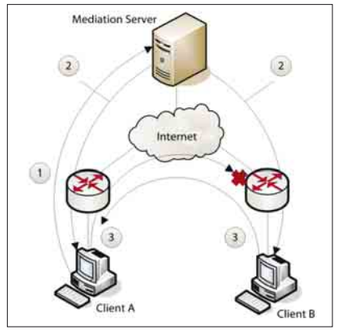
Peer-to-Peer NAT Traversal for IPsec


Tobias
Brunner


Daniel
Röthlisberger

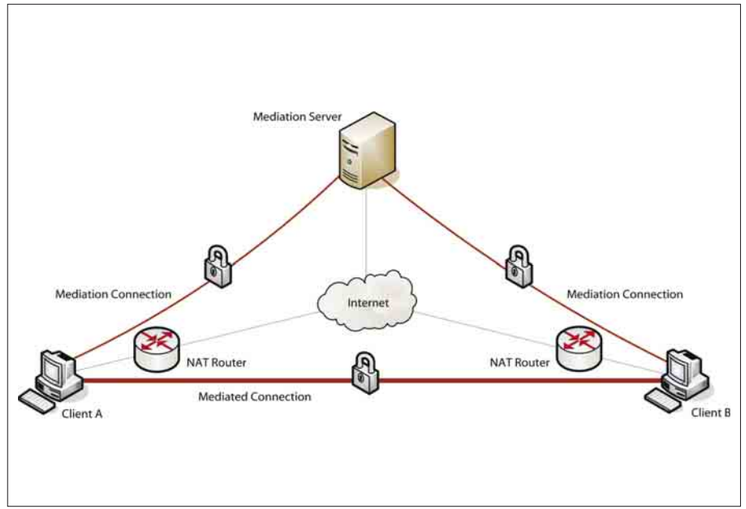
Diplomanden	Tobias Brunner, Daniel Röthlisberger
Examinatoren	Prof. Dr. Andreas Steffen, Martin Willi
Experte	Dr. Ralf Hauser, PrivaSphere, Zürich
Themengebiet	Internet-Technologien und -Anwendungen



Hole Punching

Aufgabenstellung: IPsec ist ein Standard für Virtual Private Networks (VPNs) auf IP-Basis. Internet Key Exchange v2 (IKEv2) ist die neue Generation des verwendeten Schlüsselaustausch-Protokolls. Im heutigen Internet sind Network Address Translations (NATs) weit verbreitet. LANs sind häufig über eine einzige öffentliche IP-Adresse eines NAT-Routers mit dem Internet verbunden. Verbindungen sind im Allgemeinen nur von innen nach aussen möglich. IPsec erlaubt mit NAT Traversal zwar das Überqueren von einfachen NAT von innen nach aussen, nicht aber Direktverbindungen in Situationen, wo sich beide Peers je hinter NAT befinden. Hole Punching ist eine Technik für die direkte Kommunikation in solchen Double-NAT-Situationen.

Ziel der Arbeit: Mit Hilfe von Hole Punching auf der Basis von IPsec und IKEv2 VPN sollen Direktverbindungen zwischen zwei Hosts hergestellt werden, welche sich beide hinter NAT befinden, ohne dazu die NAT-Router speziell konfigurieren zu müssen. Zusätzlich war eine Proof-of-Concept-Implementation zu entwickeln.



Verschlüsselte Direktverbindung zwischen Client A und B, vermittelt über einen Mediation Server

Lösung: Mit Peer-to-Peer NAT Traversal (P2P-NAT-T) ist eine IPsec-Erweiterung entstanden, welche es ermöglicht, Verbindungen auch in Double-NAT-Situationen direkt End-zu-End aufzubauen. Wir definieren dazu ein auf IKEv2 basierendes Protokoll zur Kommunikation mit einem Mediation Server. Je nach Verhalten der NAT-Router ist es möglich, dass keine direkte Verbindung zustande kommen kann. Für diesen Fall definieren wir zusätzlich eine Relay-Erweiterung, welche es erlaubt, IPsec-Traffic unter Beibehaltung der vollen End-zu-End-Sicherheit über den Mediation Server umzuleiten. Als Proof-of-Concept haben wir die freie, linuxbasierte IPsec-Lösung strongSwan mit P2P-NAT-T-Unterstützung (ohne Relay) ausgestattet. Unsere Arbeit wird im Rahmen von strongSwan weiterentwickelt werden. Geplant ist, P2P-NAT-T als Internet Draft zu publizieren, um allenfalls eine Standardisierung als RFC anzustreben.