OLLE MULMO AND VON WELCH

Using the Globus Toolkit® with Firewalls

As discussed in the previous *On the Grid* columns, one activity that Grids must allow is the coordination of resources not subject to central control. In practice, this means that resources distributed across different sites on the Internet, which often have firewalls in between. In this article, we discuss the use of the Globus Toolkit for Grid computing in the presence of firewalls, explaining what the issues are and what can be done to address them.

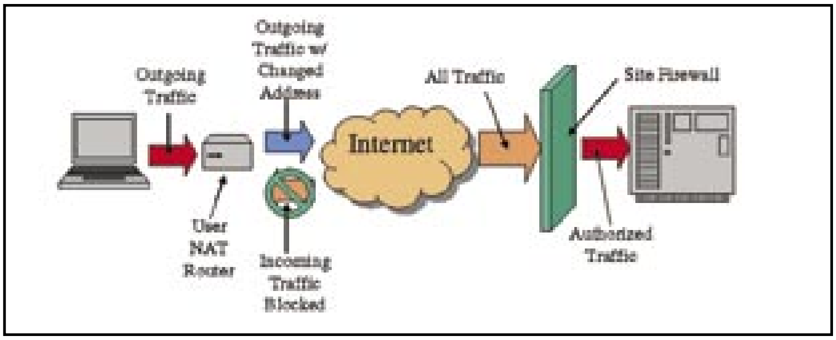

FIGURE ONE **A common scenario showing two typical types of firewalls. A user, on the left, has a gateway router in his house that is blocking incoming connections. On the right, a site has a firewall that allows only authorized traffic to enter the site.**

What is a Firewall?

First we should discuss what we mean by a *firewall*. Generically speaking, a firewall is a system that allows some wanted stuff to pass through, while keeping out unwanted stuff (like fire). In terms of this article, a firewall is a device on the network that allows some traffic to pass through while blocking other traffic.

Many firewalls filter traffic based on the source or destination of the traffic. All traffic on the Internet, like postal mail, carries a header that contains a pair of addresses: one for the recipient and another for the sender (so that the recipient knows where to send a response).

These addresses identify not only the computer but also a port number, which specifies the application for which the traffic is destined or from which it is being sent.

By filtering incoming traffic based on the recipient address in the message header, a firewall allows only traffic that is destined for specific and approved applications, such as Web and mail servers. High-end firewalls may inspect the message payload as well, in order to catch foul play, making sure the messages are not malformed or don't carry viruses. Firewalls may also filter messages based on the address of packet sender, to allow only traffic from authorized clients (it is possible to fake source addresses on the Internet, however, so this is not 100 percent reliable).

Less sophisticated devices may also act as firewalls but aren't commonly called firewalls. One common example is gateway routers that are sold to consumers. These permit multiple computers to share a single Internet connection, such as a cable modem or DSL line, by changing addresses in the outgoing traffic to permit this sharing (this technique is called NAT, or Network Address Translation). In addition, they typically block incoming network connections. For simplicity, we include such devices in our definition of firewall.

When Grids Meet Firewalls?

Let us now consider the issues that arise when trying to run a Grid in the presence of a firewall. Although we focus in this article specifically on the Globus Toolkit (GT), the first issue is common with almost any new services a site may install: they need to be accessible through a firewall. GT consists of several services, including MDS (Monitoring and Discovery Service), which allows for information discovery; GridFTP, which allows for data movement; and GRAM (Grid Resource Allocation and Management), which allows for resource management. The services listen on a set of well-known ports for incoming connections; hence, if a site wants to make these services available outside a firewall, that firewall must pass traffic on these ports.

> Generically speaking, a firewall is a system that allows some wanted stuff to pass through, while keeping out unwanted stuff (like fire).

A second issue that arises with GT is that it provides the coordination of dynamic resources, namely, user processes. When a user sets the GRAM system to run a process on a (remote) computer, GRAM creates a subservice, called a Job Manager, that lets the user monitor and control the process. For example, the user can register a callback URL with the Job Manager that is used to inform the user of state changes in the monitored process. This feature results in a network connection from the Job Manager to the user when the job completes, informing the user of that fact and providing the exit status of the job.

TABLE ONE

Default Ports Needed for GT2 and GT3 Services

SERVICE	GT2	GT3
GRAM	2119 (1,2)	8080 (2)
MDS	2135	8080
GridFTP	2811 (1,2)	2811 (1,2)

Default ports needed for GT2 and GT3 services. All ports are TCP ports. (1) Additional ports are dynamically assigned by the created user processes. (2) Application is sensitive to NAT translation.

This Job Manager functionality means that network connections are made from the site running GT back to the user. This situation may raise issues if the site's firewall doesn't allow for outbound connections or if the user has a firewall. Further complications may arise because the ports used for the callbacks are dynamically assigned by the client's operating system and not known ahead of time. Depending on the version of GT, which we will discuss in the following section, new ports may be dynamically assigned on the Job Manager side as well.

GridFTP exhibits the same problem. When a data transfer is initiated, additional ports, called data channels, are dynamically assigned to the user process, and the bulk data transfers are made on those ports. A user may start multiple parallel data channels or orchestrate a third-party transfer by creating a user processes at two different remote sites and have them initiate direct data channels between themselves.

A third issue is encountered when using NAT (Network Address Translation). GT uses the callback paradigm to allow asynchronous communication; that is, a client will send an address and port to a service and then wait for a connection back from the service. Examples are clients registering callbacks with Job Managers so they can be informed when their jobs complete or when a new data channel connection is established in GridFTP. When traffic from clients is crossing a firewall that uses NAT, the address that a client believes to be his address is different from the address that appears in the outgoing traffic because of the changes made by the NAT process. As a result, connections back to the client using the given address are sent to the wrong place and never arrive.

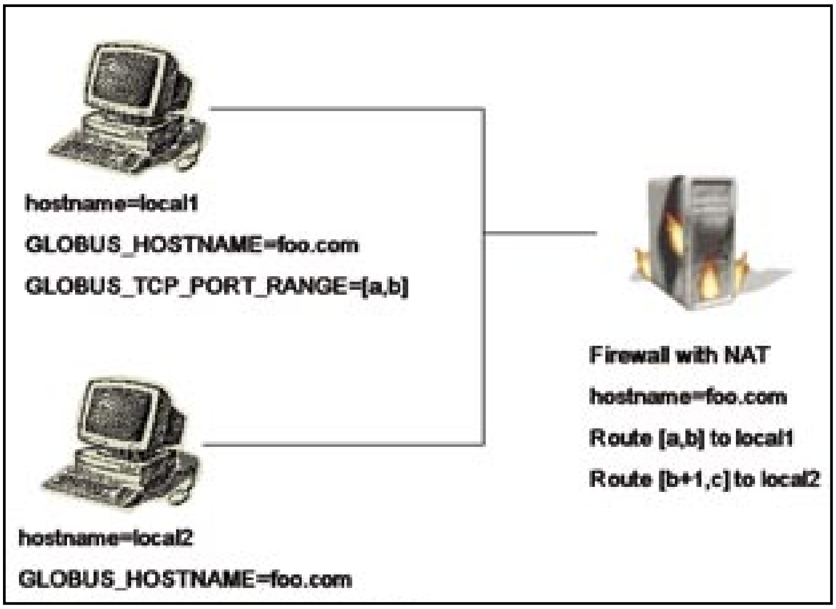

FIGURE TWO Environment variables and firewall rules necessary to make Globus Toolkit work behind a firewall that is using NAT.

Playing Nice

Fortunately, there do exist solutions to the issues described in the previous section. Here we summarize some of the information available at www.globus.org/security/firewalls site.

First, we need to distinguish between two versions of the Globus Toolkit. Version 2 (GT2) has been around for several years and is used in a number of production Grids today. Version 3 (GT3) is relatively new and is based on industry standard Web services technologies and the Open Grid Services Infrastructure (OGSI) standards. While these versions are similar architecturally (both have GRAM, MDS, GridFTP), their network traffic characteristics differ.

For the three basic services, GRAM, MDS, and GridFTP, Table 1 describes the network ports that these services use and need to be allowed into a site in order to give users access to those services.

In addition to these services, the Job Manager and GridFTP request that a range of ports in the untrusted ephemeral range (port numbers greater than 1024) be open. If the firewall blocks ports in this range (many don't), then a range must be opened, and the environment variable GLOBUS_TCP_PORT_RANGE must be set so that all ports dynamically assigned by Globus Toolkit services fall into the opened range. The exact size of the opened range will depend on the exact usage of the system, but a good rule of thumb is ten ports per simultaneous user. Note that in GT3, the Job Manager uses the same port (default 8080) as the GRAM server, so the ephemeral port range is required only for the GridFTP service.

A Client Behind a Firewall

A user behind a firewall can use GT. In order to permit this, the firewall needs to allow a port range for callback connections from the GRAM service. This range should be opened as described in the previous section and the GLOBUS_TCP_PORT_RANGE variable set in the user's environment.

If the user is behind a firewall doing NAT, the user will also need to set the environment variable GLOBUS_HOSTNAME to the external address of the firewall and configure the firewall to pass incoming connections in the port range specified by GLOBUS_TCP_PORT_RANGE through to his computer. Note that while this works with GT2, support for GLOBUS_HOSTNAME is still pending in GT3 at the time of this writing.

Most NAT devices are capable of translating the port numbers as well. Currently, however, GT does not have this capability, and therefore the port number on the internal machine on which a particular service is listening must be the same as on the external interface of the firewall. Thus, in the case of multiple machines behind a single NAT device, each machine must have a unique port range defined, and those ports must be forwarded to the appropriate machine by the firewall. (GLOBUS_HOSTNAME will be the same for all the machines, however.)

Resources

Globus Firewall Requirements

- www.globus.org/security/firewalls/

A Brief Taxonomy of Firewalls /Great Walls of Fire, SAMS Institute, 2002.

- www.giac.org/practical/gsec/Gary_Smith_GSEC.pdf

Future Directions

We hope that the leveraging of Web services protocols will enable firewalls that more intelligently allow traffic and relieve users of having to administer them manually. For example, with traffic being carried in self-describing, digitally signed XML messages, a router can easily parse and check the signature that authenticates the sender and open ports based on the result of such a validation.

This work was supported in part by the Mathematical, Information, and Computational Sciences Division subprogram of the Office of Advanced Scientific Computing Research, Office of Science, U.S. Department of Energy, under Contract W-31-109-ENG-38 and under Contract DE-AC03-76SF0098 with the University of California; by the National Science Foundation; by the NASA Information Power Grid program; and by IBM.

Information in this article was developed through the DOE Science Grid.

Globus Toolkit is a registered trademark held by the University of Chicago.

Von Welch is a security researcher at the National Center for Supercomputing Applications where he works on Grid Security and contributes to the Globus Toolkit security architecture.

Olle Mulmo is an applications expert at the Swedish Royal Institute for Technology, where he works on Grid Security in national, Nordic, and European research and development projects and contributes to the Globus Toolkit architecture.

NAT and Clusters

NAT (Network Address Translation) or IP Masquerading can be useful to clusters. If you enable NAT on the head (or gateway node), the cluster nodes can effectively communicate with the outside world. This enhancements allows nodes to access the Internet and even use NFS servers that only viewable to the head node. NAT only needs to be enables on the head node. The compute nodes only need to have their default route pointing to the head node. You can find more about NAT from the Masquerade HOWTO *www.tldp.org/HOWTO/IP-Masquerade-HOWTO.*