Network gateway security method for enterprise Grid: a literature review

A Sujarwo¹, J Tan²

¹Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia
²Faculty of Information Technology, Monash University, Caulfield, Australia

E-mail: ari.sujarwo@uii.ac.id, jefferson.tan@monash.edu

Abstract. The computational Grid has brought big computational resources closer to scientists. It enables people to do a large computational job anytime and anywhere without any physical border anymore. However, the massive and spread of computer participants either as user or computational provider arise problems in security. The challenge is on how the security system, especially the one which filters data in the gateway could works in flexibility depends on the registered Grid participants. This paper surveys what people have done to approach this challenge, in order to find the better and new method for enterprise Grid. The findings of this paper is the dynamically controlled enterprise firewall to secure the Grid resources from unwanted connections with a new firewall controlling method and components.

1. Introduction

A computational Grid is a facility for people to do massive computing over a uniformly shaped infrastructure of diverse resources [1]. Many resources from network-connected physical or virtual computers work together within the Grid infrastructure to provide a massive system. This system is designed to process multiple jobs that need intensive computation. Certain protocols are used to organize many computational nodes and facilitate the hosting of jobs that are submitted into them.

As a massive system that consists of various parts such as computational components, shared storage and many other components, Grid infrastructures are requiring advanced security. Some of the Grid resource components and data are potential for attack. The sensitive data and the computation resources must be secured properly to avoid unauthorized access. As an example, Foster and Kesselmen [2] explained in his book that computational and experimental scientists and engineers use the Grid to support their works. Data are saved and processed within the Grid resources. When these data are not secured properly, it could attract unauthorized people to access and possibly spread restricted information. In certain cases, the consequences of this issue could be damaging. Some requirements are already specified to provide basic and advanced security to this infrastructure to achieve better security for it.

2. Grid Protocols

Grid resources is controlled by the function of each Grid protocol layer. [3] defined the protocol stack of a Grid architecture that is shown in the left hand side of Figure 1, Grid consists of five layers: fabric, connectivity, resource, collective, and application.
The functionality of each layer related to the Internet Protocol (IP) architecture in the right hand side of Figure 1. The Fabric layer consists of resources owned by each node such as storage and computational resources that are shared within Grids. All of them are then interconnected using a Grid protocol. In regard to the IP architecture, the fabric layer related to the IP link layer in terms of providing the necessary hardware to be used by the upper layer. Among all of those layers, the Grid middleware such as Globus located in two layers, which is the Connectivity layer and the Resource layer [5]. These layers are closely related on how the Grid middleware provides the security and resource management of the Grid.

3. The Challenge
The Grid has characteristics that is called “the nature of the Grid” [3] which is the characteristics of users, resources, policies, and other components of a Grid. Each of those components tends to be dynamic. The number of users and organizations joining Gris as Resource Provider can be changing all the time. User at any time can join and submit a certain task. The Grid infrastructure scopes are typically wide. It could be within a university, group of the education system, or it could be extensive for certain purposes. The users could come from worldwide. As long they have an access to the node joining the Grid, they would able to run any tasks, anytime, anywhere. Furthermore, the number of resources can vary. A real organization is possible to add or withdraw its resources from a Grid. Sometimes the participating resources facing a problem and need to be turned off, it makes the number of resources possible to change.

While requesting a resource, users are likely to be assigned to an available resource and need a certain amount of time to submit tasks, distribute the data among nodes and the execution of the tasks. It creates a variable time between each task in regards to starting time and ending time. So the requirements of the Grid resources are likely to vary and make the computation cycle more dynamic. The nature of Grid mentioned above brings a consequence in term of security. The security system must be able to overcome the Grid infrastructure requirements to keep Grid running well without compromising the whole system security.

4. Basic Grid Security
The Grid Security Infrastructure (GSI) is an integrated security system for Globus which provides the basic security infrastructures for Grids [6]. The GSI mainly focus on the phase of user verification [7]. The user verification is the primary security function that Grids must have to identify users and offer services to users. Based on [8], the basic security of a Grid requires Security Policy as necessary rules to define the involved objects to the Grid. The inter-organization security that covers the security among different organizations either internal or external. There is no doubt that disruption can come from anywhere even from internal organization. Grids also need a larger security system to protect from external disruption. Authentication and authorization mechanism are designed with properties that all of the Grid components remain safe and running properly. These are two Grid’s basic security: Grid User Credentials – The X.509v3 Certificate and Proxy Certificate for Single Sign-on (Figure 2).
5. Approaches

The explanation about the Grid architecture and the basic security of a Grid system gave a clear understanding that the Grid needs more advanced security system. Many security schemes are invented for a common network and server, such as the authentication system and the firewall. The useful way to protect a Grid is separating the Grid infrastructure from the public network and placing the Grid system behind a firewall. Newman [9] have defined the firewall as an entity that has a right to enforce rules to make a decision on passing data over a network. The firewalls are applied to filter all incoming and outgoing data to the Grid. However, the nature of firewalls is static. Static firewalls need administrators to add or remove the firewall rules. This nature of the firewalls is contradicted with the nature of Grid which is dynamic.

The Grid needs several ports to be opened in order to operate. The needed ports are depending on each user’s requirements. To allow a user to access the Grid, certain firewall rules are added to the firewall. Since the firewall is not controlled all the time, it makes rules stay active on the firewall longer until the administrators change or remove the rules. The unused ports remain accessible for a long time; this situation makes the Grid infrastructure more vulnerable. To overcome this problem, scientists and researchers have tried to find out the better way to operate a Grid in a firewalled area with the integration of the currently invented security scheme. There are two approach to overcome this problem: Proxy mechanism and dynamic firewall.

5.1. Proxy Mechanism for Firewall Traversal

The concept of proxy mechanism is by operating a currently opened firewall ports to establish a new connection between the users and resources [10]. An application sits between the users and the Grid infrastructure to accept the user’s connection, receive data, and forward it to the Grid. The following explains several methods on how the proxy mechanism works to move data through the firewall. Metsch [11] explained Generic Connection Brokering (GCB) as a the first technique to enable data passing firewall by relaying the data packets between the users and the Grid. As shown in Figure 3, the left hand side is the initiating party (could be an external network). It sends data to a relay point which is a GCB broker. The broker then makes a decision to allow or reject the connection based on the firewall rules. When the connection is allowed, the GCB then negotiates a connection to the Grid infrastructure, and let the Grid to send a reply to the client through a relay point.

![Figure 3 GCB Architecture](image1)

![Figure 4 Remus Diagram](image2)

Considering to this project design which avoids an excessive change to the Grid infrastructure or the client’s application, the GCB is not an appropriate approach to be applied in this project. The GCB needs a modification either in the Grid infrastructure and the client to insert a GCB layer. This layer is a library that is invoked when the application wants to send a message to the GCB broker[11].

The second technique called Remus. Rerouting and multiplexing system are the way Remus works. [13] created Remus to pass data across a firewall by operating the currently registered port within a firewall. All data are wrapped as new packets addressed with port numbers that are open in the firewall. The Remus diagram is shown in Figure 4. Remus approach requires data to be processed in additional processes. The data are encapsulated several times to be able to pass the tunnel. [12] explained that this process increases the size of the data, and makes data heavy enough to be transferred. The Remus is not suitable for this project implementation model caused by the heavy data size, but it gives an understanding that the proxy and tunnel mode put a large data overhead to be able to traverse a firewall.
5.2. Dynamic Firewall

Another approach to traverse a firewall besides proxy mode is by managing a firewall and makes a firewall more dynamic to modify the rules without any administrator intervention. This method enables a firewall to alter its rules when user is successfully authenticated such as Cooperative On-Demand Opening (CODO)—a method to change firewall rules based on user request, Dyna-fire—works by the knocking mechanism, Firewall Traversal Protocol (FiTP), and Romulus. Cooperative On-Demand Opening (CODO) works by planting a CODO agent inside the firewall [11]. This is called the CODOfirewall agent (FA). CODO also requires a CODO client library (CL) to be integrated in each of user’s application that wants to pass through a firewall [14] as shown in Figure 5.

![Figure 5 CODO: Cooperative On Demand Opening, borrowed from [14]](image)

![Figure 6 Dyna-fire port knocking, borrowed from [15]](image)

The CODO needs its agent installed within the communicating devices. For certain systems, it would not be feasible to add an application to it. Rewriting all the client’s application and the Grid infrastructure is not a simple matter, so another approach with a simpler solution is required. Almost the same with CODO, Dyna-Fire uses knocking to open a firewall port. It needs the Dyna-fire daemon to be installed within a firewall. [15] explained that four aspects must be fulfilled to be allowed to pass data: client must encrypt the knock in a right encryption method; client must ensure that the format of knocks sequence is right; client must use registered IP address; and a valid user’s identity must be presented. A set of firewall rules are be added to open firewall ports after the client fulfils those requirements as shown in Figure 6. However, a problem with Dyna-fire is that the Dyna-fire is possible to be attacked with a replay and a man-in-the-middle attack [11]. The next approach is called Firewall Traversal Protocol (FiTP) released by Firewall Virtualization for Grid Applications – Working Group (FVGA-WG), a group that works focus on proposing a security solution for a Grid based on the current firewall filtering system. The FiTP plan was introduced in 2009 [16]. Up to today, there is no developed protocol that manages a firewall directly to make a firewall aware of what kind of application data needs to traverse the firewall. The FiTP is proposed to be a protocol that has such ability. The FiTP diagram is shown in Figure 7.

![Figure 7 FiTP diagram, borrowed from [17]](image)

![Figure 8 Romulus pinhole request process, borrowed from [13]](image)
Since FiTP has not been done, [18] introducing Romulus as a controller to open and close firewall with the use of agent. The firewall agent has a right to accept a request sent by users or reject the request if it does not satisfy the security requirements. It runs a security procedure to ensure the incoming message was sent from a valid user. It authenticates user based on the validity of the use certificate [13] as shown in Figure 8. [13] implemented the Romulus in two type of firewalls: a Linux IPTables and a Cisco router Access Control Lists (ACL). For a larger scope, based on research done by [19], IPTables do not have the capabilities to check all the incoming packet coming from a large network due to a hardware and software constraints of the PC firewall. The implementation of the IPTables and the Cisco ACL as the additional security system within a Grid infrastructure could make Grid running underneath the performance standard due to the capability constraints in both of those firewalls. To avoid the potential problem, the Grid infrastructure supposed to use a professional stand-alone firewall [20] as the enterprise security.

6. Evaluation and Conclusion
The Grid infrastructure interconnects computers to cooperate in such a way to finish tasks submitted to the Grid. As a large system comprises of components, the Grid needs an advanced additional security system. The firewall proposed as an additional security system to filter all the incoming data. The firewall becomes the potential security system for a Grid. However, some issues such as the static rules of the firewall could arise security vulnerability for Grid. The Romulus could be a model of the firewall controlling method for enterprise Grid infrastructure. The method used by Romulus that is called firewall virtualization, could be extended with the use of authentication, authorization, and accounting to give a more flexible credential checking to ensure the accessing party is a valid one.

References
[1] Foster I, Zhao Y, Raicu I and Lu S 2008 Cloud Computing and Grid Computing 360-Degree Compared 2008 Grid Comput. Environ. Work. pp. 1–10.
[2] Foster I and Kesselman C 2003 The Grid 2: Blueprint for a new computing infrastructure (Elsevier).
[3] Foster I, Kesselman C and Tuecke S 2001 The anatomy of the grid: Enabling scalable virtual organizations Int. J. High Perform. Comput. Appl. vol. 15 no. 3 pp. 200–22.
[4] Welch V, Foster I, Kesselman C, Mulmo O, Pearlman L, Tuelce S, Gawor J, Meder S and Siebenlist F 2004 X. 509 proxy certificates for dynamic delegation in 3rd annual PKI R&D workshop vol. 14.
[5] Foster I 2003 The grid: A new infrastructure for 21st century science Grid Comput. Mak. Glob. Infrastruct. a Real. pp. 51–63.
[6] Butler R, Welch V, Engert D, Foster I, Tuecke S, Volmer J and Kesselman C 2000 A national-scale authentication infrastructure Computer (Long. Beach. Calif). vol. 33 no. 12 pp. 60–6.
[7] Foster I and Kesselman C 1999 The Globus project: A status report Futur. Gener. Comput. Syst. vol. 15 no. 5 pp. 607–21.
[8] Foster I, Kesselman C, Tsudik G, and Tuecke S 1998 A security architecture for computational grids in Proceedings of the 5th ACM conference on Computer and communications security pp. 83–92.
[9] Newman D 1999 Benchmarking terminology for firewall performance.
[10] Mahjoubi P 2010 RADIUS-based Firewall Virtualization for Grids (Monash University).
[11] Metsch G I T, Gommans F R L, de Smet A, Volpato G L, and LUH R 2010 Requirements on operating Grids in Firewalled Environments.
[12] Tan J, Abramson D and Enticott C 2009 REMUS: a rerouting and multiplexing system for Grid connectivity across firewalls J. Grid Comput. vol. 7 no. 1 pp. 25–50.
[13] Tan J, Abramson D and Enticott C 2009 A virtual connectivity layer for grids in Fifth IEEE International Conference on e-Science pp. 307–12.
[14] Son S, Alcock B and Livny 2005 M Codo: Firewall traversal by cooperative on-demand opening in Proceedings. 14th IEEE International Symposium on High Performance Distributed Computing HPDC-14 pp. 233–42.

[15] Green M L, Gallo S M and Miller R 2004 Grid-enabled virtual organization based dynamic firewall in Proceedings of the 5th IEEE/ACM International Workshop on Grid Computing pp. 208–216.

[16] Niederberger R 2009 FiTP-A protocol draft for dynamic opening of Firewalls in 25th Open Grid Forum (OGF25).

[17] Niederberger R, Monga I and Metsch T 2008 Firewall Virtualization for Grid Applications in Open Grid Forum - OGF23 (Barcelona).

[18] Tan J, Abramson D, and Enticott C 2010 Firewall Traversal in the Grid Architecture in 12th IEEE International Conference on High Performance Computing and Communications (HPCC) pp. 189–96.

[19] Ranganath V P and Andresen D 2003 A set-based approach to packet classification in Proceedings of the IASTED International Conference on Parallel and Distributed Computing and Systems pp. 889–94.

[20] Thomason S 2012 Improving Network Security: Next Generation Firewalls and Advanced Packet Inspection Devices GJCST-E Network, Web Secur. vol. 12 no. 13.