WG
Date 2008-09-02

Group Abbreviation:
fvga-wg

Group Name:
Firewall Virtualization for Grid Applications - Working Group

Area:
Infrastructure

Group Leadership:

tbd	Ralph Niederberger	Chair
tbd	Thijs Metsch	Chair
tbd	Inder Monga	Chair

Group Summary:
Grid Computing expounds the 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. As grids move towards forming dynamic, seamless Virtual Organizations (VOs) using distributed resources, they require application driven transport privileges from the network. Pre-existing security policies within the network such as in firewalls, network address translators, application level gateways, VPN style gateways etc. tend to interfere with these new applications and the VO formation, and usually require an administrator/manual intervention to work.

The Firewall Issues research group (fi-rg) has documented the use cases and classified the issues that Grid applications experience when trying to traverse and/or control data transport policy enforcement devices (GFD.83). The group is also in process of publishing a document that analyzes and categorizes new firewall protocols, architectures and on-demand frameworks.

This working group will leverage the application requirements from the FI-RG to standardize a set of service definitions for a virtualized control interface into firewalls and other midboxes allowing the grid applications to securely and dynamically request application/workflow-specific services from those devices, for the duration of the service.

Charter Focus / Purpose and Scope:

The research-group findings indicate that the dynamic nature of Grid VO formation, policy-driven grid resource management and scheduling are best served with a grid application-driven firewall service. The purpose of the firewall virtualization working group is to produce the following standards:

1. A standard set of service definitions that provide an abstract interface for an authorized grid applications to specify its data-path traversal requirements.
2. 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

3. A best practices document for the network-administrator and a grid-administrator to understand the architecture and security implications of this deployment

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.

Goals / Deliverables:

The goal of the firewall virtualization working group is to produce the following standards:

1. A standard set of service definitions that provide an abstract interface for an authorized grid applications to specify its data-path traversal requirements. This includes:
   Port opening service
   Port closing service
   Data Plane and Service Plane interactions
   Requests from within the security domain
   Requests from outside the security domain

2. 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

3. A best practices document for the network-administrator and a grid-administrator to understand the architecture and security implications of this deployment

   This includes:
   Deployment scenarios and use-cases
   Interactions between various Grid components
   Examples of successful prototype deployments

Timeline

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 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.

Exit Strategy:
The work of the FVGA-WG will be deemed complete when all the documents proposed are completed and a couple of prototype implementations exist in the Grid community that validate the architecture and the standard.

Abstract:
Grid Computing expounds the 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. As grids move towards forming dynamic, seamless Virtual Organizations (VOs) using distributed resources, they require application driven transport privileges from the network. Pre-existing security policies within the network such as in firewalls, network address translators, application level gateways, VPN style gateways etc. tend to interfere with these new applications and the VO formation, and usually require an administrator/manual intervention to work. The aim of this working group is to abstract and virtualize the complexity of Firewall control while still maintaining the security requirements of the Grid Infrastructure.

Type: Select Document Type...

Milestone	Date (YYYY-MM)	Completed?	Completed Date (YYYY-MM)
First Draft Public Comment			
Publication			

Type: Select Document Type...

Milestone	Date (YYYY-MM)	Completed?	Completed Date (YYYY-MM)
First Draft Public Comment			
Publication			

Seven Questions:

1. Is the scope of the proposed group sufficiently focused?
Yes. We will define and standardize a protocol which describes a secure way for application programmers to request dynamically access through Firewalls and other midboxes after they have been successful authenticated and authorization has been checked. The access will be granted for a negotiated and restricted time only.

2. Are the topics that the group plans to address clear and relevant for the Grid research, development, industrial, implementation, and/or application user community?
Yes. The problems grid applications have with firewalls are addressed in two documents prepared by the OGF FI-RG. The second one is in public comment currently. This document has shown the pitfalls which cannot be solved by currently available protocols. The lack of services available, i.e. dynamic

and secure opening of firewall ports for Grid applications, will be closed by the work of this OGF working group.

3. Will the formation of the group foster (consensus-based) work that would not be done otherwise?

Yes. IETF is working on midboxes since several years, but has not come up with appropriate solutions yet. The scope the new OGF working group will have, will fill this gap of services.

4. Do the group's activities overlap inappropriately with those of another OGF group or to a group active in another organization such as IETF or W3C?

No. As explained in 3 IETF workgroups do not address appropriate solutions. Of course, the OGF FVGA-WG will use work already address in other groups, i.e. authentication and authorization protocols standardized in OGF can be used.

5. Are there sufficient interest and expertise in the group's topic, with at least several people willing to expend the effort that is likely to produce significant results over time?

Yes. We have addressed this issue in the FI-RG and got a lot of feedback and interest in working with our future group.

6. Does a base of interested consumers (e.g., application developers, Grid system implementers, industry partners, end-users) appear to exist for the planned work?

Yes. Any application using dynamic ports for applications communicating between firewall separated systems will benefit from this work.

7. Does the OGF have a reasonable role to play in the determination of the technology?

Yes. As described above, it is of great interest for Grid applications to communicate in a secure manner. Ports should be opened automatically at any time when requested by authorized applications/users and only as long as they are required. Normally this cannot be realized by firewall administrators just in time and on a 24/7 basis (24 hours, 7 days a week).

Group Status:

Established

Public Description (for print & web site):