

Bridge the gap or tunnel straight through!

Studiengang: BSc in Informatik | Vertiefung: Distributed Systems and IoT
Betreuer: Prof. Dr. Reto Koenig

Wer mit wem welche Daten austauschen kann und soll sind offensichtliche Fragen im Zeitalter von IoT und Industrie 4.x. Nicht so offensichtlich ist die Antwort auf die Frage, wie die Daten geteilt werden können. In dieser Thesis wurde untersucht, wie MQTT-Nachrichten zwischen privaten, öffentlich nicht erreichbaren MQTT-Brokern sicher ausgetauscht werden können, ohne dass dafür tiefgreifende Netzwerk-Konfigurationen vorgenommen oder Server im Internet gehostet werden müssen.

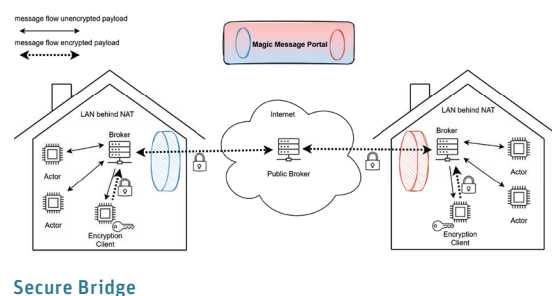
Heutzutage ist es üblich, über das Einrichten eines VPNs oder durch Port-Forwarding einen Zugang zu schaffen, so dass auf private MQTT-Broker von aussen zugegriffen werden kann. Es erfordert jedoch technisches Verständnis und ist aufwändig, die entsprechenden Netzwerk-Konfigurationen vorzunehmen oder die benötigten Hard- und Software-Komponenten zu betreiben. In dieser Bachelorarbeit wurde der Frage nachgegangen, ob schlankere Lösungen möglich sind, die direkt auf der Anwendungsebene eingesetzt und verwaltet werden können. Konkret wurden die Möglichkeiten des «Bridgings», einer Funktionalität von MQTT-Brokern, und die Möglichkeit des «Tunnels» von Daten mit Hilfe von WebRTC untersucht.

Die von uns entwickelte Lösung, das **«Magic Message Portal»**, besteht aus zwei Teilen, dem **«MQTT-Tunnel»** und der **«Secure Bridge»**. Beim MQTT-Tunnel wird mittels WebRTC eine Peer-to-Peer-Verbindung zum Austausch der Daten eingerichtet. Die MQTT-Nachrichten werden über einen WebRTC-Datenkanal direkt zwischen den Brokern in den unterschiedlichen

lokalen Netzwerken ausgetauscht. Wenn das Erstellen eines MQTT-Tunnels nicht möglich ist, z.B. wegen zu restriktiven Firewall-Einstellungen oder ungeeigneten NAT-Verhaltens der Gateways, werden die Nachrichten mit der Secure Bridge über einen potenziell unsicheren, öffentlichen MQTT-Broker gesendet. Um dabei die Vertraulichkeit, Authentizität und Integrität der MQTT-Nachrichten sicherzustellen werden die Nutzdaten vor dem Senden verschlüsselt.



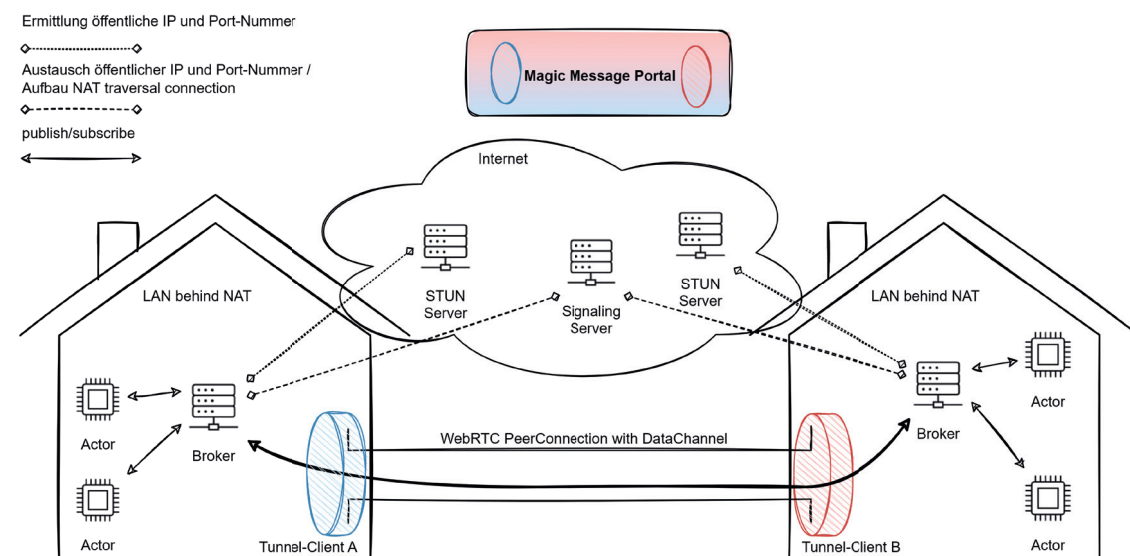
Remo Meyer



Secure Bridge



Markus Salvisberg



MQTT-Tunnel