

# 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
- Issues
- Benchmarks
- Future Work

# 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

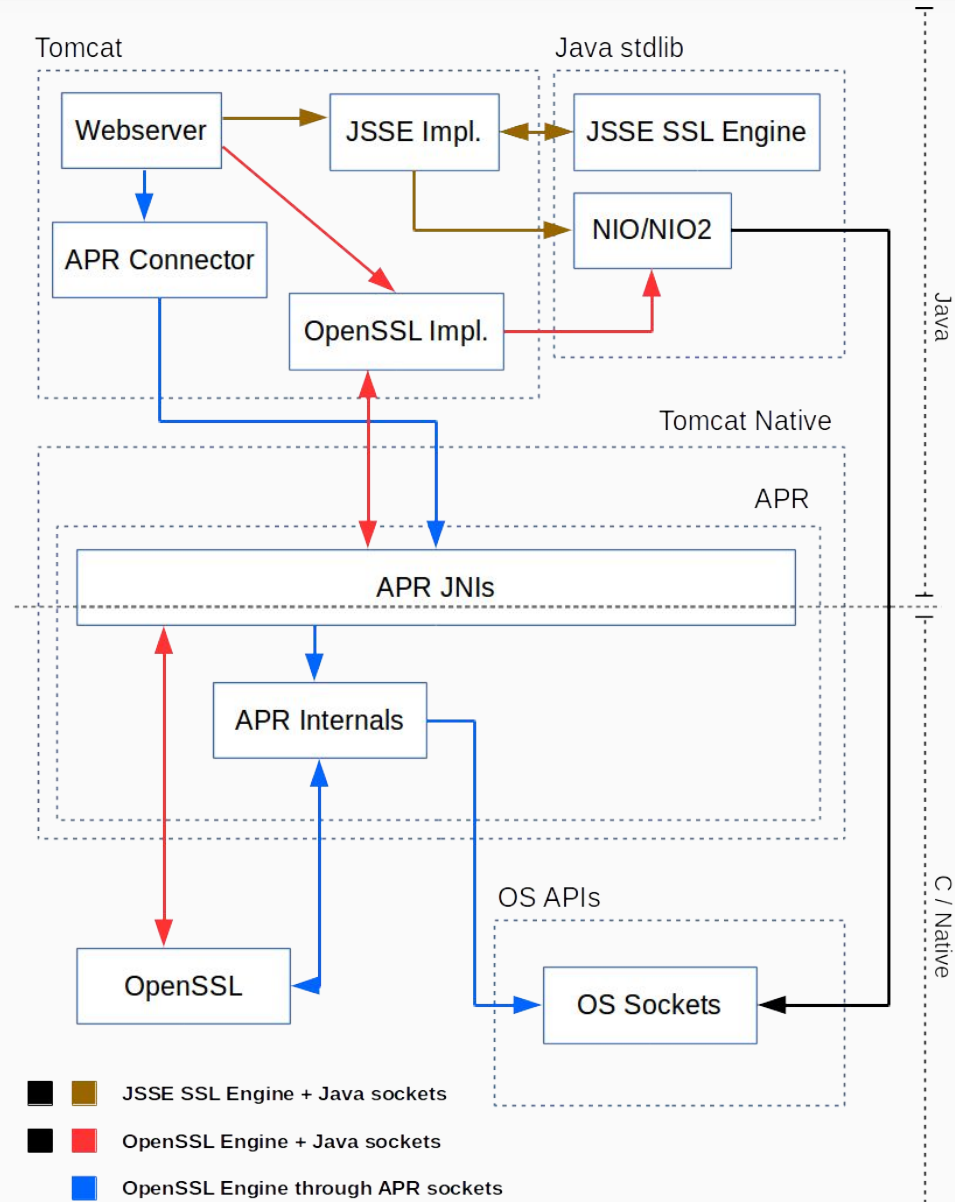
“An optional component for use with Apache Tomcat”

- 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 is not 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

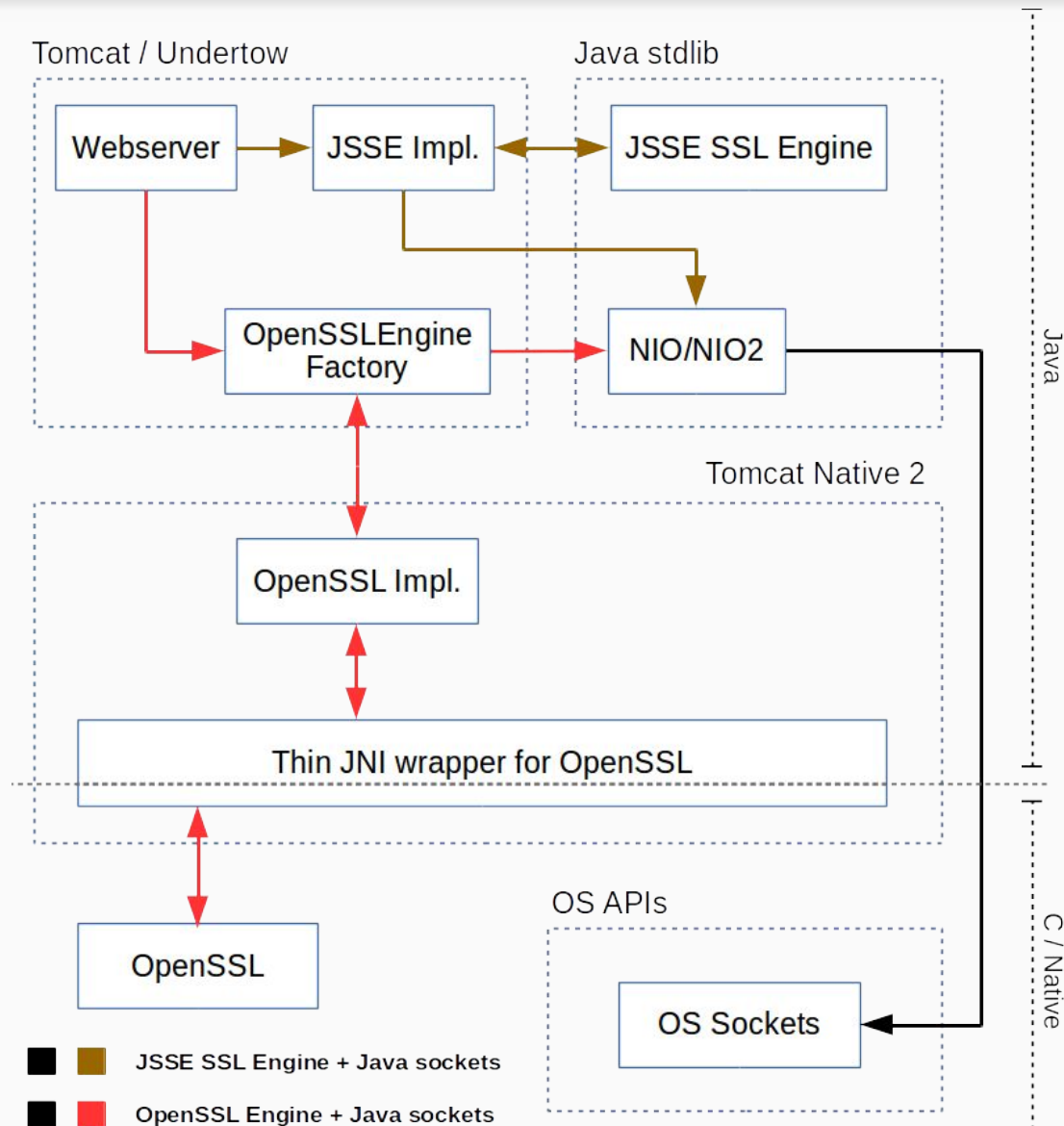
## **Tomcat + Tomcat Native 2**

- 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

# What has been accomplished: Tomcat Native 2 in Tomcat/Undertow





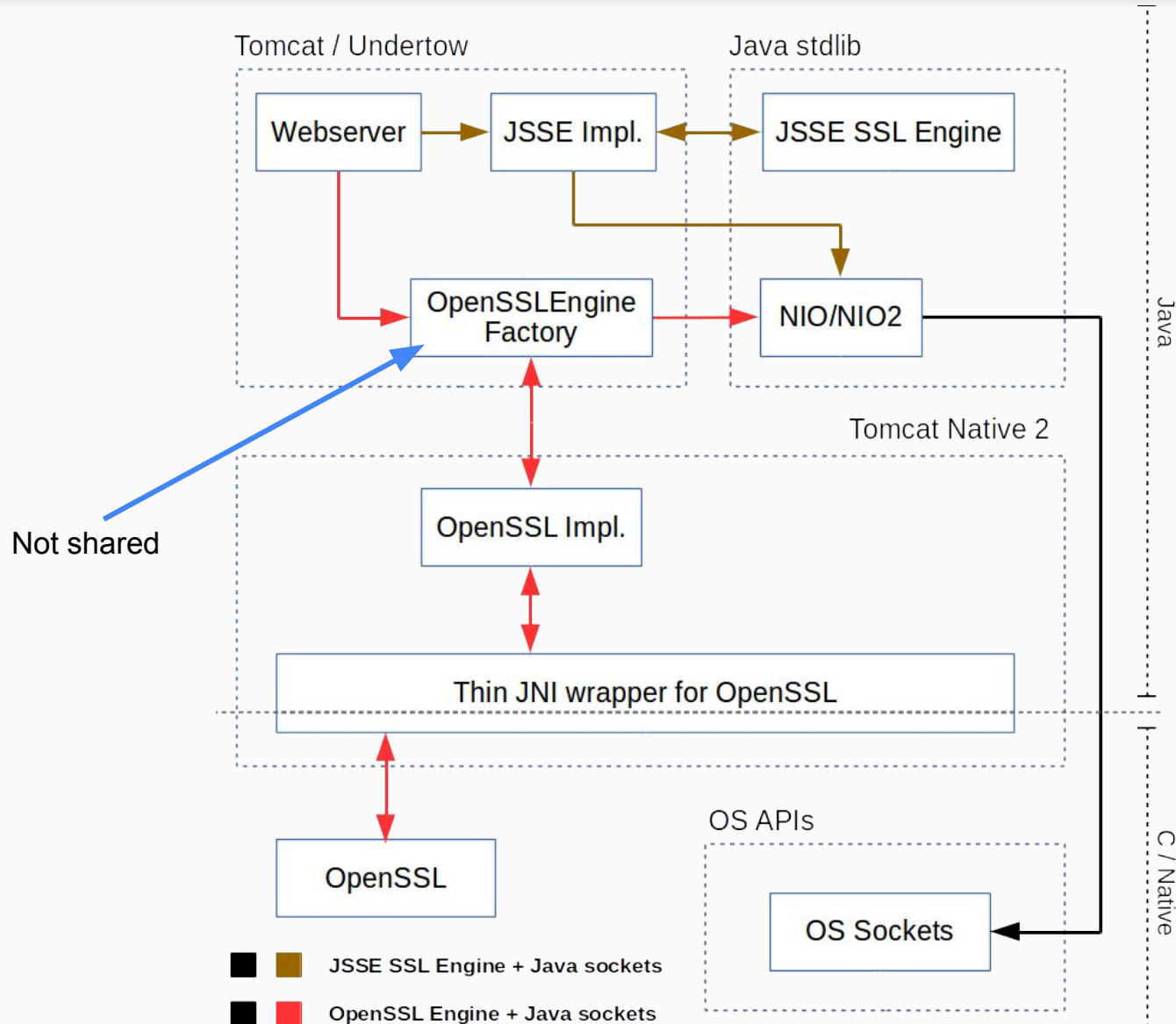
# What has been accomplished

- 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

# Issues

- Dynamic Loading
  - Took more time than wanted
  - More complex since OpenSSL v1.1.0 compatibility
- Diverging Philosophies
  - Tomcat and Undertow maintainers didn't agree on everything
  - Modify architecture to accommodate this divergence

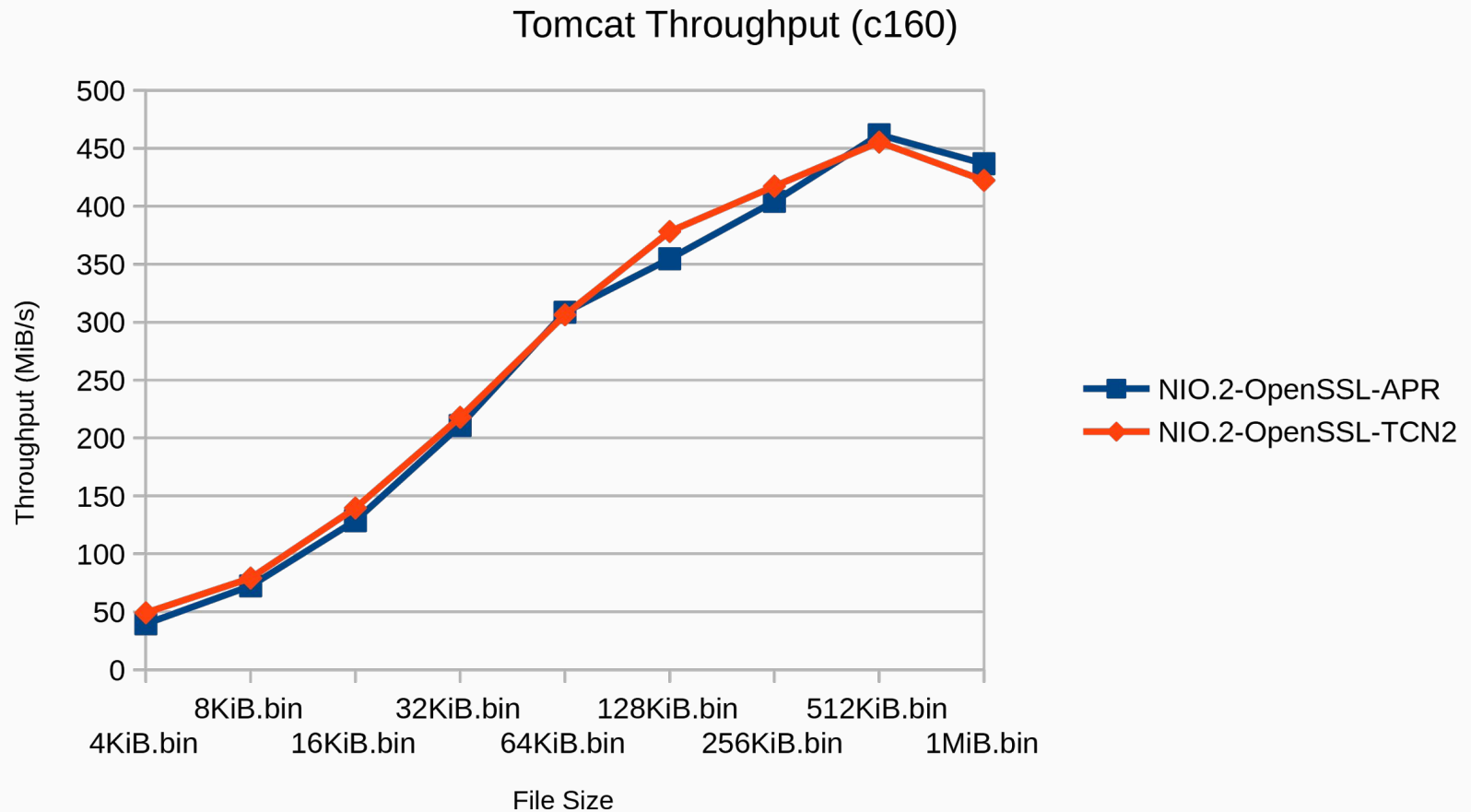
# Tomcat Native 2 in Tomcat/Undertow



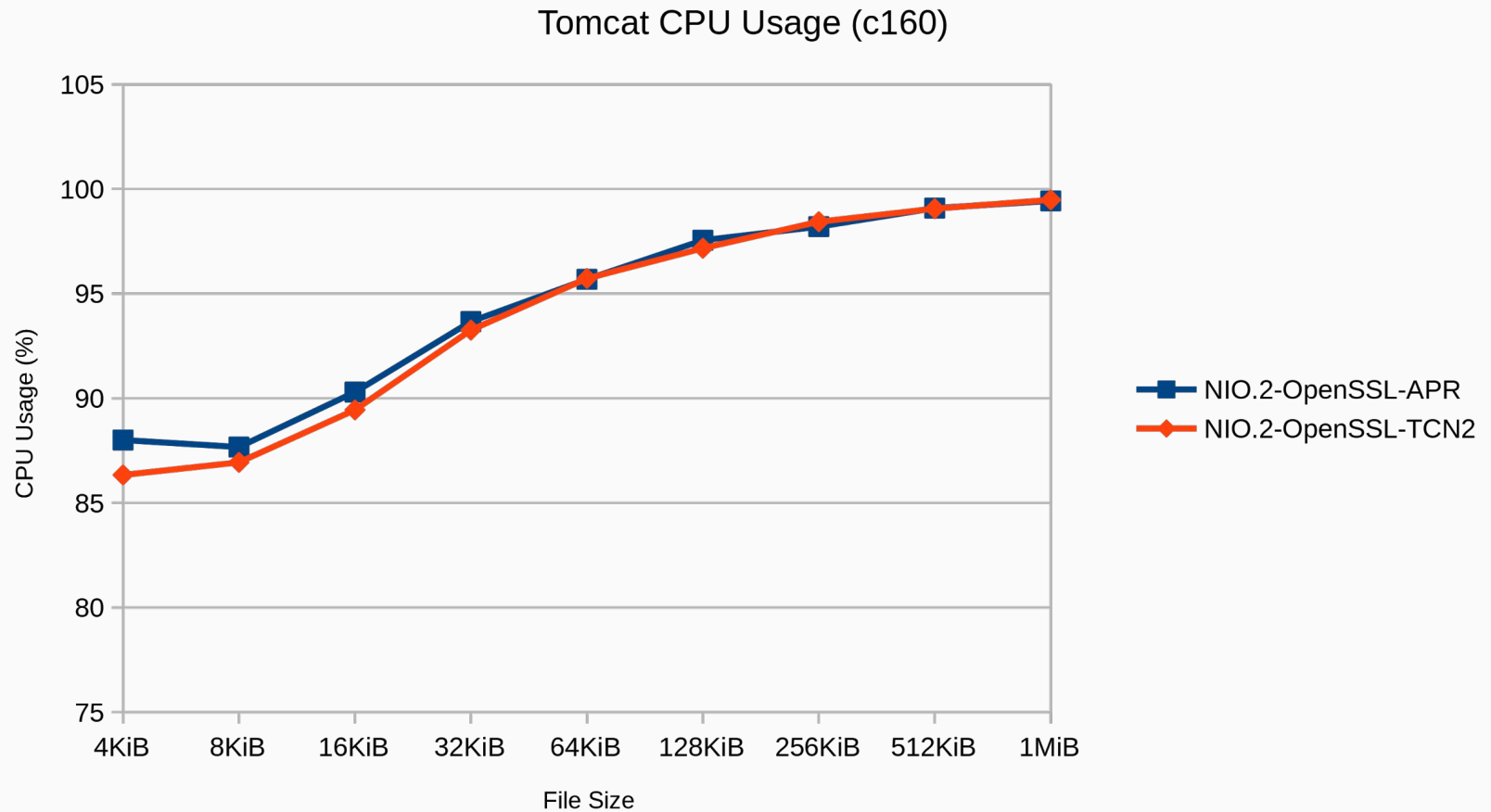
# Benchmarks

- Many concurrent HTTP requests
- Measure server throughput (and CPU load)
- Try with different file sizes
- Test bed
  - Tomcat: RedHat cluster
  - Undertow: personal desktop computer

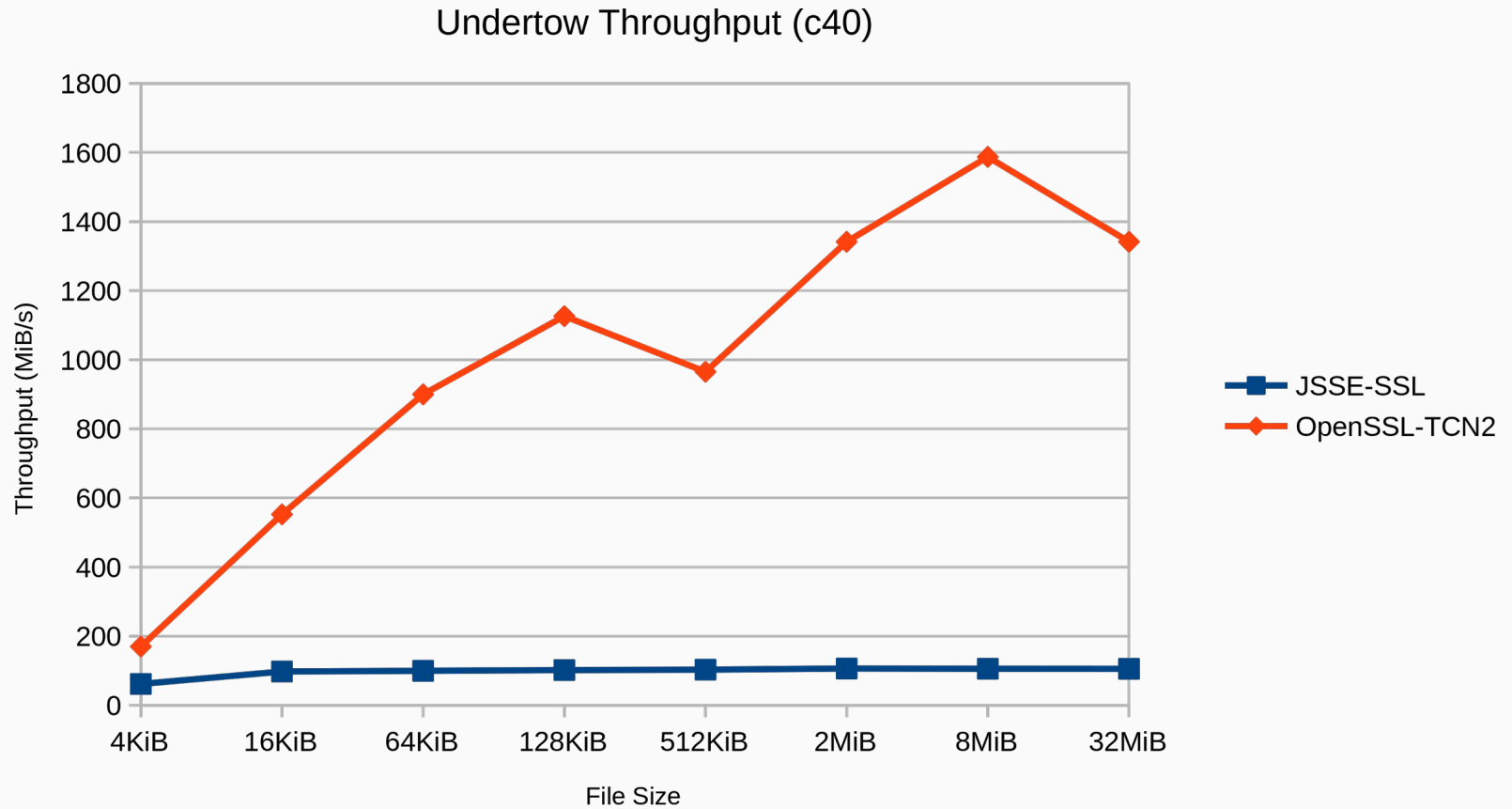
## Benchmarks : Tomcat



# Benchmarks : Tomcat



## Benchmarks : Undertow



# Future Work (1)

- Implement Dynamic Loading
  - Big boon for the project
- Implement TLS Sessions
  - Incomplete support in current Tomcat-Native
  - Was not important for a prototype
- Better integration with Undertow
  - ALPN callback always prefers H2
  - SSL client mode unsupported



# Future Work (2)

- Implement OpenSSL handshake callback
  - Do not rely on a hack
- Cross-platform support
  - Currently only compatible with POSIX platforms
  - Target same platforms as original Tomcat Native

# Questions

