



Raffael
Fischer



Daniel
Kolb

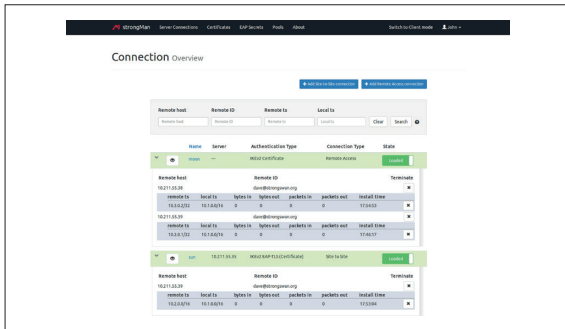


Josip
Valencic

Diplomanden	Raffael Fischer, Daniel Kolb, Josip Valencic
Examinator	Prof. Dr. Andreas Steffen
Experte	Dr. Ralf Hauser, PrivaSphere AG, Zürich, ZH
Themengebiet	Sicherheit

strongMan Management-Tool-Erweiterung für grosse VPN Server

Intuitives, modernes Web-Interface auf der Basis von Python/Django



Ausgangslage: Für «strongSwan», die IPsec-basierte und einzige Open-Source-VPN-Lösung mit vollständiger IKEv2-Implementation, existierte bereits eine Webanwendung namens «strongMan». Sie bot die Möglichkeit, für Clients Zertifikate zu verwalten und Verbindungen zu einem VPN-Server aufzubauen. Ziel dieser Bachelorarbeit war es, strongMan um einen Server-Modus für Administratoren zu erweitern. Dieser neu zu implementierende Server-Modus sollte somit das Gegenstück zum existierenden Client-Modus darstellen. Er soll Verbindungen von Clients, Verbindungen zu einem anderen strongSwan-VPN-Server, Server-Zertifikate, Benutzernamen und Passwörter sowie IP-Address-Pools verwalten können.

Vorgehen/Technologien: Das bestehende strongMan-Projekt für VPN-Clients wurde in Python implementiert und verwendet das Web-Framework Django. Für die Persistenz der Daten wurde die leichtgewichtige Datenbank SQLite verwendet. Die Kommunikation mit dem strongSwan-Daemon, der das VPN-Backend darstellt, erfolgte via Unix-Socket. Um eine möglichst einfache Integration zu garantieren, wurde im Server-Modus auf den gleichen Technologie-Stack gesetzt.

Ergebnis: Es entstand ein vollumfänglicher Server-Modus, der durch die gegebenen Anforderungen einer einfachen, übersichtlichen und sinnvollen Anwendung für Systemadministratoren dient. Als grosse Herausforderung stellte sich der Umgang mit vielen Verbindungen und deren übersichtliche Darstellung heraus. Dazu kam die Schwierigkeit der Visualisierung der Daten aus der eigenen Datenbank, kombiniert mit Live-Daten aus dem strongSwan-Daemon via Unix-Socket. Dank flexiblen und detaillierten Filterfunktionen, die auf den Listen der Connections agieren, können heute jedoch problemlos mehrere Hundert Verbindungen verwaltet und übersichtlich dargestellt werden. Eine übersichtliche Darstellung auch ohne Filterung wurde erreicht, indem zum Beispiel aufklappbare Tabellen für Detailinformationen oder Scrollbars für viele Einträge innerhalb einer aufgeklappten Untertabelle implementiert wurden. Sollte das VPN-Backend oder sogar der ganze VPN-Server einmal neu gestartet werden, wird vom neuen Server-Modus direkt die komplette Konfiguration aller Verbindungen, Benutzernamen und Passwörter, Zertifikaten und Pools wieder in den strongSwan Daemon geladen und somit die aktuellen Status der Verbindungen und deren Clients in Echtzeit angezeigt. Nebenbei kann vom Server-Modus einfach per Knopfdruck in den simplen Client-Modus und auch wieder zurück gewechselt werden.

