Firewall Configuration Information for AGTk 2.0

Author: Ivan R. Judson
Status: Draft
Contact: ag-info@mcs.anl.gov

Date: 04-12-2003

Abstract

This document specifies what firewall configuration options need to be considered to use the Access Grid in a firewalled network environment. Specific firewall solutions are not addressed in this document.

Copyright

Discussion

The Access Grid Toolkit provides distributed collaboration system with parts that communicate over both the local area and wide area network. In order to function properly the various parts of the system need to be able to initiate and use network connections in various directions (both incoming and outgoing). When the term connection is used it is meant to mean a GSI Secured TCP Socket.

For the streaming media, which is carried via RTP, two ports are required. The first (even numbered) port is the data port, the next odd port (first port + 1) is used for RTP Control data.

In the current version of the toolkit, the network interfaces are served via SOAP. These interfaces are exposed on:

Service	**Default Port(s)**
Services	dynamically assigned
Service Manager	11000
Node Service	12000 and 1 dynamically assigned
Venue Client [*]	*optional* 1 dynamically assigned
Venue Server	8000, 8002, 8004, 8006
Bridge Server	Each stream is statically configured or dynamically assigned
Beacon Server	(233.4.200.21, 10002/10004), beacon.dast.nlanr.net:10004

The following services need special configuration to operate correctly.

Service	**Default Port(s)**
Venue Client	*optional* 1 dynamically assigned
Venue Server	8000, 8002, 8004, 8006
Bridge Server	Each stream is statically configured or dynamically assigned
Beacon Server	(233.4.200.21, 10002/10004), beacon.dast.nlanr.net:10004

These services make no *wide area* network connections, but do require any firewall on the local machine be configured appropriately [†].

Service	Default Port(s)
Services	none
Service Manager	11000
Node Service	12000 and 1 dynamically assigned

Service Details

- Venue Server (defaults to port 8000, 8002, 8004, 8006)

  The venue server listens for incoming connections on four ports, which are configurable. These ports are for incoming connections only, there are no outbound connections from the venue server.

- Bridge Server (multiple ports used)

  The bridge server can use either statically assigned ports for the media bridges it starts, or it can dynamically assign the ports for media bridges.

- Beacon Server (one group, one outgoing connection)

  The beacon server uses one multicast group and one outbound connection to a reporting server. These are both configurable, but the defaults are the correct configuration to be a part of the Access Grid Multicast Beacon infrastructure.

Multicast

In order for audio and video to flow among users multicast needs to be able to be allowed through the firewall. There is currently no set of static configurations that are used for multicast (although they could be used, if needed), so ideally the firewall would allow data from any group *that is subscribed to from inside* the firewall to come through the firewall from the outside.

The media tools we use have two different behaviors for how they send data. For audio the source port for the data is identical to the destination port for the data. For video, the source port for the data is selected randomly.

Example of a Secured Static Environment

This is an example of a small installation configured for a paranoid network configuration. The configuration has only three venues to keep the example simple.

To keep this example even more simple, the bridge, data and venue server are all running on the same machine, *host.domain*.

Meeting Room Venue

Media	Multicast Groups	Bridge Ports
static video	224.1.2.3/[1234/1235]	9000/9001
static audio	224.1.2.3/[1236/1237]	9002/9003

Laboratory #1 Venue

Media	Multicast Groups	Bridge Ports
static video	224.1.2.4/[1234/1235]	9004/9005
static audio	224.1.2.4/[1236/1237]	9006/9007

Laboratory #2 Venue

[*] Disabling incoming connections to the Venue Client is possible and doesn't significantly hinder collaboration. Personal data sharing is not possible if incoming connections are not allowed.

Media	Multicast Groups	Bridge Ports
static video	224.1.2.5/[1234/1235]	9008/9009
static audio	224.1.2.5/[1236/1237]	9010/9011

Venue Server

- running on host.domain
- ports: 8000, 8002, 8004, 8006

If the firewall is configured to allow multicast through, then

Bridge Server

- running on host.domain
- ports: 9000-9011

otherwise,

Bridge Server

- running on some host with working multicast
- ports: 9000-9011

Beacon Service

- running on host.domain
- Multicast Group: (233.4.200.21, 10002/10004)
- Outbound TCP: beacon.dast.nlanr.net:10004

Summary Configuration

Incoming **to host.domain** from the rest of the world:

- *Ports:* 8000, 8002, 8004, 8006
- If Bridge Server is **inside the firewall**: 9000-9011

Outgoing Conduits **from host.domain** to the rest of the world:

- beacon.dast.nlanr.net:10004
- If Bridge Server is **outside the firewall**: bridgehost.domain:9000-9011

Multicast Group Conduits:
All hosts on the local network should be able to send and receive traffic via these multicast groups.

- (224.1.2.3,1234)
- (224.1.2.3,1235)
- (224.1.2.3,1236)
- (224.1.2.3,1237)
- (224.1.2.4,1234)
- (224.1.2.4,1235)
- (224.1.2.4,1236)

- (224.1.2.4,1237)
- (224.1.2.5,1234)
- (224.1.2.5,1235)
- (224.1.2.5,1236)
- (224.1.2.5,1237)
- (233.4.200.21, 10002)
- (233.4.200.21, 10004)

Conclusion

This document describes the firewall requirements for the AGTk 2.0 software, for both clients and services. For more information please see:

- The AGTk Home Page
- The Access Grid Project Home Page
- The Access Grid Documentation Project Home Page