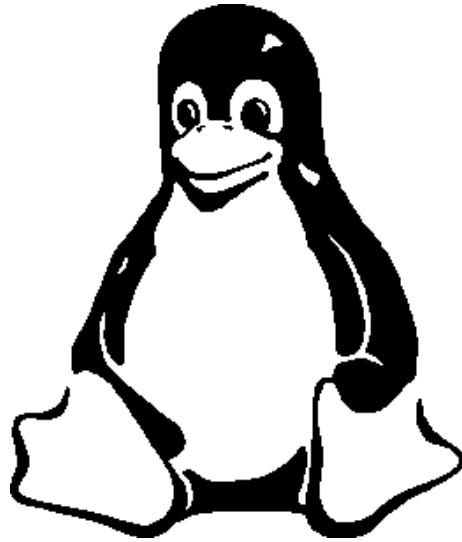


VPN – Virtual Private Network



Martin Erleben
Magdeburger Linux User Group e.V.



Einführung

- Begriffsklärung und Motivation
- Realisierungsmöglichkeiten
- IPsec
- Ausblick



VPN

- VPN – Eine Begriffsklärung
 - privates Netzwerk
 - Nutzdaten bleiben vertraulich
 - Teilnehmer bleiben nach außen geheim
 - über ein öffentliches Medium (Internet)



Motivation

- Warum ein VPN?
 - Verlust der Privatsphäre
 - Verlust der Datenintegrität
 - Sichere Kommunikation
 - Kommunikationskosten



Anforderungen

- Authentifizierung
- Integrität
- Abhörsicherheit
- Identitätsverbergung
- Schutz des lokalen Netzes
- Interoperabilität



Grundlagen

- Kryptographie
- Hash-Verfahren
- Tunneling



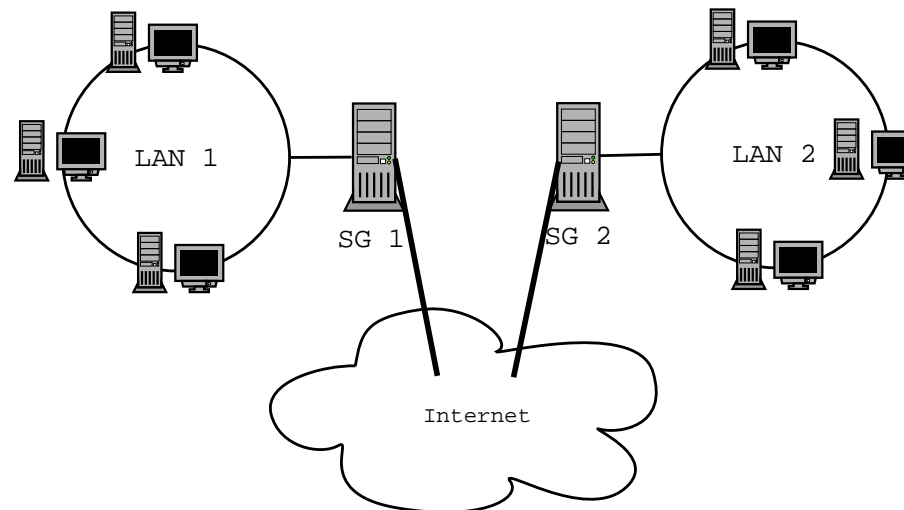
Topologien

- Site-to-Site
- Host-to-Host
- Host-to-Site



Site-to-Site

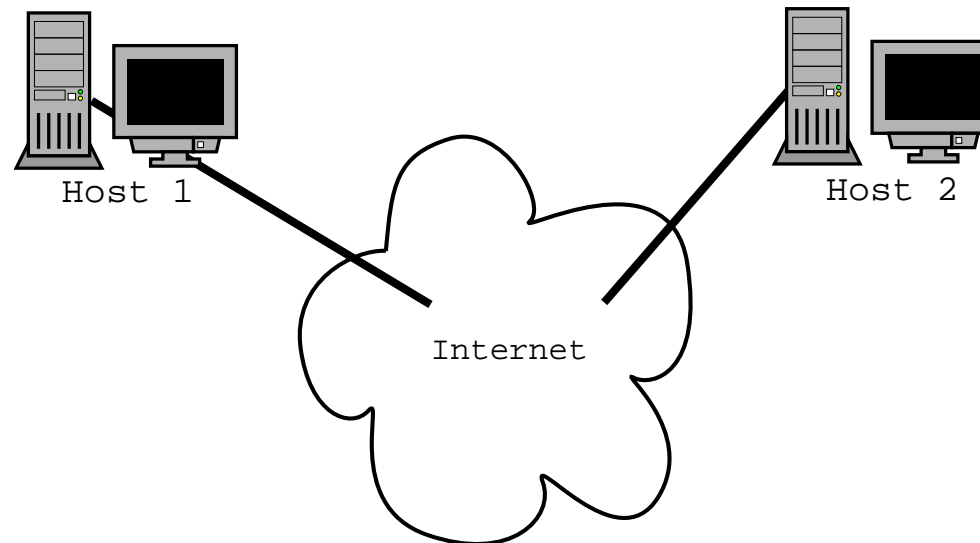
- Verbindung mehrere lokaler Netzwerke
- nur Gateways verfügen über VPN Software
- VPN transparent für Endgeräte





Host-to-Host

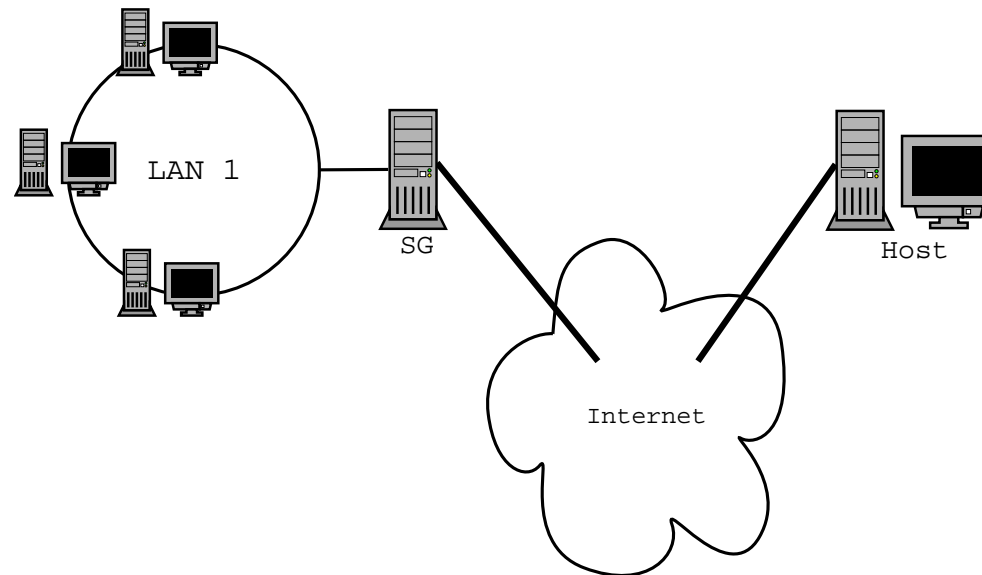
- direkte Verbindung zweier Rechner
- beide Endgeräte verfügen über VPN Software





Host-to-Site

- Mobile Endgeräte von Außendienstmitarbeitern (Road Warrior)
- Endgerät und Gateway verfügen über VPN Software





Realisierungsmöglichkeiten

- IPsec
- L2TP
- PPTP



L2TP/PPTP

- werden häufig für Wählleitungen verwendet
- Erweiterungen von PPP
- andere Protokolle können getunnelt werden (IPX/SMB/usw.)



IPsec(1)

- von der IETF entwickelt
- Erweiterung für IPv4
- ist fester Bestandteil von IPv6
- bietet Authentifizierung, Integrität und Vertraulichkeit



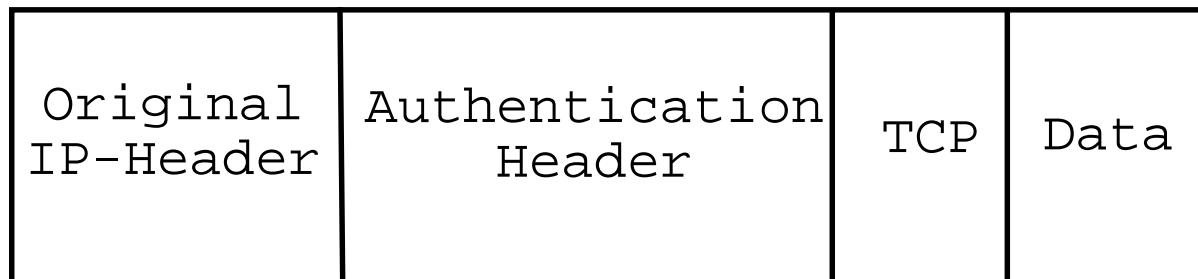
IPsec(2)

- Bestandteile des IPsec Standards
 - Authentication Header (AH)
 - Encapsulating Security Payload (ESP)
 - Internet Security Association Key Managment Protocoll (ISAKMP)
- können zusammen und auch einzeln verwendet werden



IPsec - Authentication Header

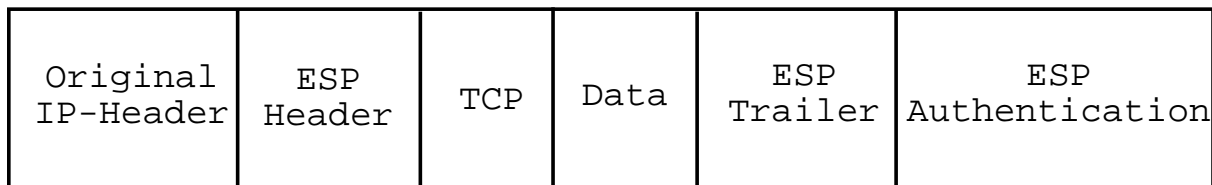
- stellt Integrität und Authentizität der Daten sicher
- das Original IP Paket wird um AH verlängert
- es werden Hash-Methoden verwendet





IPsec – Encapsulating Security Payload

- stellt Vertraulichkeit, Integrität und Authentizität der Daten sicher
- Original IP Paket wird verschlüsselt und in neues Paket verpackt





IPsec – Transportmodus

- Nutzdaten werden verschlüsselt
- Quell- und Zieladressen sind einsehbar



IPsec – Tunnelmodus

- Nutzdaten und Header werden verschlüsselt
- verschlüsselte Daten werden Nutzdaten eines neuen IP Paketes
- nur Tunnelendpunkte können identifiziert werden



VPN und Linux

Existierende Lösungen für:

- IPsec – FreeS/WAN
- PPTP – pptp Project
- L2TP – l2tp Project



Zusammenfassung

- wird in Zukunft weiter an Bedeutung zunehmen
- Offenlegung der Verfahren wird Vertrauen erhöhen
- Sicherheit besteht nicht allein aus VPN Software