Tomcat Native 2

Using our own JNI wrapper for OpenSSL in Tomcat and Undertow

Workshop R&D - Red Hat

Supervisors : Jean-Frederic Clere & Rémy Maucherat

Team : Jocelyn Thode & Simon Brulhart

Summary

- Overview
- What has been accomplished
- Benchmarks
- Issues
- Future Works

Undertow & Tomcat

Undertow and Tomcat are very similar, they:

- Are Web servers
- Are Servlet containers using JSSE
- Can use JSSE SSL Engine

Old State: Tomcat + Tomcat Native

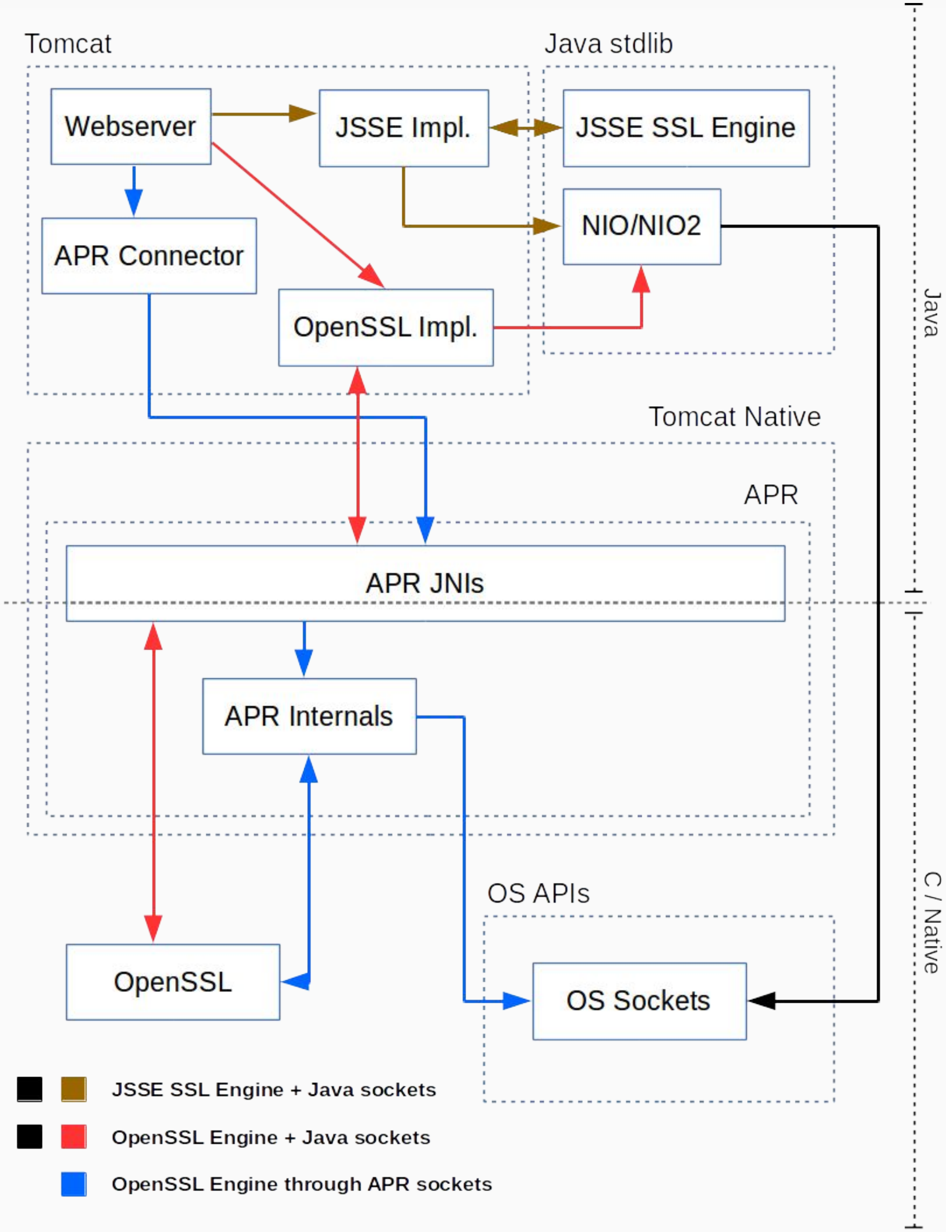
“An optional component for use with Apache Tomcat“

- Better performance and compatibility with OS
- Uses encrypted sockets through Apache Portable Runtime (APR)
- Uses OpenSSL APIs through APR

Old State: Undertow + JSSE

- Can only use JSSE SSL Engine
  - Only Java Code
  - SSL/TLS performance aren’t great
- Already some work done to port Tomcat Native
  - Helps us port Tomcat Native 2 to Undertow

Old State: Ways to Use SSL



New State : Tomcat Native 2

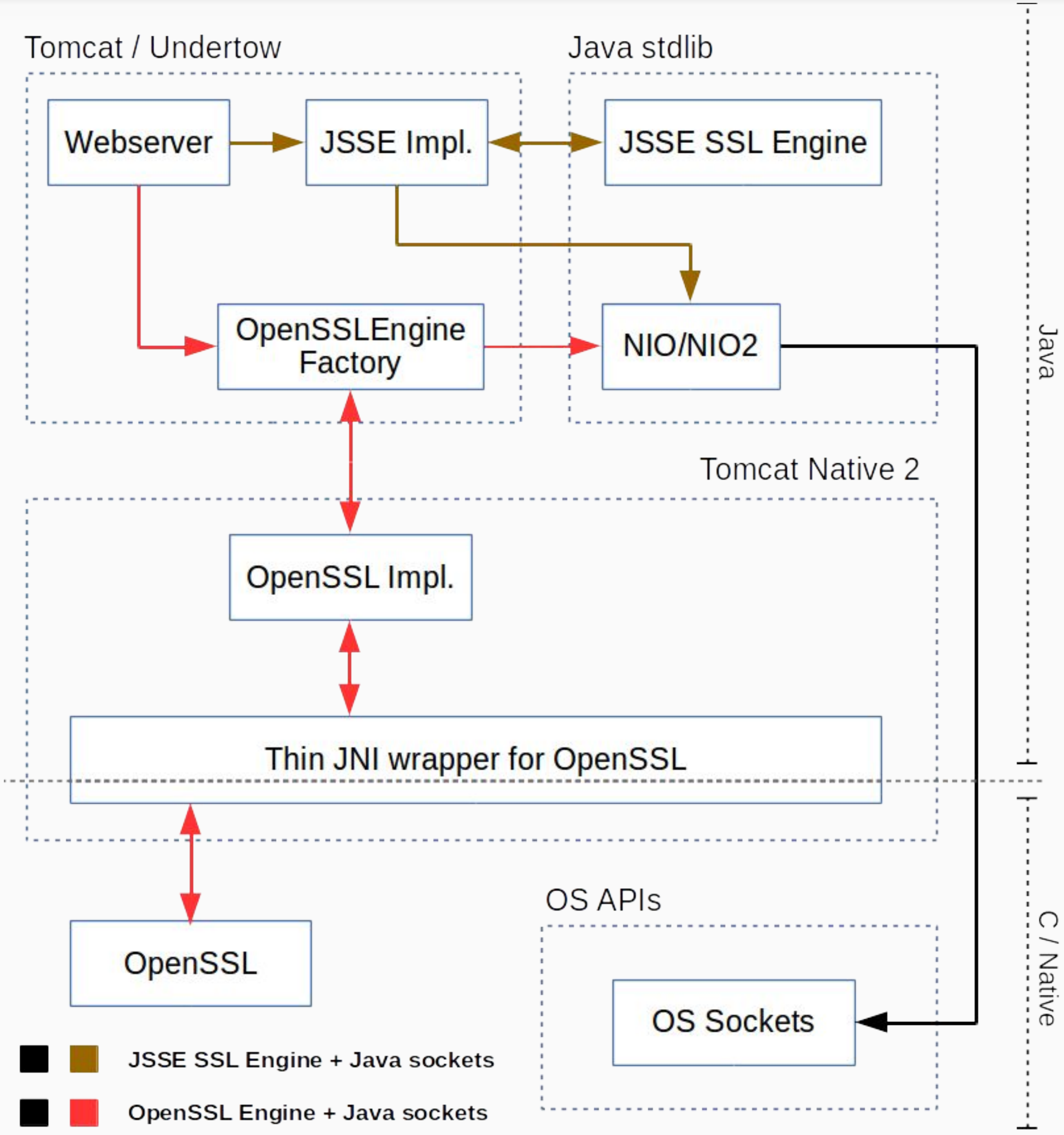
Tomcat + Tomcat Native 2

- Reduces dependencies (no APR)
- Reduces project complexity
- Native/Java bridge with JNI+Homebrewed code

Undertow + Tomcat Native 2

- Brings OpenSSL
- Small dependencies (no APR)
- Native/Java bridge with JNI+SPI

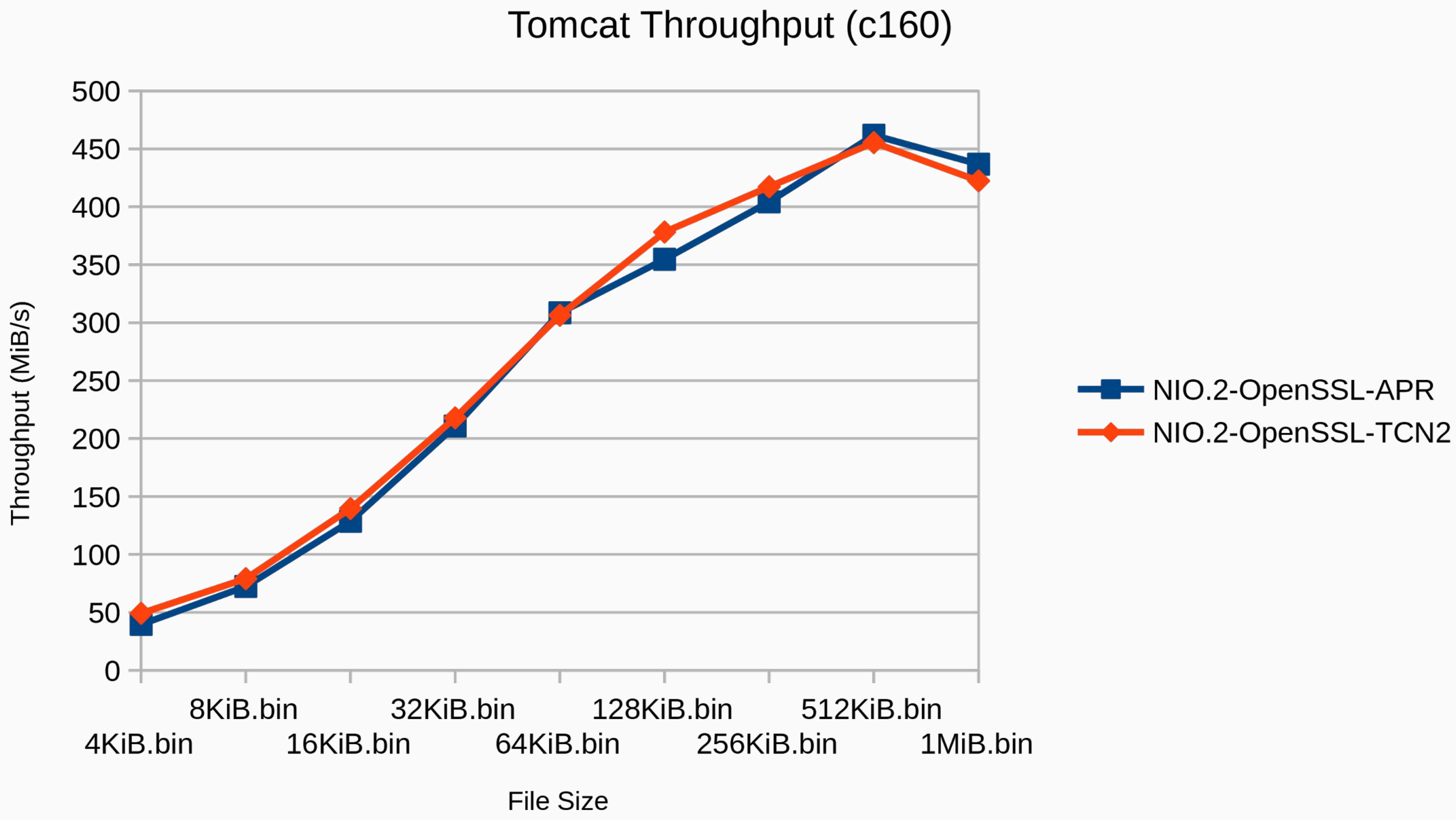
Tomcat Native 2 in Tomcat/Undertow



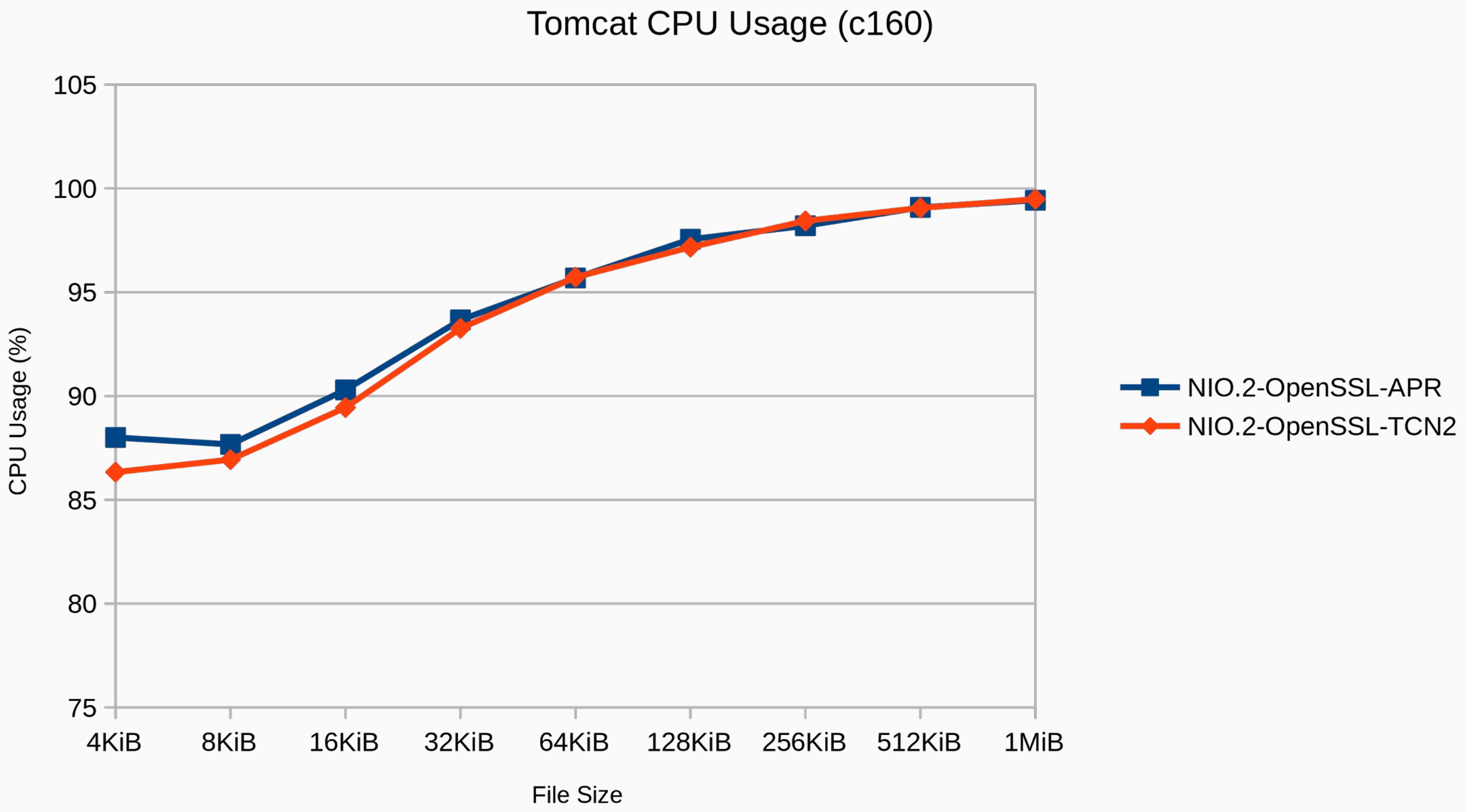
What has been accomplished (2)

- Integrate Tomcat Native 2 in Undertow
- Merge changes to Tomcat Native in Tomcat Native 2
  - OpenSSL 1.1
- Write documentation on how to build and run Tomcat Native 2
- Run Benchmarks

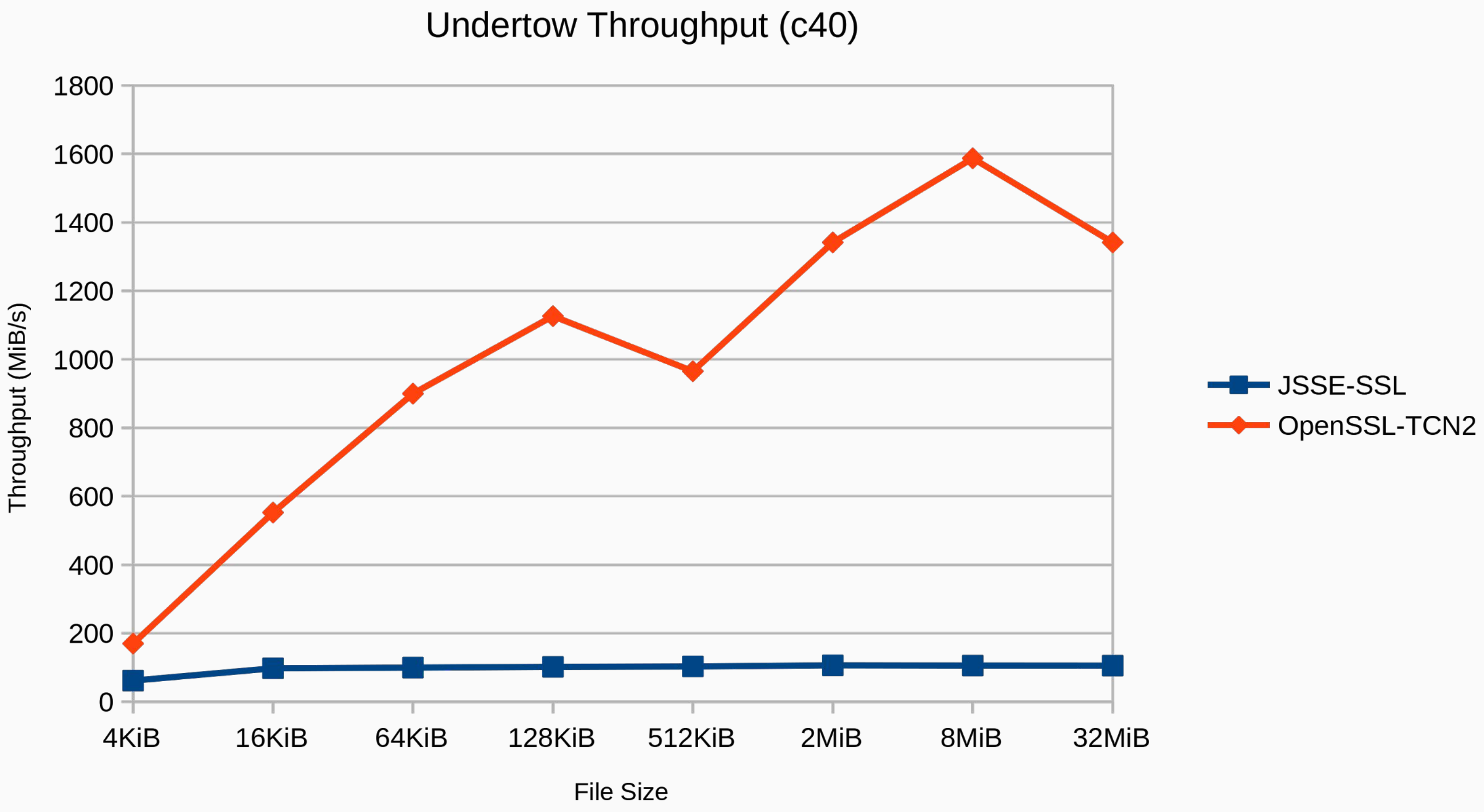
Benchmarks : Tomcat



Benchmarks : Tomcat



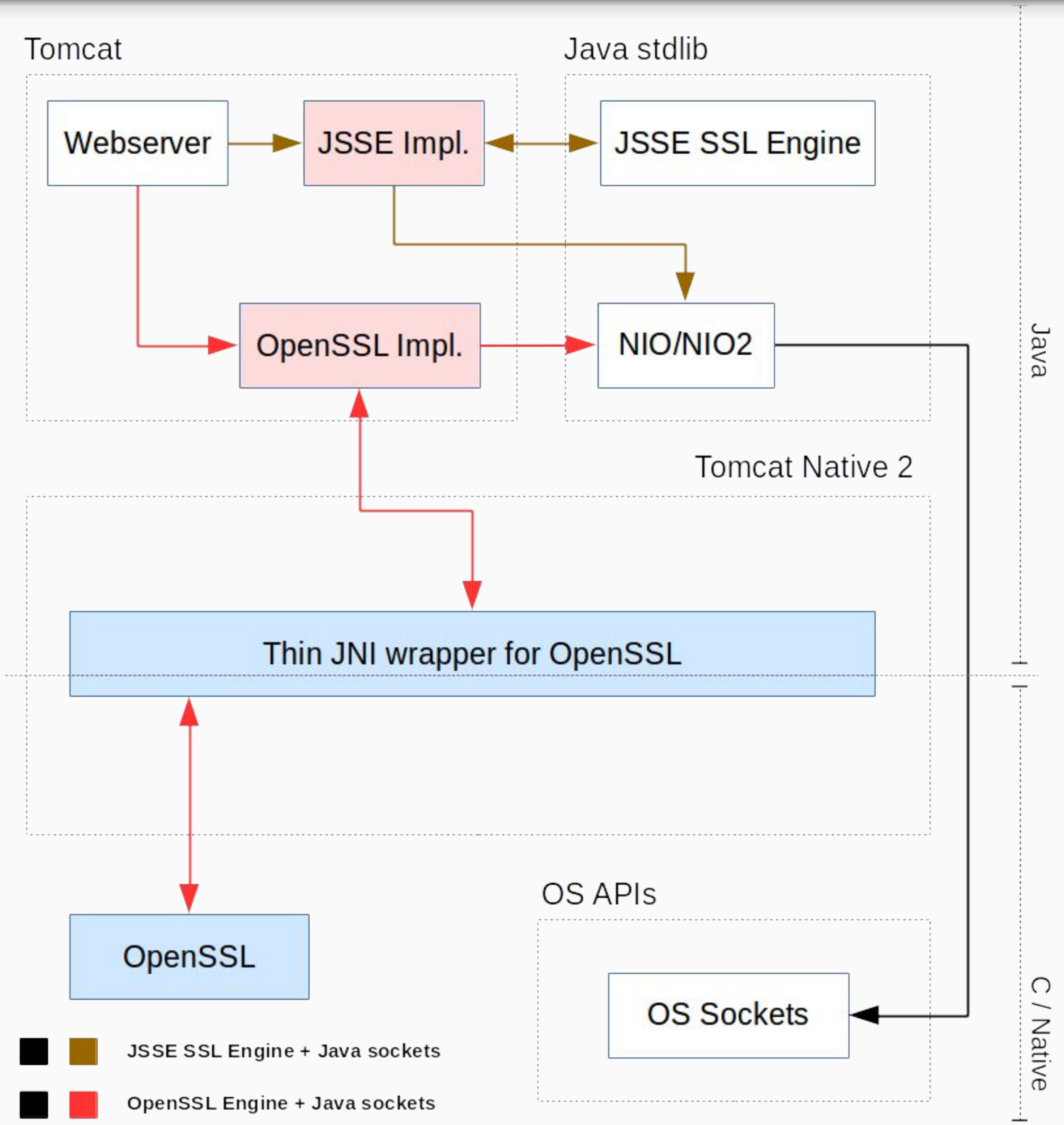
Benchmarks : Undertow



Issues

- Dynamic Linking
  - Bug during implementation
  - Took more time than wanted
  - Debugging would be too long
- Diverging Philosophies
  - Tomcat and Undertow maintainers didn't agree on everything
  - Modify architecture to accommodate this divergence

Issues: Diverging Philosophies



Tomcat

Webserver

JSSE Impl.

OpenSSL Impl.

Java stdlib

JSSE SSL Engine

NIO/NIO2

Tomcat Native 2

Thin JNI wrapper for OpenSSL

OpenSSL

OS APIs

OS Sockets

Java

C / Native

⬛ 🟫 JSSE SSL Engine + Java sockets

⬛ 🟥 OpenSSL Engine + Java sockets

🟦 Common code

🟥 Forked code

Future Work (1)

- Implement Dynamic Loading
  - Big boon for the project
- Implement TLS Sessions
  - Can only be done in Undertow for now
  - Was not important for a prototype
- Implement OpenSSL handshake callback
  - Do not rely on a hack

Future Work (2)

- Better integration with Undertow
  - ALPN callback always accept H2
- Multi platform support
  - Only compatible with POSIX platforms

Questions