Quassel IRC - Feature #1866

Implicit TLS (with SNI) connection mode

07/30/2023 12:50 PM - Avamander

Status:	New	**Start date:**	07/30/2023
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
OS:	Any		

Description

It would be very useful if Quassel had a client-core connection mode that use pure implicit TLS (with SNI).

This would provide multiple benefits:

- Adds the ability to use any TLS load balancer or terminator (traefik/nginx/etc. with more nuanced configuration)
- Implicit TLS like implemented by other software is likely less failure-prone thus more secure than any ad-hoc TLS support
- Resists protocol fingerprinting
- Adds the potential to leverage things like mTLS (using a YubiKey/smartcard for auth), ECH or QUIC in the future

In theory it shouldn't also be that difficult to implement using already available libraries.