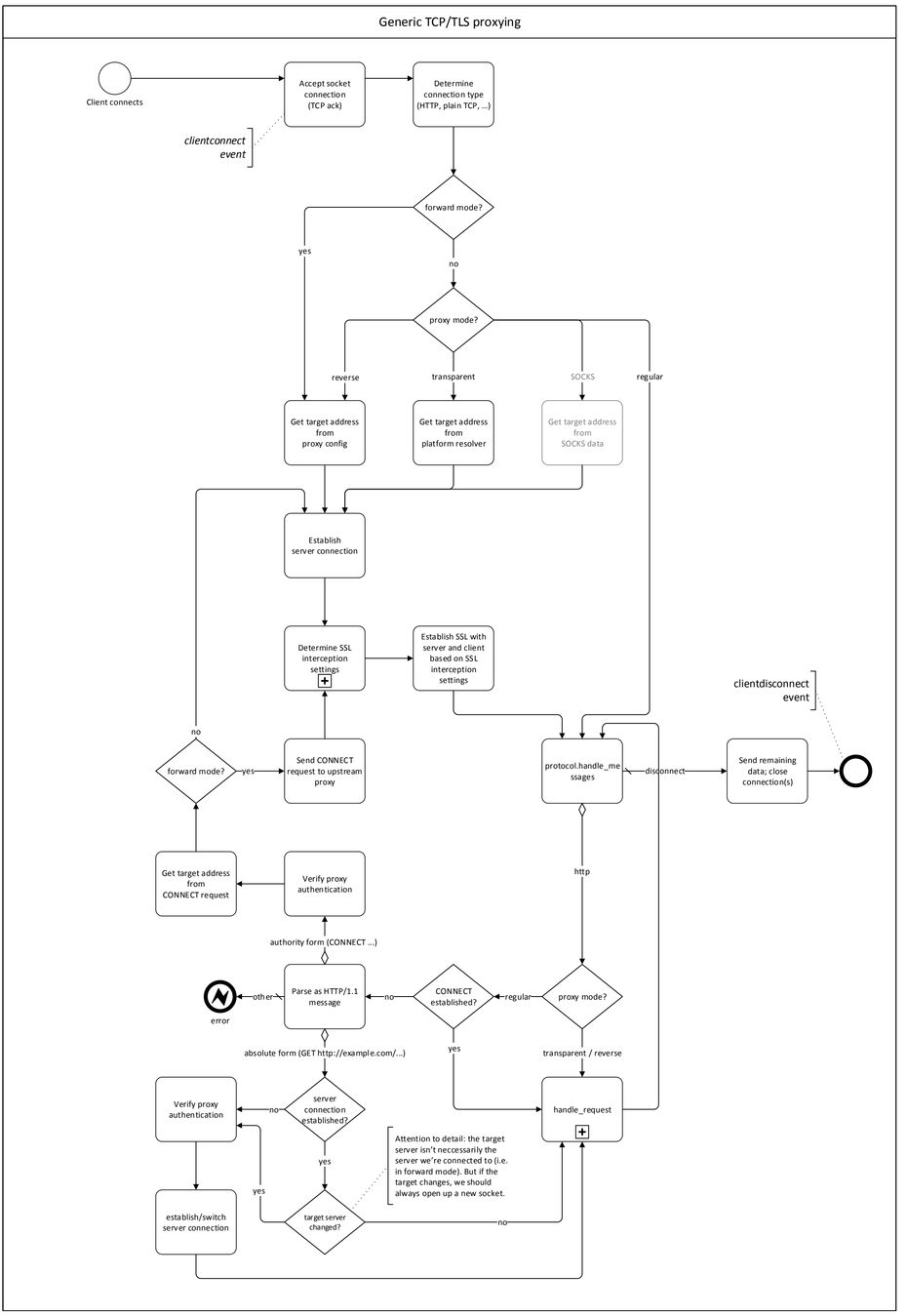

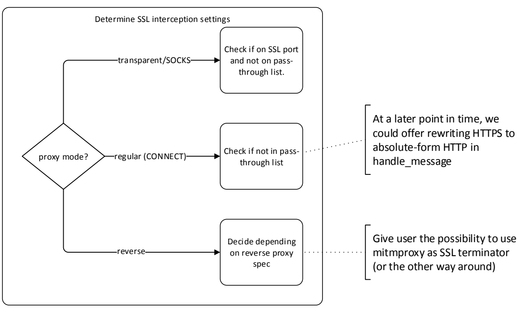

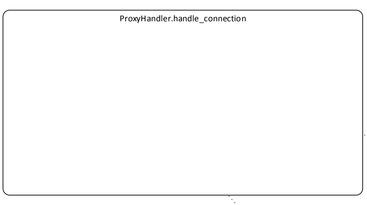

How do we save traffic dumps?
A) tnetstrings as before.
B) SQLAlchemy: Each flow type subclasses the Flow class -> SQLAlchemy docs: Mapping Class Inheritance Hierarchies

HTTP: As before
TCP: Per Connection

When/How do we do HTTP assembly, or, generally speaking $protocol assembly?
This is difficult as we need to delay traffic forwarding if we want to intercept and modify based on higher-level attributes (e.g. HTTP content)

-> Introduce „conntype" attribute of the ProxyHandler that signals the current connection type and allows appropriate protocol assembly. Also, we introduce an InterceptionWatchdog that handles interception rules (for HTTP, TCP and possibly other layer 5-7 protocols) and manages forwarding (incl. streaming).

If we do pass-through (based on exclude list), *conntype* is always TCP.
For reverse proxy mode, we can use the reverse proxy spec to deterministically set the *conntype* (probably just HTTP/S in most cases)
In regular mode without established CONNECT, *conntype* is always HTTP.

In regular mode with intercepted CONNECT, in reverse mode with tcp:// reverse proxy spec (exotic) and in transparent mode (all without pass-through), we can't be sure and need a heuristic. Proposal:
Always use default mode based on port, unless external events occur (e.g. switch to websocket or SSL pass-through).