Volume

1

SYSLOG JUNCTION

User's Guide

User's Guide

Introduction

In simple terms, Syslog junction is a log viewer with graphing capabilities. It can receive syslog messages from a server which are then filtered and plotted as graphs. Although message from any syslog server can be received by Syslog Junction, currently a parser is available for Cisco PIX firewall. Parsers for other syslog servers will be added in the future.

System Requirements

Syslog Junction is server based software that can run on multiple operating systems. Following table lists the minimum system requirement for Syslog Junction.

Operating System	Windows NT, XP, 2000, 2003, Linux, Solaris, MacOS X
Processor	500 MHz or above clock speed
Memory	128 Minimum (512 Recommended)
Hard disk	30 MB
JVM	Only required for Solaris and MacOS X. A JVM is included with the Windows and Linux version of the installer

Installation

Installation of Syslog Junction is pretty straight forward – download the installer from AboutMyX website and run it. On Windows it will create a Windows Service. However, on other operating systems you have to manually add a starter script in /etc/init.d/ directory. Contact support if you need help in creating this script.

Configuration

Before Syslog Junction can plot graphs and display data, you have to configure your PIX firewall to send logging information to the machine where Syslog Junction is running. It is assumed that you are familiar with how to change configuration on a PIX firewall. Consult Cisco documentation for further information.

Following steps show how to configure your PIX firewall.

1. Open a TELNET session to your firewall and provide necessary login information.

2. Turn on privilege commands mode by typing "enable" at the prompt.

3. Type "configure terminal" to go into configuration mode

4. Type the following command to enable logging

```
logging on
logging trap informational
logging host inside 192.168.1.50
```

5. After typing the above lines type the show command and confirm the settings.

```
show logging
```

6. Save and exit

```
write memory
exit
exit
```

NOTE: The last line in the above script assumes that you have installed Syslog Junction on a machine where the IP address is 192.168.1.50. Most likely, you will have a different IP and therefore, will have to change it.

Using Syslog Junction

Once your PIX firewall is properly configured and Syslog Junction is installed on the machine, you should see traffic graph through a browser. To connect to Syslog Junction open up a browser window and type the following URL.

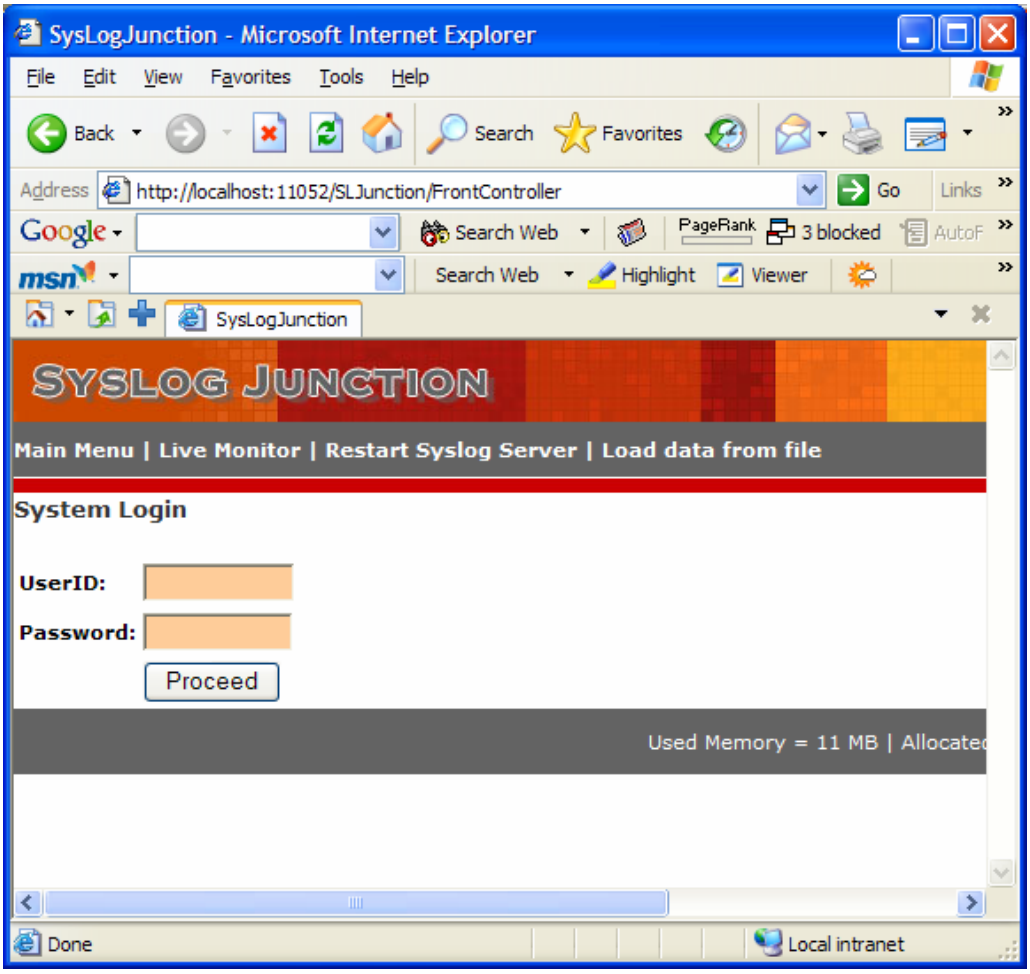
This document assumes that the IP address of the machine is 192.168.1.50. Change this value if you are running it on a different machine

http://192.168.1.50:11052

This will open up the login screen. The default user ID and password for Syslog Junction is:

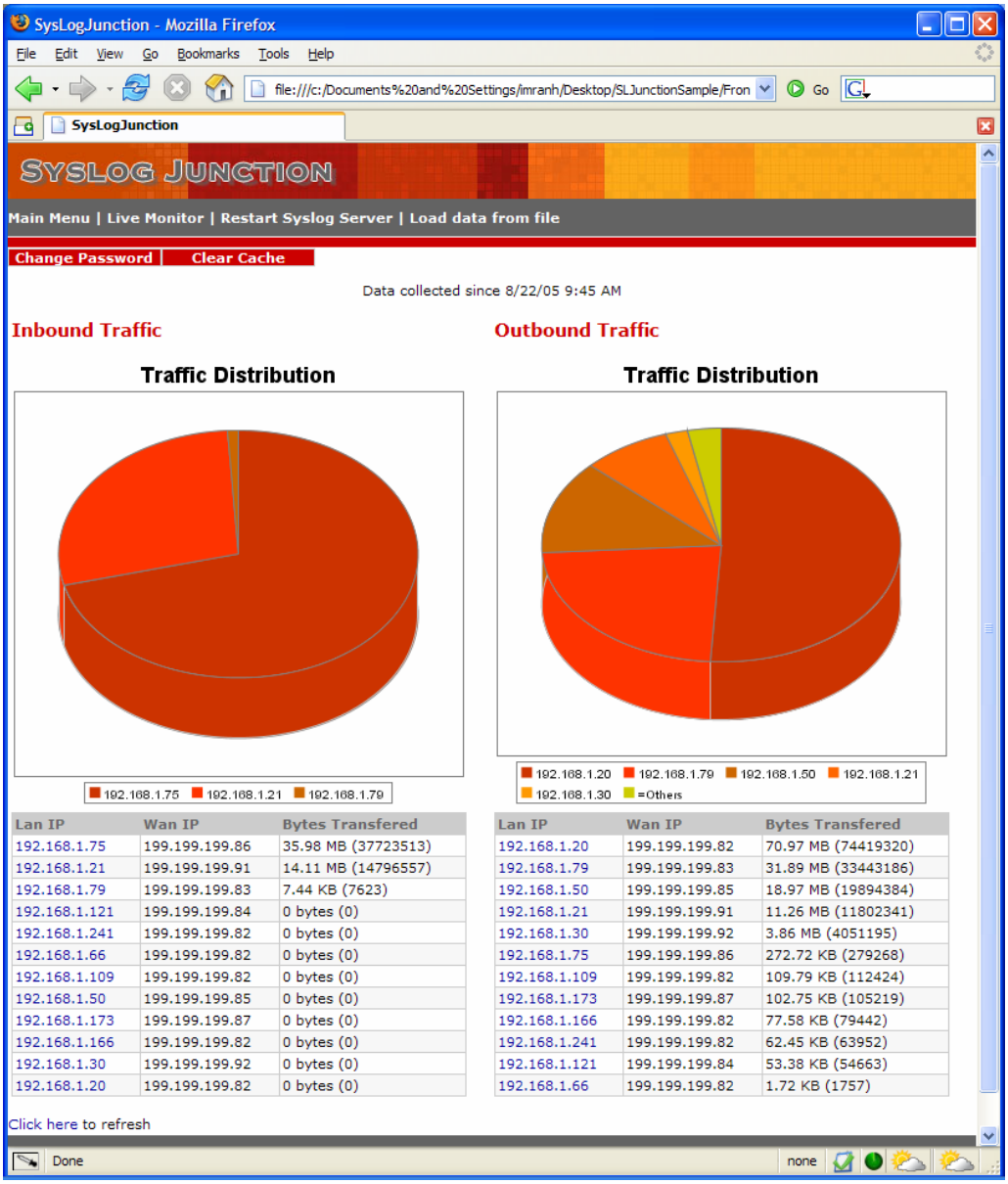
UserID: admin

Password: letmein



Viewing graphical data

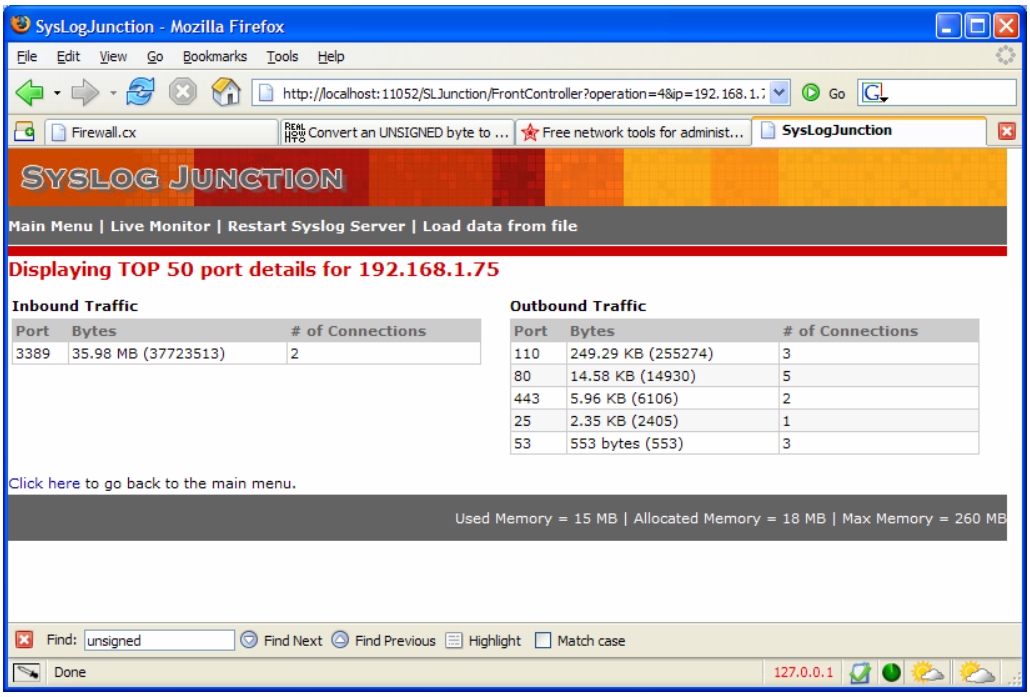
After you login, you will automatically be redirected to the reports screen



This graph shows you inbound as well as outbound traffic passing through your firewall with the amount of data transfer for every machine. Following table explains each column in the report

Lan IP	This is the internal IP address of a machine in your network
Wan IP	This is the external IP address of a machine in your network. If a one-to-one mapping does not exist, you will see more than one machine having the same external IP. This is normally the case when you use NAT.
Bytes Transferred	Amount of data that is either sent or generated by a machine

Click on the link for a machine's IP to see the detail information.



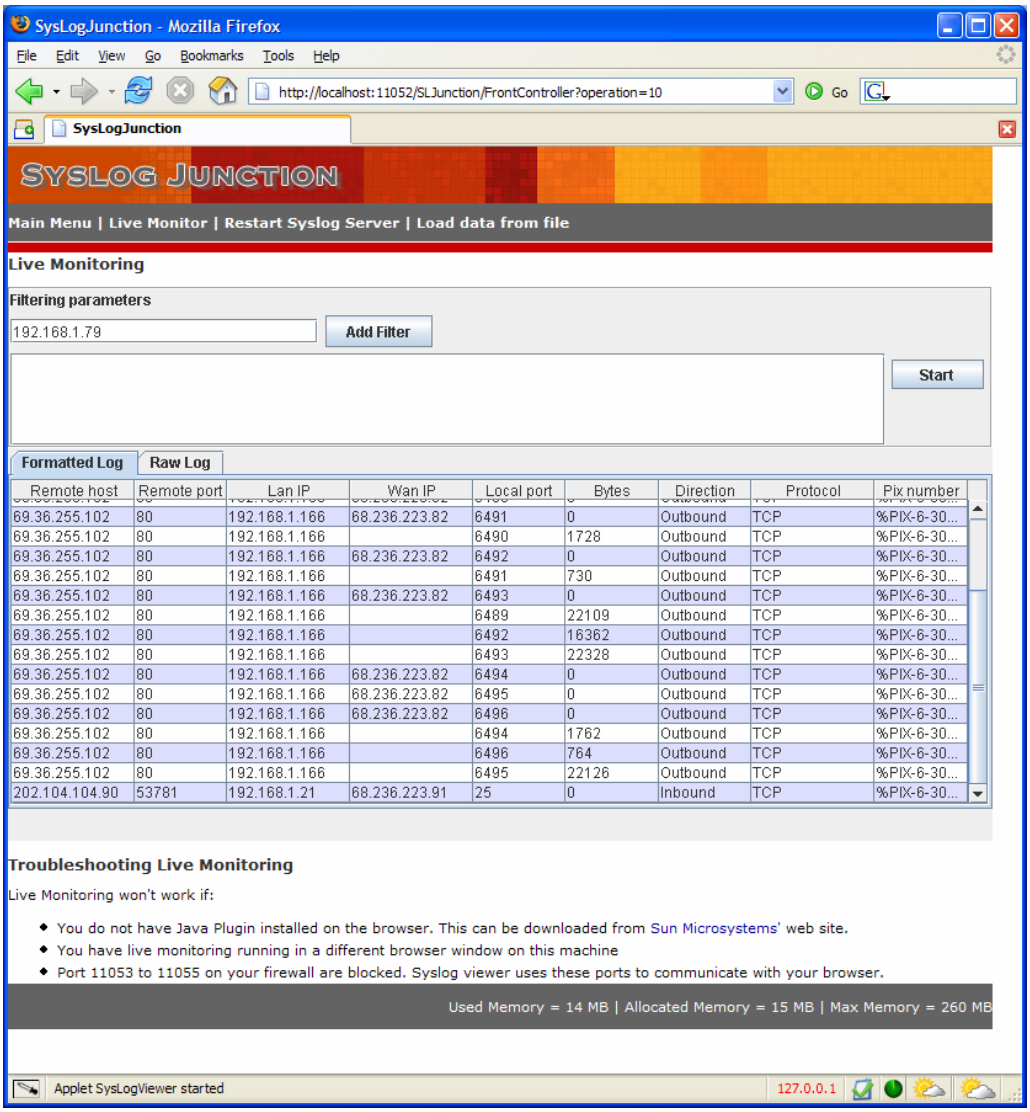
The detail view shows you transferred bytes and the number of TCP/IP connections for a particular port. The image above is an example of a machine that is running a POP3, HTTP, SMTP and DNS server.

Clearing Cache

Syslog Junction maintains an internal cache that holds data counters for the server. When you clear the cache, these counters get reinitialized and all graphs will start from 0 bytes.

Live Monitoring

Live monitoring allows you to see records as they are sent by your firewall. In order to view messages in Live Monitor, you have to install Java plugin for your browser.



Note: When messages are displayed in formatted grid, you will not see all messages that are sent from the firewall. To see all messages view the raw log.

Filtering messages

Live monitor can generate lots of rows in matter of seconds. Therefore, it is highly recommended that you filter messages. Message filters work by specifying one or more Regular Expressions that are used against any incoming message. Therefore, let's say

you want to see messages for one machine, the simplest way is to put that machine's IP address.

Changing Configuration

By default the HTTP server within Syslog Junction listens on port 11052. This value can be changed by modifying SLJunctionConfig.xml file in the config folder.

The same file holds the login password for the admin account.