Philip
Bötschi

Adrian
Dörig

Webmanager für IKEv2 Mediation Service

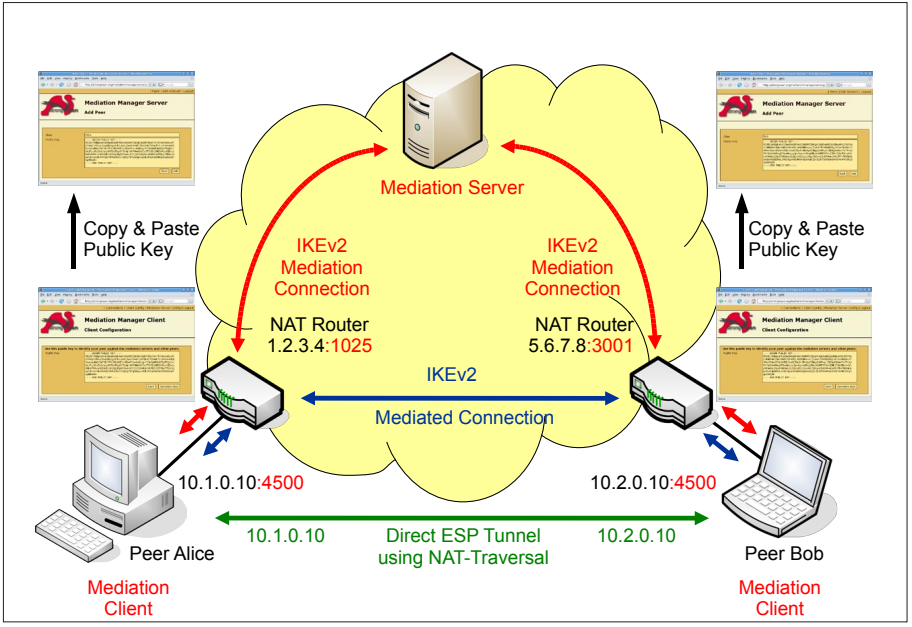
Diplomanden	Philip Bötschi, Adrian Dörig
Examinator	Prof. Dr. Andreas Steffen
Experte	Prof. Dr. Ralf Hauser, PrivaSphere AG, Zürich
Themengebiet	Internet-Technologien -Anwendungen
Projektpartner	ITA Institut für Internet-Technologien und -Anwendungen, HSR, Rapperswil-Jona SG

Aufgabenstellung: Die Open-Source-VPN-Software strongSwan ermöglicht es, eine direkte IPsec-VPN-Verbindung zwischen zwei Computern, welche sich je hinter einem NAT-Router befinden, herzustellen. Für den Aufbau einer solchen Verbindung sind die Vermittlungsdienste eines Mediation Servers notwendig. Die strongSwan Erweiterung dafür wurde von HSR-Diplomanden entwickelt.

Die HSR möchte einen öffentlichen Mediation Server zur Verfügung stellen, damit dieses Verfahren getestet werden kann. Voraussetzung dafür ist ein benutzerfreundliches Webinterface, um die Verbindung zu konfigurieren.

Ziel der Arbeit: Es soll eine Web Applikation realisiert werden, mit der das Erstellen einer Mediation-Server-vermittelten Peer-to-Peer-Verbindung einfach möglich ist. Dabei soll eine hohe Sicherheit für die gegenseitige Authentifizierung der drei Parteien gewährleistet werden.

Lösung: Es wurde sowohl für den Mediation Server als auch für den Mediation Client eine Web-Applikation entwickelt. Über diese können



Schematische Darstellung der realisierten Lösung

Mediation-Server-vermittelte Peer-to-Peer-Verbindungen einfach konfiguriert werden. Es wird definiert, zu welchem Client und über welchen Mediation Server eine IPsec-VPN-Verbindung hergestellt werden soll.

Für die Authentisierung verwendet jeder Partner ein RSA-Public/Private-Key-Paar. Dies bietet eine hohe Sicherheit bei gleichzeitig einfacher Handhabung. Es müssen jeweils nur die Public Keys mittels Copy & Paste zwischen den Parteien ausgetauscht werden.

Die realisierte Lösung wird fester Bestandteil des strongSwan-Projektes.

Weitere Informationen zu strongSwan:
www.strongswan.org