

Server To Server HowTo's

HowTo's ordered by date of creation.

?

?

Gato's HowTo:

?

?

Server-2-server communication occurs on port 5269 (by default).

So the first thing to check is that there is no firewall closing that port.

The second task would be to verify that the server name of each Wildfire server can be resolved by the DNS. XMPP servers will do a DNS SRV look up to figure out the actual IP address and port to use to connect to the remote server. As a consequence of this we can say that remote servers should be accessible from the internet or any remote net that you want to use (e.g. VPN).

?

Reference: <http://www.igniterealtime.org/community/thread/22874>

?

LG's HowTo:

?

Special use case:

?

s2s between two offices with internet connection and firewalls

?

With OfficeN I mean one of the offices and it's IP address.

?

Firewall setup

?

Make sure that Wildfire in Office1 can create outgoing connections to Office2:5269 and vice versa.

Make sure that Office2:5269 accepts connections from Office1:1024-65536 and vice versa.

Make sure that Office2:5269 forwards the incoming requests to Wildfire (R-NAT or whatever you want to call it).

This should allow the Wildfire servers to connect to each other but not to other XMPP servers.

?

Walter's HowTo:

?

Server to Server (s2s) How to Guide

?

Introduction

?

Openfire server allow the connection from one server to another (s2s) to allow users of different servers to chat. The connection is established by the servers on request by the users. There is no mechanism to establish a server 2 server connection in the admin interface of the server. The server configuration is limited to security related settings and some technical parameters. The server 2 server connection will be started as soon as a

contact is added to the client roster that is not belonging to the server were the user is connected to.

?

This guide shows the setup between an Openfire server and the public server jabber.org. There are also some comments regarding secure (TLS, SSL) server to server communications at the end.

?

Setup

?

Assumptions: You have a home network (intranet) behind a firewall. A openfire server is set up in this network. You also have access to a pc, that is connected to the internet.

?

Install your openfire server. Configure your server for s2s connections:

??The server name of the openfire (Server/Server Manager/Server Settings) has to be a name, that can be resolved by DNS (e.g. homebase.dyndns.org)

??Check the Server to Server Port (Server/Server Manager/Server Settings). It should be 5269

??The xmpp.domain (Server/Server Manager/System properties) has to be a DNS resolveable name

??Allow server to server connections by enabling the service? (Server/Server Settings/Server to Server)

??Allow anyone to connect. Ensure that you are not blocking any server

??Check the Security Settings (Server/Server Manager/Security Setting). For Jabber.org you have to set the Server Connection Security to "optional" (as of 19.04.2007)

??Switch on the debug log (Server/Server Manager/Logs-> Debug Tab)

?

Get a user at your Openfire server e.g. myhomeuser@myserver.dyndns.org.

?

Get a user at jabber.org by using your client e.g. mypublicuser@jabber.org

?

Ensure IM connectivity to both servers from a client connected to your home network. Test logon, chat etc..

?

NOTE: The servers will try to establish a connection with each other on port 5269. This requires that this port is open on the firewall of your network. Also, the servers will try to resolve each others name by DNS. Hence you have to ensure, that both servers can be resolved by DNS. The request send from your server to jabber.org will be in the debug log. It looks somewhat like this (for add contact from Spark): `<presence id="aeAgv-42" to="mypublicuser@jabber.org" type="subscribe" from="myhomeuser@myserver.dyndns.org"/>`. A failure of the DNS resolution for jabber.org or myserver.dyndns.org will make the s2s impossible.

?

Ensure connectivity on port 5269. Get a Telnet client on your PC (Windows users may use DTELNET from <http://dtelnet.sourceforge.net>) and install it (if necessary) on your notebook and the internal network client. Open a telnet session to your internal server on port 5269. You will get something like `</stream:stream>`. If not, there is an error (maybe a firewall?). Open a telnet session at jabber.org. Your should also get a statement containing `</stream:stream>`. This has to be done for an internal client and for a client connected to the internet. If successful, you know that jabber.org can resolve your server (e.g. myserver.dyndns.org) and connect to port 5269 and that your network can connect to jabber.org on port 5269.

?

Establish a server to server connection via myserver. Logon with myhomeuser to myserver via spark. Add the jabber.org contact to your roster by entering the contact with a domain e.g. mypublicuser@jabber.org. The server should establish a session. This can be checked in (Sessions/Server Sessions) and the logs.

?

Troubleshooting

?

Problem: The server names can not be DNS resolved. Resolution: Enter your server names in the DNS Servers of your intranet. Enter the server names in the file hosts of your operating system. Use dyndns.org or similar services, if you want to provide the chat service to others.

?

Problem: Port 5269 connectivity is missing. Resolution: Change the settings of your firewall. Make sure, that you control all firewalls (e.g. the WinXP internal firewall and the one of your DSL router).

?

Problem: Still no connection to Jabber.org. The security setting should be set to Optional.

?

Problem: Checked everything and still not working? Go to sleep and check again the next day. Use the logs and keep on trying.

?

Problem: The server is not accepting parameter changes. Don't just start/stop the server, stop it and quit Openfire.

?

Establish secure server to server communication

?

The methods above should also apply, if you set up several servers within your intranet. To establish a secure communication between servers, you do have to set the Server Connection Security (Server/Server Manager/Security Setting) to "Required". You have to check that TLS is enabled for s2s. The value of the property `xmpp.server.tls.enabled` (within Server/Server Manager/System properties) has to be "true". Also, if you are using self signed server certificates, you should add a system property " `xmpp.server.certificate.verify`" and set it to "false". A properly working encrypted s2s session is shown with a lock in the server session view.