Environmental Systems Research Institute, Inc., 380 New York St., Redlands, CA 92373-8100 USA • TEL 909-793-2853 • FAX 909-307-3014

ESRI Systems Integration Technical Brief

Identifying Firewall TCP Server Ports In a Enterprise ArcIMS Configuration

Technical Brief
Rev 2. March 17, 2004

Copyright © 2003 ESRI
All rights reserved.
Printed in the United States of America.

The information contained in this document is the exclusive property of ESRI. This work is protected under United States copyright law and other international copyright treaties and conventions. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system, except as expressly permitted in writing by ESRI. All requests should be sent to Attention: Contracts Manager, ESRI, 380 New York Street, Redlands, CA 92373-8100, USA.

The information contained in this document is subject to change without notice.

U.S. GOVERNMENT RESTRICTED/LIMITED RIGHTS

Any software, documentation, and/or data delivered hereunder is subject to the terms of the License Agreement. In no event shall the U.S. Government acquire greater than RESTRICTED/LIMITED RIGHTS. At a minimum, use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in FAR §52.227-14 Alternates I, II, and III (JUN 1987); FAR §52.227-19 (JUN 1987) and/or FAR §12.211/12.212 (Commercial Technical Data/Computer Software); and DFARS §252.227-7015 (NOV 1995) (Technical Data) and/or DFARS §227.7202 (Computer Software), as applicable. Contractor/Manufacturer is ESRI, 380 New York Street, Redlands, CA 92373-8100, USA.

@esri.com, 3D Analyst, ADF, AML, ARC/INFO, ArcAtlas, ArcCAD, ArcCatalog, ArcCOGO, ArcData, ArcDoc, ArcEdit, ArcEditor, ArcEurope, ArcExplorer, ArcExpress, ArcFM, ArcGIS, ArcGrid, ArcIMS, ArcInfo Librarian, ArcInfo, ArcInfo—Professional GIS, ArcInfo—The World's GIS, ArcLogistics, ArcMap, ArcNetwork, *ArcNews,* ArcObjects, ArcOpen, ArcPad, ArcPlot, ArcPress, ArcQuest, ArcReader, ArcScan, ArcScene, ArcSchool, ArcSDE, ArcSdl, ArcStorm, ArcSurvey, ArcTIN, ArcToolbox, ArcTools, ArcUSA, *ArcUser,* ArcView, ArcVoyager, *ArcWatch,* ArcWeb, ArcWorld, Atlas GIS, AtlasWare, Avenue, *Business*MAP, Database Integrator, DBI Kit, ESRI, ESRI—Team GIS, ESRI—The GIS People, FormEdit, Geographic Design System, Geography Matters, Geography Network, GIS by ESRI, GIS Day, GIS for Everyone, GISData Server, *Insite*MAP, MapBeans, MapCafé, MapObjects, ModelBuilder, MOLE, NetEngine, PC ARC/INFO, PC ARCPLOT, PC ARCSHELL, PC DATA CONVERSION, PC STARTER KIT, PC TABLES, PC ARCEDIT, PC NETWORK, PC OVERLAY, Rent-a-Tech, *Route*MAP, SDE, SML, Spatial Database Engine, StreetEditor, StreetMap, TABLES, the ARC/INFO logo, the ArcAtlas logo, the ArcCAD logo, the ArcCAD WorkBench logo, the ArcCOGO logo, the ArcData logo, the ArcData Online logo, the ArcEdit logo, the ArcEurope logo, the ArcExplorer logo, the ArcExpress logo, the ArcFM logo, the ArcFM Viewer logo, the ArcGIS logo, the ArcGrid logo, the ArcIMS logo, the ArcInfo logo, the ArcLogistics Route logo, the ArcNetwork logo, the ArcPad logo, the ArcPlot logo, the ArcPress for ArcView logo, the ArcPress logo, the ArcScan logo, the ArcScene logo, the ArcSDE CAD Client logo, the ArcSDE logo, the ArcStorm logo, the ArcTIN logo, the ArcTools logo, the ArcUSA logo, the ArcView 3D Analyst logo, the ArcView Business Analyst logo, the ArcView Data Publisher logo, the ArcView GIS logo, the ArcView Image Analysis logo, the ArcView Internet Map Server logo, the ArcView logo, the ArcView Network Analyst logo, the ArcView Spatial Analyst logo, the ArcView StreetMap 2000 logo, the ArcView StreetMap logo, the ArcView Tracking Analyst logo, the ArcWorld logo, the Atlas GIS logo, the Avenue logo, the *Business*MAP logo, the Data Automation Kit logo, the Digital Chart of the World logo, the ESRI Data logo, the ESRI globe logo, the ESRI Press logo, the Geography Network logo, the MapCafé logo, the MapObjects Internet Map Server logo, the MapObjects logo, the MOLE logo, the NetEngine logo, the PC ARC/INFO logo, the Production Line Tool Set logo, the *Route*MAP IMS logo, the *Route*MAP logo, the SDE logo, The World's Leading Desktop GIS, *Water Writes,* www.esri.com, www.geographynetwork.com, www.gisday.com, and Your Personal Geographic Information System are trademarks, registered trademarks, or service marks of ESRI in the United States, the European Community, or certain other jurisdictions.

Other companies and products mentioned herein are trademarks or registered trademarks of their respective trademark owners.

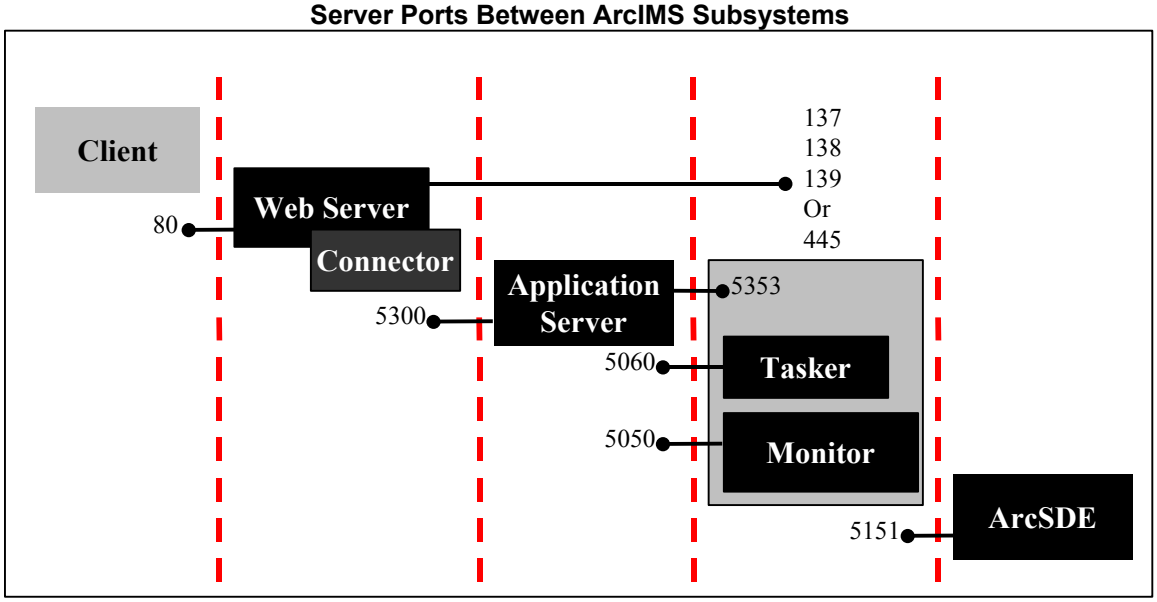
Introduction

The purpose of this technical brief is to identify the firewall server ports used between the various ArcIMS subsystems (Web Server, Application Server, Monitor and Tasker). This brief will also look at the technical challenge of maintaining TCP persistent connections within ArcIMS. This information is critical when designing for enterprise environments, which typically distributes the ArcIMS subsystems across several different servers.

ArcIMS Subsystem Server Port Descriptions

This conceptual diagram shows server ports associated with each ArcIMS subsystem. The "lollypop" symbol identifies the specific listener port associated with each individual ArcIMS Subsystem. The dashed line indicates a firewall, which is to help identify the individual server ports that would need to be open to maintain communication.

Figure 1
Server Ports Between ArcIMS Subsystems



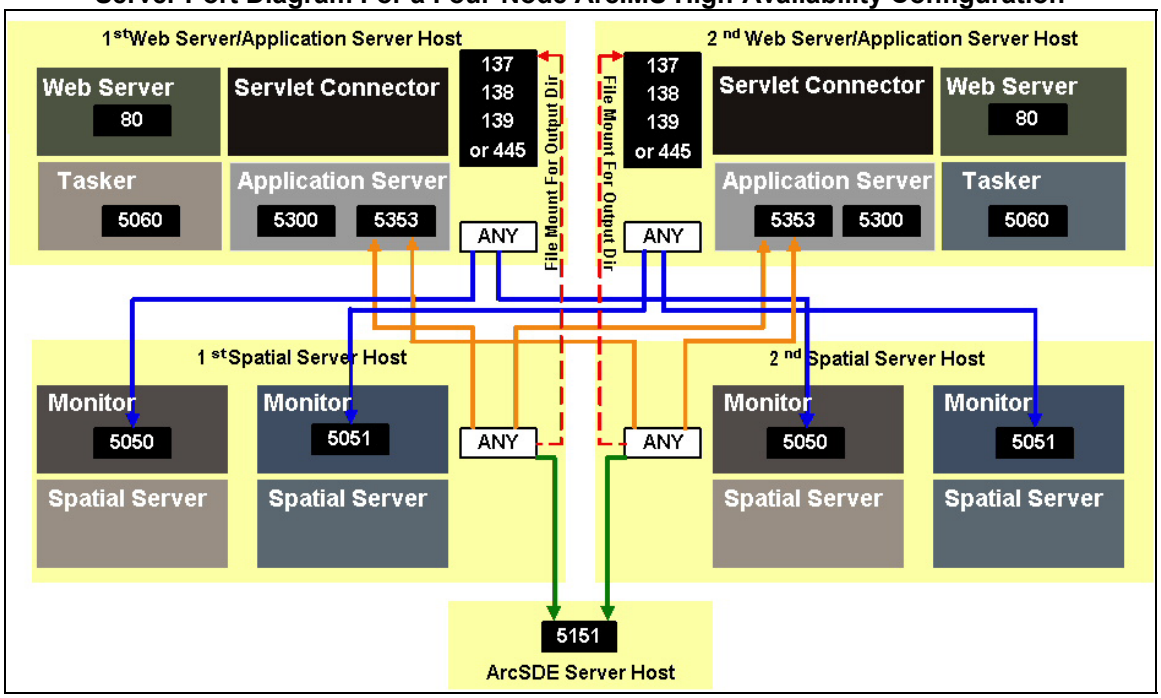
- Web Server: Allow incoming connections to listener port 80 for web clients. Also allow incoming connections to listener ports 137, 138 and 139 from any port on spatial server machine. Ports 137, 138 and 139 are needed for the Server Message Block (SMB) protocol, which is used for file sharing in a Windows NT / 2000 environment. SMB is needed to write the output image files from the Spatial Server to the Web Server. With Windows NT, SMB ran on top of NetBIOS for TCP (NBT), which uses ports 137, 138 and 139. Windows 2000 has the ability to run SMB directly over TCP with port 445. To use port 445, NBT must be disabled.

- Application Server: Allow incoming connections to listener port 5300 from any port on web server machine.
- Application Server: Allow incoming connections to listener port 5353 from any port on spatial server machine.
- Monitor Service: Allow incoming connections to listener port 5050 from any port on application server machine.
- Tasker Service: Allow incoming connections to listener port 5060 from any port on application server machine. Application Server and Tasker Services are typically on the same host. When the ArcIMS subsystems communicate on the same host, the TCP connections will be routed internally through the loopback adaptor and are of no concern to the firewall administrator.
- ArcSDE: Allow incoming connections to listener port 5151 from any port on spatial server machine.

ArcIMS High-Availability TCP Port Diagram

There are several design alternatives when architecting an ArcIMS site. The diagram below shows the outgoing and incoming server port traffic in a typical four-node ArcIMS High-Availability Configuration. All the outgoing TCP connections on a ArcIMS component are consolidated onto a single "any" port. Listening ports are illustrated with black boxes and white numbers.

Figure 2
Server Port Diagram For a Four-Node ArcIMS High-Availability Configuration



Technical Considerations

There are additional considerations associated with placing firewalls between ArcIMS system components. These considerations include the need to maintain persistent, idle TCP connections if the ArcIMS map services are not accessed for an extended period. In addition to packet filtering rules, most firewalls are automatically configured to sever idle TCP connections after a specified timeout value is reached, and some may allow only limited administrative control of this timeout value - consult the firewall's documentation for details. TCPKEEPALIVE settings will not address these TCP connection issues adequately. Based on the experience of ESRI's Support teams, the likelihood of a firewall causing difficulties for ArcIMS depends on the TCP connection administration rules that the firewall employs, the firewall placement, and the length of time that the ArcIMS services might go unused. The following is a very general listing of the likelihood of idle connection termination by a firewall causing problems with the ArcIMS configuration:

High Risk
Between ArcIMS Spatial Server and ArcSDE
Low Risk
Between Web Server and ArcIMS Application Server
Low Risk
Between ArcIMS Application Server and ArcIMS Spatial Server

Increasing the firewall's internal timeout value could produce undesired results within the network. Possible repercussions include degraded firewall performance and additional security risks. If it is determined that the costs of increasing the firewall timeout values outweigh the benefits, an alternative would be to incorporate a "keep-alive" routine within an application that sends requests to all ArcIMS map services and public virtual servers at an interval less than the TCP connection timeout value of the firewall. Such a routine will keep all necessary TCP connections open without the need to change the firewall settings.

Conclusion

When implementing a firewall into an enterprise ArcIMS design there are several server ports that need to be identified to insure communication between the various subsystems. The distribution of the ArcIMS subsystems and placement of firewall will determine which specific server ports will need to be open.

In addition, maintaining persistent connections between the ArcIMS subsystems needs to be considered, since many firewalls often terminate idle connections. To overcome this, the firewalls internal timeout value could be extended or a TCP "keep-alive" routine could be implemented. In any case in which a firewall is to be employed, a complete understanding of the TCP/IP communication needs for ArcIMS/ArcSDE and the administration capabilities of the firewall device and/or software is required.

Support

Enterprise GIS system design is addressed in the *System Design Strategies* white paper at http://www.esri.com/library/whitepapers/pdfs/sysdesig.pdf. For answers to additional GIS capacity planning and solution questions, contact ESRI Systems Integration at sihelp@esri.com. For technical support, contact ESRI Technical Support at http://support.esri.com.

A test report for the Four-Node ArcIMS 4.0.1 Configuration using Network Load Balancing can be obtained at http://www.esri.com/systemsint/kbase/testrep.html.