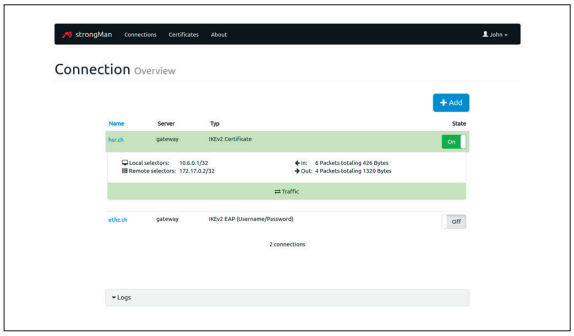
Severin Bühler

Samuel Kurath

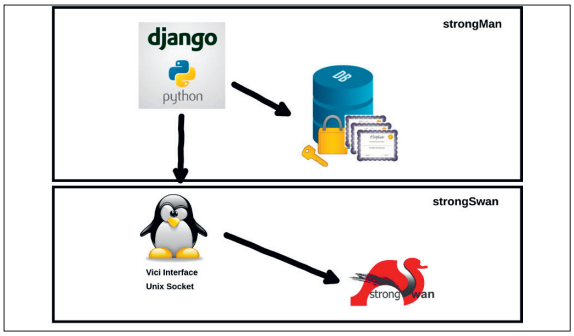
Diplomanden	Severin Bühler, Samuel Kurath
Examinator	Prof. Dr. Andreas Steffen
Experte	Dr. Ralf Hauser, PrivaSphere AG, Zürich, ZH
Themengebiet	Sicherheit

Django Management Tool für strongSwan

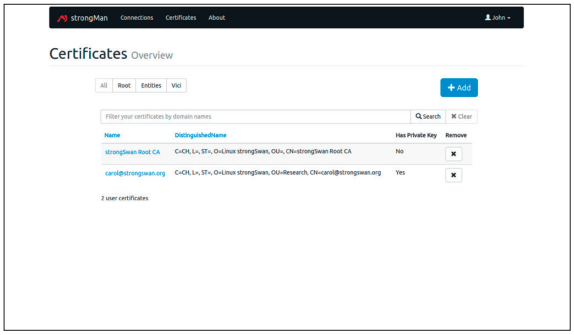
Management UI für strongSwan



Laufende Verbindung in strongMan



Architekturübersicht



Zertifikatsübersicht

Ausgangslage: strongSwan ist eine IPsec-basierte Open-Source-VPN-Lösung für verschiedene Betriebssysteme, die standardmässig über Konfigurationsdateien und eine Kommandozeilenanwendung verwaltet wird. Diese Vorgehensweise richtet sich hauptsächlich an erfahrene Systemadministratoren und ist nur schwer brauchbar für normale Benutzer ohne grosse Informatikerfahrung. Deshalb besteht schon länger eine Nachfrage für eine grafische Management-Oberfläche, diee das Konfigurieren und Starten von IPsec-Verbindungen erleichtern soll.

Vorgehen/Technologien: Zur Lösung dieses Problems stellt strongSwan das neue Versatile IKE Configuration Interface (VICI) zur Verfügung, das für diverse Skriptsprachen eine JSON-artige Schnittstelle bietet. Im Rahmen dieser Bachelorarbeit ist die «strongMan»-Applikation entstanden, die auf dem Python Web-Framework Django basiert. Mit einem eigenen Docker-Setup für das Testing wurde der Entwicklungsprozess stark erleichtert.

Ergebnis: strongMan unterstützt eine benutzerfreundliche Konfiguration diverser Internet-Key-Exchange(IKEv2)-Authentisierungsmethoden, die in einer Datenbank persistiert werden. Diese können auf der Hauptübersicht bearbeitet werden. Weiter lassen sich diese Verbindungen auf- und abbauen. Das Starten einer Verbindung hat zur Folge, dass strongMan die Konfigurationsdaten in ein Dictionary umwandelt und dem strongSwan Daemon über die VICI-Schnittstelle übergibt, wobei für die Kommunikation ein Unix Socket verwendet wird. Ist die Verbindung erfolgreich etabliert, können Status-Informationen zu Traffic Selectoren, sowie zum übermittelten Datenvolumen dargestellt werden. Parallel dazu werden die Log-Einträge des strongSwan Daemons ausgelesen und visualisiert. Die interne Zertifikatsverwaltung ermöglicht den Upload von PKCS#1, PKCS#8, PKCS#12 Schlüsseldateien, sowie von X.509 Zertifikaten. Diese werden in einer Datenbank gespeichert, wobei alle sensitiven Daten verschlüsselt abgelegt werden. Nach dem Erfassen können wichtige Felder wie der Canonical Name (CNAME) direkt in der Zertifikatsvorschau eingesehen werden. Zusätzlich werden auch alle durch strongSwan verwalteten Zertifikate in der strongMan-Applikation dargestellt. Zusätzlich bietet eine Informationsseite eine Übersicht über die verwendete strongSwan-Version und allen installierten Plugins.