Scolaris Bridge

Hybride Datenanbindung von Scolaris und Scolaris Market

«Scolaris Bridge» ermöglicht die geschützte und gezielte Anbindung zwischen dedizierten Diensten des Kunden (beispielsweise eine Datenbankinstanz oder ein Service) und den Cloud-Lösungen der PMI.AG (beispielsweise Scolaris Connect). Scolaris Bridge implementiert zeitgemässe Hybridlösungen für die moderne Schulverwaltungslösung Scolaris.

Einrichtung

Im Netzwerk des Kunden wird der Windows Service «Scolaris Bridge Client» installiert. Mittels der mitgelieferten, integrierten Konfigurationsoberfläche bestimmt der Kunde, welche Services verbunden werden sollen. Zwecks Authentifizierung kommt die SSH-Public-Key Authentifizierung zum Einsatz. Die Generierung des Schlüsselpaares (private & public key) erfolgt auf einem Device des Kunden.

Authentifizierung und Autorisierung der verbundenen Services bleiben von «Scolaris Bridge» unberührt.

Zugriff auf Services

Die Services werden durch die Erstellung eines so genannten «Reverse-Port-Forwardings» verfügbar gemacht. Dabei wird auf dem «SSH Relay Server» auf einem TCP-Port gelauscht.

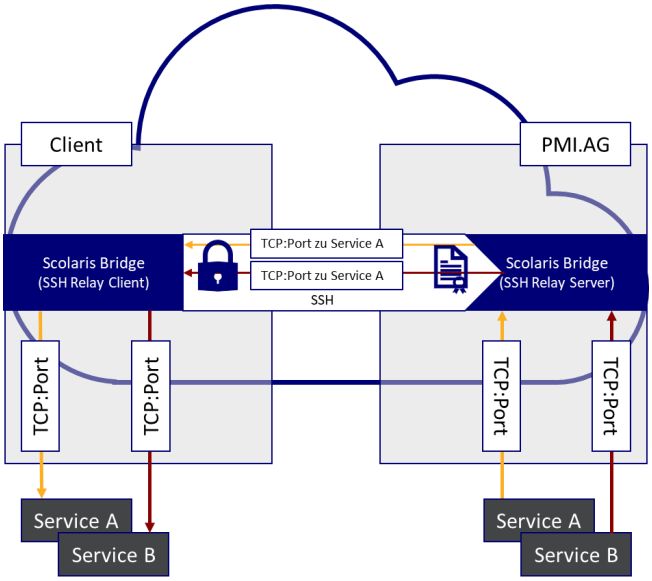
Erfolgt ein Verbindungsaufbau auf diesen Port, werden die Pakete durch die SSH-Verbindung verschlüsselt ins Netzwerk des Kunden übertragen.

Wohin die Daten im Kunden-Netzwerk genau geleitet werden können, wird im «SSH Relay Client» definiert.

Voraussetzungen Firewall

Ausgehende TCP-Verbindungen - Ports 20020 - 20022

62.2.102.160/27	(62.2.102.160 - 62.2.102.191)
77.109.132.64/27	(77.109.132.64 - 77.109.132.95)



Verbindungsaufbau

- Der «SSH Relay Client» stellt eine TCP-Verbindung zum SSH-Endpunkt des «SSH Relay Servers» her.
- «SSH Relay Client» und «SSH Relay Server» einigen sich auf die SSH-Protokollversion und das Verfahren für den Schlüsselaustausch.
- Im Rahmen des Schlüsselaustauschs liefert der «SSH Relay Client» dem «SSH Relay Server» mittels Signatur seinen «public key» und beweist damit, im Besitz des entsprechenden «private key» zu sein.
- Der «SSH Relay Client» prüft den «public key» des Servers gegen die lokale Konfiguration.
- Die Authentifizierung durch den «SSH Relay Client» erfolgt durch die Erstellung einer digitalen Signatur mit dem «private key». Ist der passende «public key» beim Server gelistet, ist die Authentifizierung erfolgreich und die SSH-Verbindung ist etabliert.
- Die «Port-Forwardings» werden aktiviert.

PMI.AG
Projektmanagement & Informatik AG
Aarau – Bellinzona – Lausanne

März 2020