Laborübung zu VPN mittels IPsec

Allgemeine Hinweise für die Durchführung unter Linux:
Im Meta-Paket `ipsec-tools` befinden sich die notwendigen Programme, um die SAD[1] und SPD[2] zu konfigurieren. Das entscheidende Programm lautet `setkey` und kann mittels einer Konfigurationsdatei beeinflusst werden. **Für beide Seiten wird eine eigene Konfigurationsdatei benötigt.** Zunächst werden mittels der beiden `flush`-Befehle die SAD und SPD gelöscht, damit es keine Beeinflussung mit alten Einträgen gibt. Im Anschluss werden zunächst die SAs für beide Richtungen angelegt und zum Schluss die Policies für die entsprechenden Richtungen (hier sind Source und Destination sowie die Richtung von Bedeutung).

1. Aufgabe: IPsec im manuell konfigurierten[3] Transport-Modus (End-to-End)

Das Szenario umfasst ein vereinfachtes Modell, bei dem das öffentliche Internet über einen Router (eigener PC) repräsentiert wird. Das folgende Schaubild zeigt den prinzipiellen Aufbau. Die beiden Kommunikationspartner (Amy und Berny) sollen die VPN-Verbindung aufbauen.

Als IPsec Protokoll soll **AH** im **Transport-Modus** verwendet werden. Nach erfolgreichem Aufbau soll auf dem Router die Kommunikation zwischen den beiden Endstationen mitgeschnitten werden oder über einen weiteren Hub.

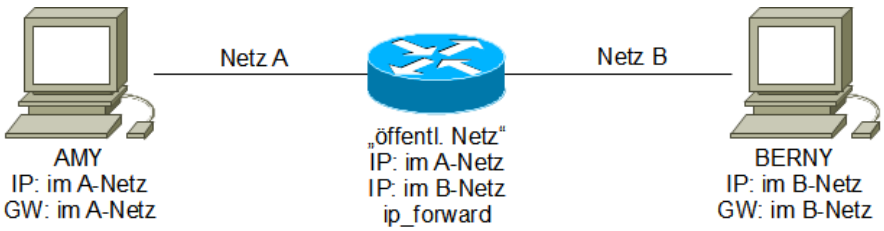

Abbildung 1: VPN: End-to-End im Transport-Modus (manuell konfiguriert)

2. Aufgabe: IPsec im manuell konfigurierten[4] Tunnel-Modus (End-to-End)

Aktivieren Sie in dieser Aufgabe **ESP** sowie den **Tunnel-Modus** und protokollieren Sie wieder auf dem Router. **Zeichnen** Sie erneut **auf** und **notieren** Sie die **Änderung** zu Aufgabe 1.

3. Aufgabe: IPsec mit automatisch ausgehandelten Schlüsseln

Für die automatische Aushandlung der Schlüssel können unterschiedliche Produkte zum Einsatz kommen. Allen gemeinsam ist das IKE bzw. das darin verwendete ISAKMP. In dieser Laborübung wird `racoon` eingesetzt. `StrongSWAN` oder `OpenSWAN`[5] sind Alternativen hierzu. Weiterhin soll in dieser Aufgabe eine **Site-to-Site-Verbindung** zwischen zwei LANs über zwei VPN-Gateways aufgebaut werden.

Protokollieren Sie auf der Strecke zwischen Amy und Berny (auf dem Router) die **ISAKMP-Nachrichten** sowie die Nachrichten, die **zwischen Client 1 und Client 2 transportiert** werden.

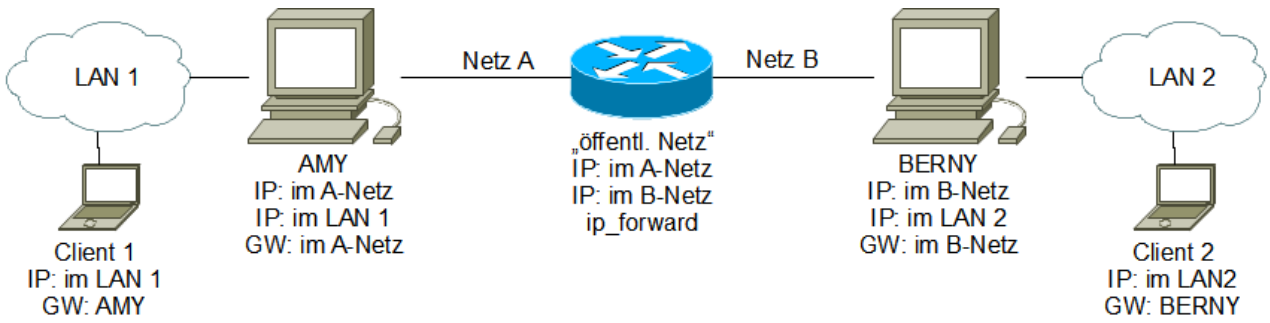

Abbildung 2: VPN: Site-to-Site im Tunnel-Modus (automatisch konfiguriert)

1 SAD: Security Assoziation Database
2 SPD: Security Policy Database
3 ohne IKE/ISAKMP
4 ohne IKE/ISAKMP
5 SWAN: Secure WAN