
Slingshot Deployment Guide

Slingshot Version 2

Document Version 1.1
May 2002

For more information contact:

Swissrisk Financial Systems GmbH
Technical Support
Holzhausenstrasse 44
D-60322 Frankfurt
Germany

Phone +49 69 50952 111
Fax: +49 69 50952 199
Email hotline@sr-financial-systems.com
Website www.sr-financial-systems.com

Copyright Information

This document is protected by copyright law and may not be reproduced or distributed either in part or in total. The licensee is not allowed to pass on the software or the accompanying written materials to third parties or make them otherwise available without prior written agreement of the licensor. Information in this document that refers to possible product extensions or to available accessories is not legally binding, especially because the products are subject to continuous adaptation and because the information may also relate to future development. The contents of this document can change without prior notice and does not represent any legal obligation on the part of Swissrisk Financial Systems GmbH.

Swissrisk Financial Systems GmbH cannot be made liable for the correctness of information in this document nor for damages resulting from the use of this information or the impossibility of using this information. All other legal regulations for using the software and the corresponding documentation are set in the applicable license agreement.

Slingshot is a trademark of Swissrisk Financial Systems GmbH. All other product and company names mentioned in this manual are trademarks of their respective companies

Published by:

Copyright © Swissrisk Financial Systems GmbH |
All rights reserved

Swissrisk Financial Systems GmbH
Holzhausenstrasse 44
D-60322 Frankfurt
Germany

Phone: +49 69 50952-0
Fax: +49 69 50952-333
Website: www.swissrisk.com

Slingshot Deployment Guide

Background	1
Important Concepts	1
Basic Configuration.....	1
Recommended Configuration.....	1
Signed Java Applets.....	2
Simple Deployment	2
Deployment Diagram.....	3
Deployment Diagram.....	4

Background

This document is intended to describe how the Slingshot Web Distribution Server can be deployed in a production environment. It also discusses the considerations for deploying Java Applications

Note: This document uses the word 'Internet' to describe the transfer html and data from the WebServer and Slingshot Web Distribution Server to compatible Browser client devices. The technologies involved are also applicable to Intranets and Extranets, with differing levels of security built in. This document will use the term Internet to describe all these.

Important Concepts

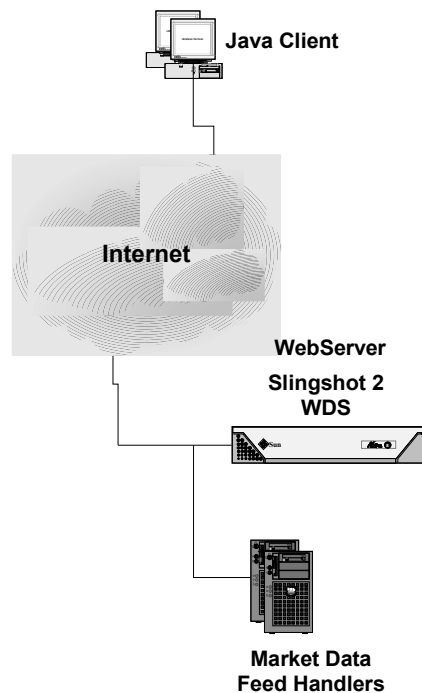
Basic Configuration

This is the most basic configuration possible to deploy Slingshot.

The WebServer is resident on one machine, with the WDS also resident. It is assumed that the WDS publishes its data on a port other than 80 (because the WebServer will use this port).

This configuration is unlikely to work through a firewall without modification to the configuration of the firewall, as firewalls are usually configured to only allow http connections through Port 80.

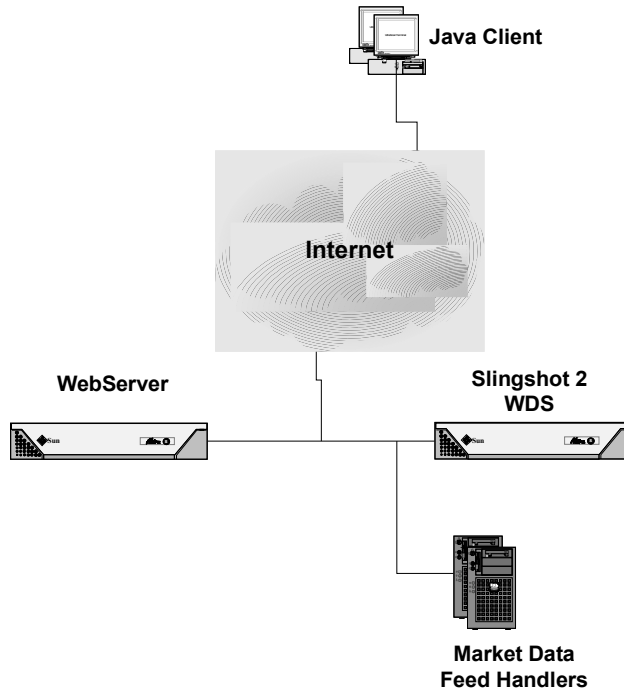
The WDS makes a connection to the relevant Market Data Server and distributes this information to any Slingshot Java Clients that request the information.



Recommended Configuration

This diagram is a typical configuration, showing connection to the market data system, webserver and Slingshot Web Distribution System (WDS). This example is relevant to intranets and associated configurations where security is not an important consideration.

It is worth noting that both the WebServer and the Slingshot WDS are publishing their data on Port 80 (normal http) and so this configuration should be able to transmit streaming data without firewall modification.



Signed Java Applets

An important consideration when designing a Slingshot installation is where Java applets are served from. In the configuration above (recommended) the Java applets can be served from either the WebServer or the Slingshot WDS.

Java applets can either be signed or unsigned. Signed applets verify the manufacturer of the applet with a certified authority that the user trusts. An example of such an authority is Thawte Consulting (Pty) Ltd. The security rules implicit in the use of unsigned Java applets will cause an exception (ie the applet will not execute) if the Client device (ie the Java Virtual Machine within a browser) accesses another device on the network that is not the one from which the Java was downloaded. The simplest way around this situation is to use signed applets, rather than the basic unsigned ones.

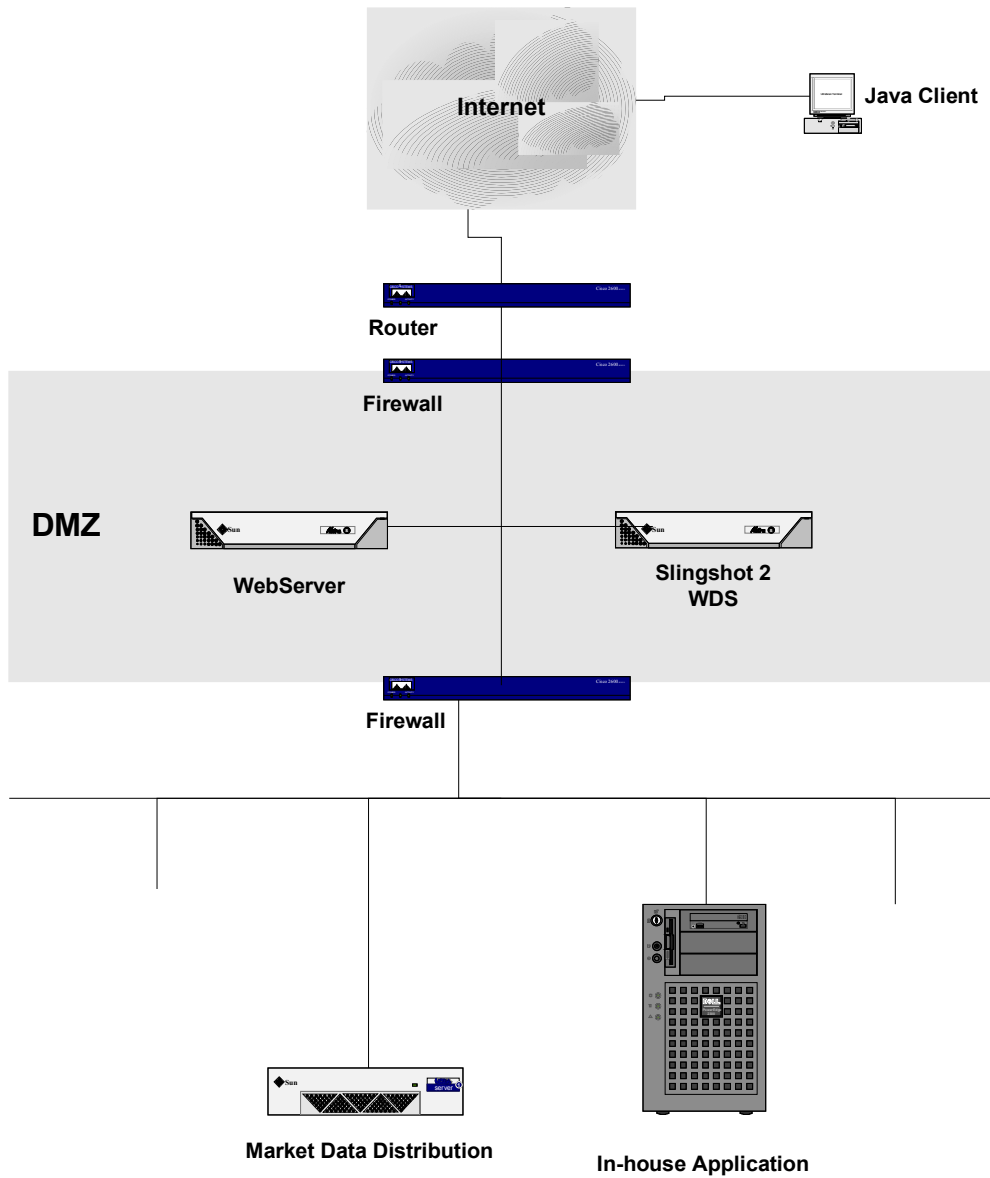
The Slingshot WDS has been designed to operate as a Web Server as well as for the distribution of streaming data. This allows us to use it to serve Java applets instead of a more typical WebServer. The location for the relevant Slingshot files are given below.

	WebServer (eg Apache)	Slingshot WDS
Contains...	HTML code (the basic framework of the page, graphics, text and the position and size of the Slingshot Java Applet)	Java Applets, SLS Files (files describing the format and content of the streaming data)

Simple Deployment

The diagram below shows a simple Slingshot Deployment Layout. It assumes a simple 'De-Militarised Zone' is in place to separate the internal LAN of the network, containing a potential Market Data Distribution platform and other in-house application servers connecting to the Slingshot Components.

Deployment Diagram



Resilient Deployment

The diagram below shows a resilient Slingshot Deployment Layout. A load balancing router configuration at the hosting site will manage traffic between the relevant servers.

Deployment Diagram

