Proseminar Rechnernetze

NAT & VPN

Adressübersetzung und Tunnelbildung

Bastian Görstner

Gliederung

1. **NAT**
    1. Was ist ein NAT
    2. Kategorisierung

2. **VPN**
    1. Was heißt VPN
    2. Varianten
    3. Tunneling
    4. Security

NAT = Network Address Translation

- Einsatzgebiet: Router und Firewalls
- Ziel: Port und IP Adressen auf andere abzubilden
- Vorteil: Möglichkeit IPv4 Adressknappheit zu lösen
  Schutz vor Angriffen aus dem Internet
- Nachteil: keine End–to–End Kommunikation möglich

Source NAT

Es erfolgt eine Ersetzung der Quell-IP Adresse

local	
Quell-IP	**Ziel-IP**
192. 168.1.1	84.56.214.162
192. 168.1.2	84.56.214.162
192. 168.1.3	84.56.214.162
192. 168.1.4	84.56.214.162

öffentlich	
Quell-IP	**Ziel-IP**
64.233.183.99	84.56.214.162
66.205.71.102	84.56.214.162
132.230.167.230	84.56.214.162
195.71.11.67	84.56.214.162

Source NAT

Es erfolgt eine Ersetzung der Quell-IP Adresse

local			öffentlich	
Quell-IP	**Ziel-IP**		**Quell-IP**	**Ziel-IP**
192. 168.1.1	84.56.214.162	NAT →	64.233.183.99	84.56.214.162
192. 168.1.2	84.56.214.162		66.205.71.102	84.56.214.162
192. 168.1.3	84.56.214.162		132.230.167.230	84.56.214.162
192. 168.1.4	84.56.214.162		195.71.11.67	84.56.214.162

Mapping von privater Quell-IP auf öffentliche Quell-IP wird gespeichert

192.168.1.1 <-> 64.233.183.99
192.168.1.2 <-> 66.205.71.102
192.168.1.3 <-> 132.230.167.230
192.168.1.4 <-> 195.71.11.67

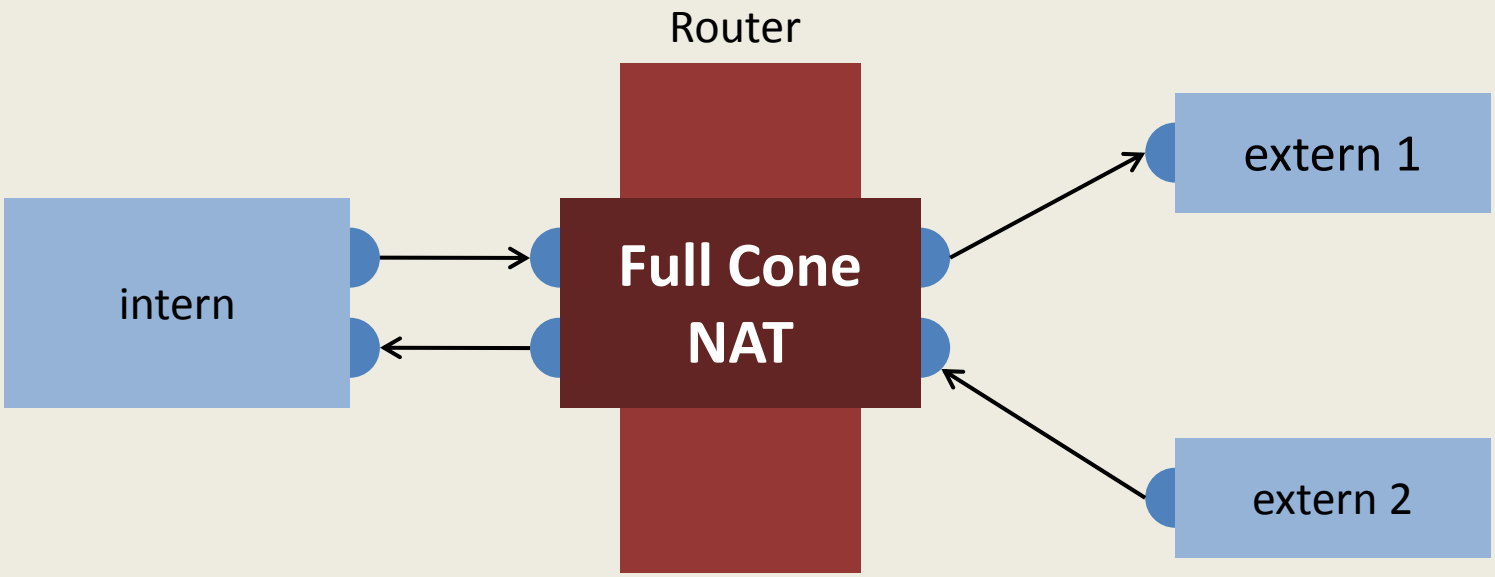
Destination NAT

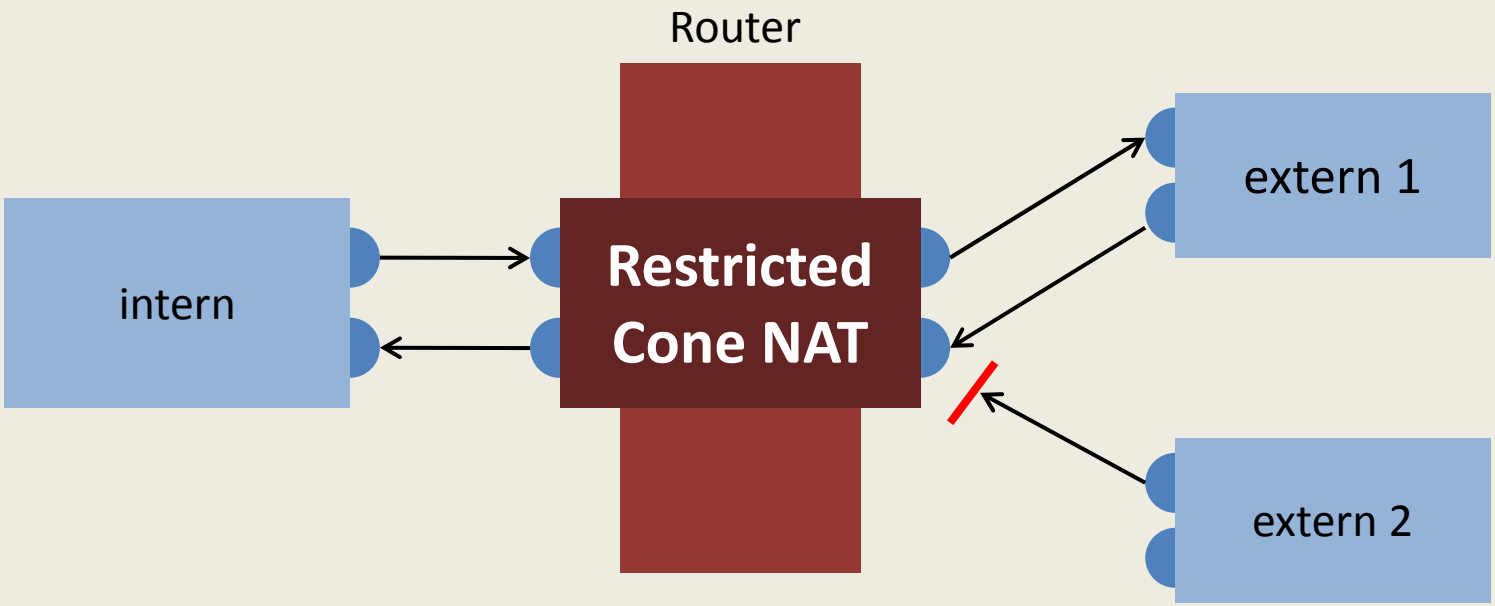
local	
Quell-IP	**Ziel-IP**
84.56.214.162	192. 168.1.1
84.56.214.162	192. 168.1.2
84.56.214.162	192. 168.1.3
84.56.214.162	192. 168.1.4

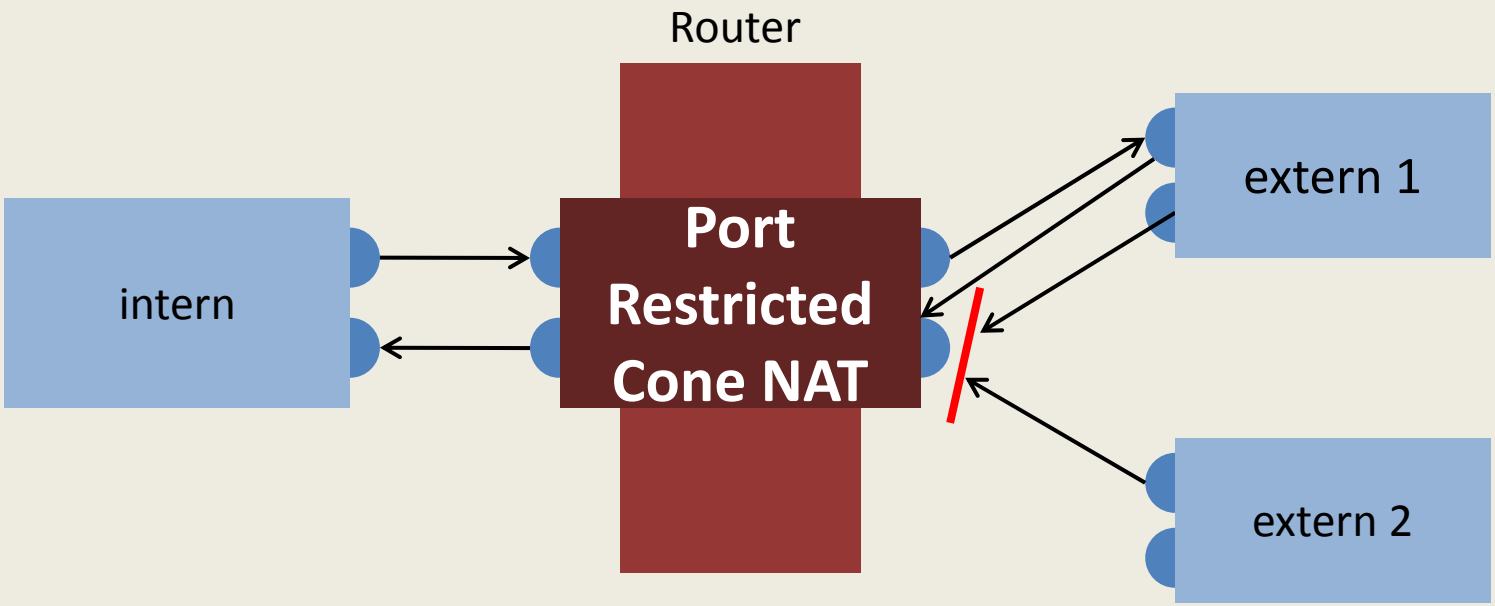
NAT

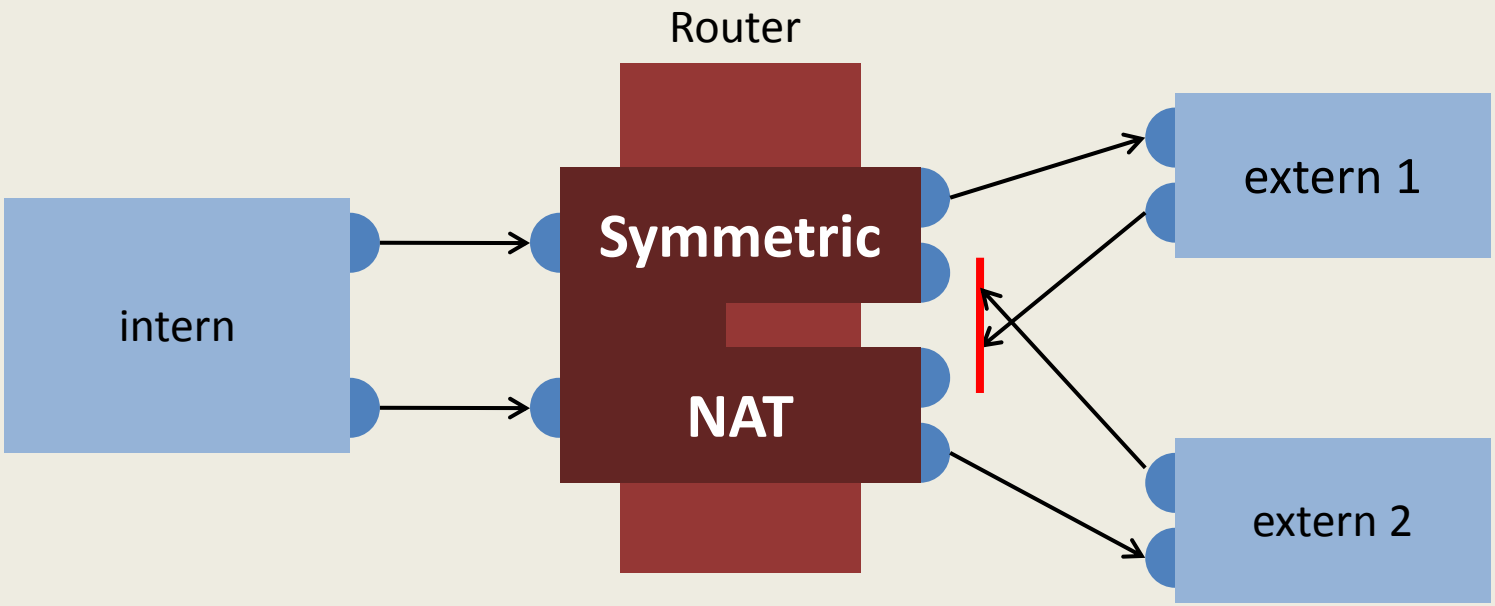
öffentlich	
Quell-IP	**Ziel-IP**
84.56.214.162	64.233.183.99
84.56.214.162	66.205.71.102
84.56.214.162	132.230.167.230
84.56.214.162	195.71.11.67

Klassifizierung nach rcf 3489




Router
intern
Restricted
Cone NAT
extern 1
extern 2

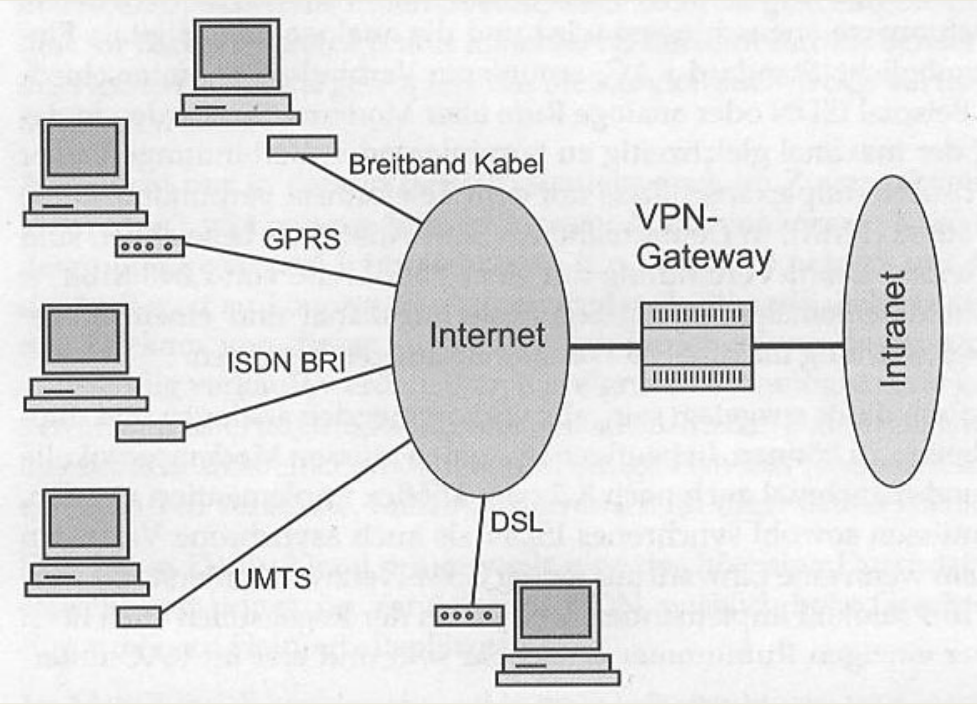

Router
intern
Port
Restricted
Cone NAT
extern 1
extern 2


Router
Symmetric
NAT
intern
extern 1
extern 2

VPN = Virtuelle Private Netzwerke

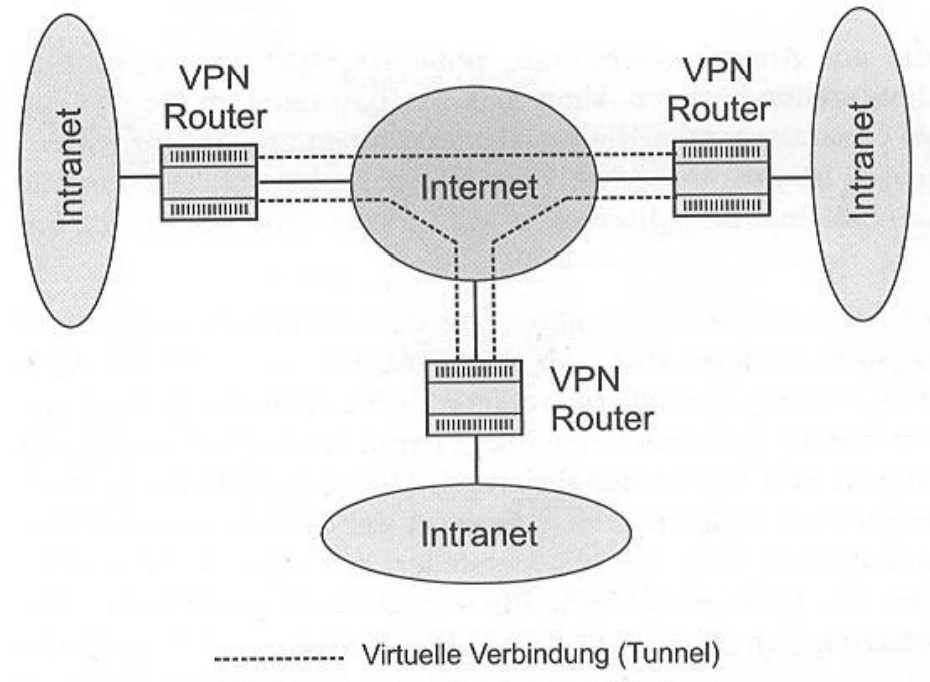
- Verwendung eines öffentlichen Netzes zum Transport privater Daten
- Zunehmende Bedeutung durch Globalisierung und Dezentralisierung

Remote Access VPN



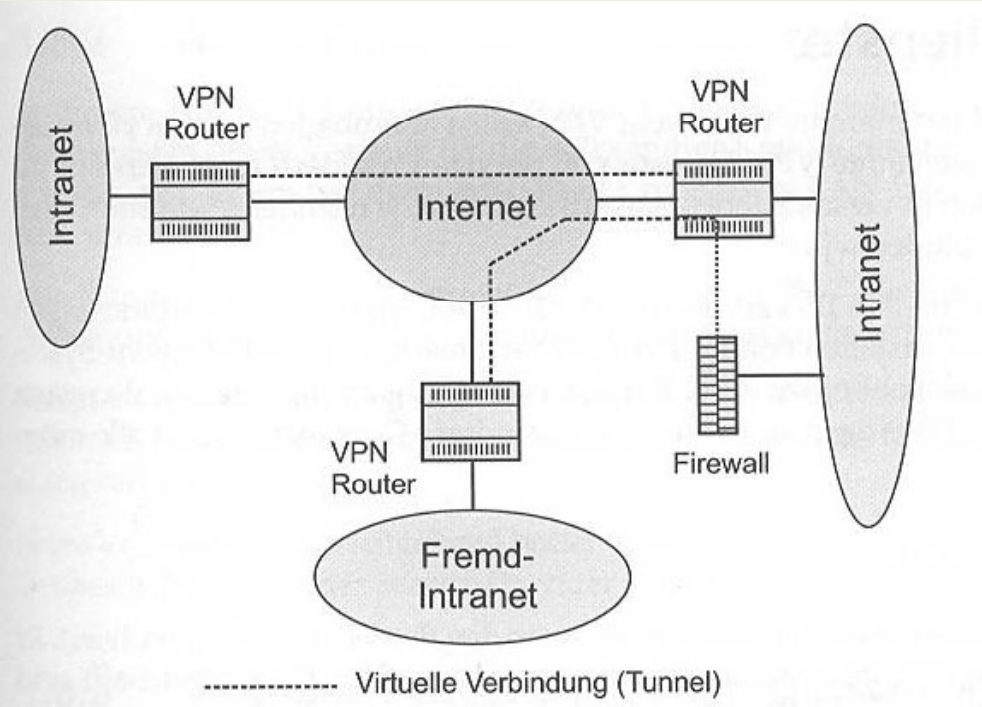
Manfred Lipp: Remote Access VPN in VPN Aufbau und Sicherheit, Seite 42

Branch Office VPN



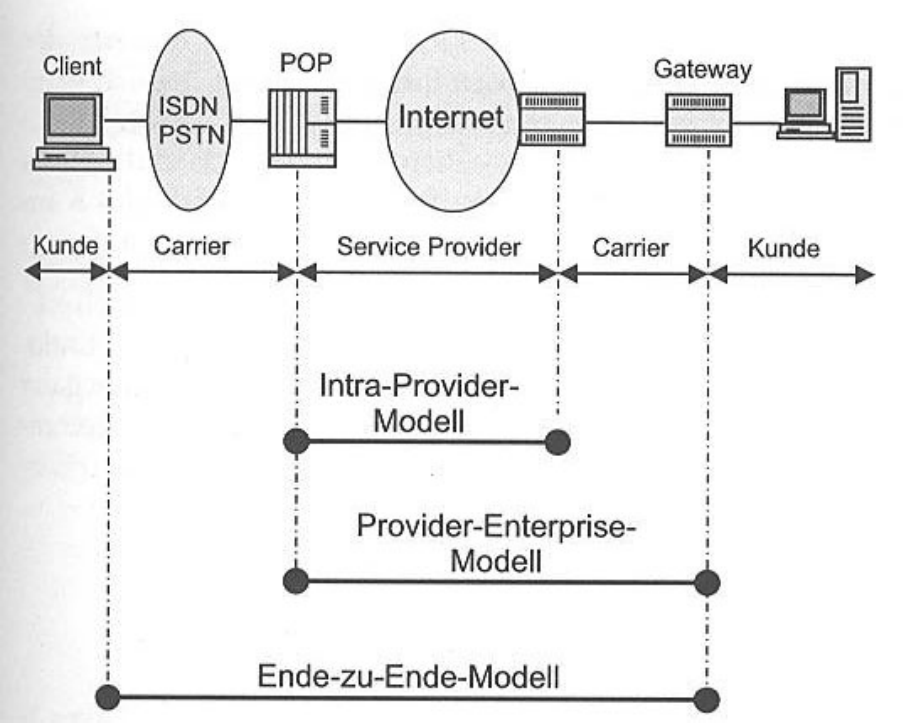
Manfred Lipp: Branche Office VPN in VPN Aufbau und Sicherheit, Seite 44

Extranet VPN



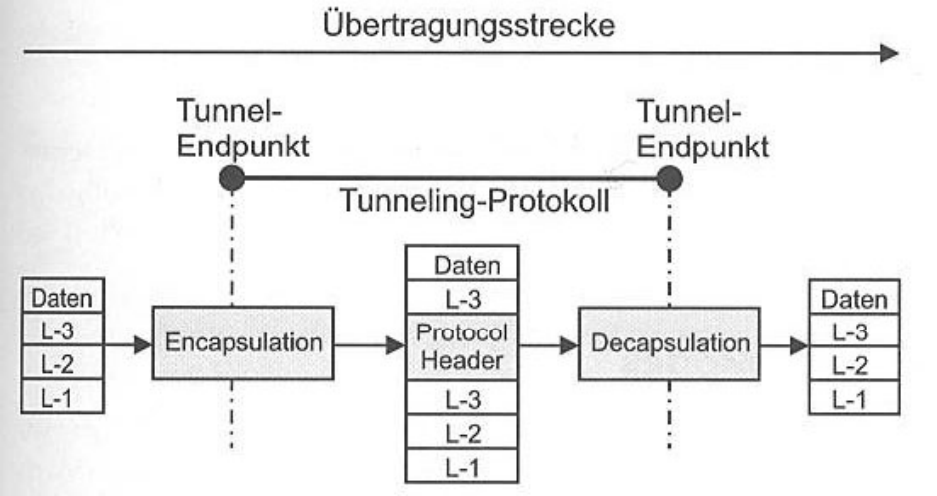
Manfred Lipp: Extranet-VPN in VPN Aufbau und Sicherheit, Seite 45

Tunnelmodelle



Manfred Lipp: Tunneling- Modelle in VPN Aufbau und Sicherheit, Seite 77

Das Layer-3-Tunneling-Protokoll (L3TP)



Manfred Lipp: das Prinzip Tunneling- Protokolle in VPN Aufbau und Sicherheit, Seite 76

- Tunnelbildung findet auf der Netzwerkschicht statt
- wird als End-to-End-Modell verwendet

Das Layer-2-Tunneling-Protokoll (L2TP)

- vornehmlicher Einsatz als Provider – Enterprise – Modell
- Verkapselung erfolgt auf Sicherungsschicht (Layer 2)
- Transport der Daten bis zum Provider erfolgt per PPP
- Remote Access Connector (RAC) unterscheidet ob es sich um normale Internet oder VPN Daten handelt
- beinhaltet keine Sicherheitsmechanismen

Anforderungen:

1. Sicherheit
2. Verfügbarkeit
3. Koexistenz
4. Quality of Service
5. Skalier – und Migrationsfähigkeit
6. Integration in bestehende Netze
7. Interoperabilität
8. Adressmanagement

Sicherheitsziele:

1. Vertraulichkeit
2. Authentizität
3. Integrität
4. Schutz vor wiederholten Senden
5. Identifikation
6. Schutz vor Angriffen auf das gesamte VPN-System

Verschlüsselungsalgorithmen:

Symmetrische Verfahren:

Sender und Empfänger nutzen denselben Schlüssel
Beispiel: DES, Triple-DES, AES

Verschlüsselungsalgorithmen:

Symmetrische Verfahren:

Sender und Empfänger nutzen denselben Schlüssel
Beispiel: DES, Triple-DES, AES

Asymmetrische Verfahren:

Sender und Empfänger nutzen 2 verschiedene Schlüssel
Sender verschlüsselt mit Public Key
Empfänger entschlüsselt mit dem nur ihn bekannten Private Key
Beispiel: Diffie-Hellman, RSA

DES = Data Encryption Standard

- Symmetrisches Verschlüsselungsverfahren
- 64-Bit Klartext wird mit Hilfe eines 54-Bit Schlüssels in einen 64-Bit Codierten Text überführt
- Verbesserungen: Triple – DES oder AES

DES = Data Encryption Standard
- Symmetrisches Verschlüsselungsverfahren
- 64-Bit Klartext wird mit Hilfe eines 54-Bit Schlüssels in einen 64-Bit Codierten Text überführt
- Verbesserungen: Triple – DES oder AES

RSA = benannt nach Ron Rivest, Adi Shamir und Len Adleman
- asymmetrisches Verfahren
- beruht auf Primfaktorzerlegung einer großen Zahl
- public Key: $C = M^e \bmod n$
- private Key: $M = C^d \bmod n$

IPSEC

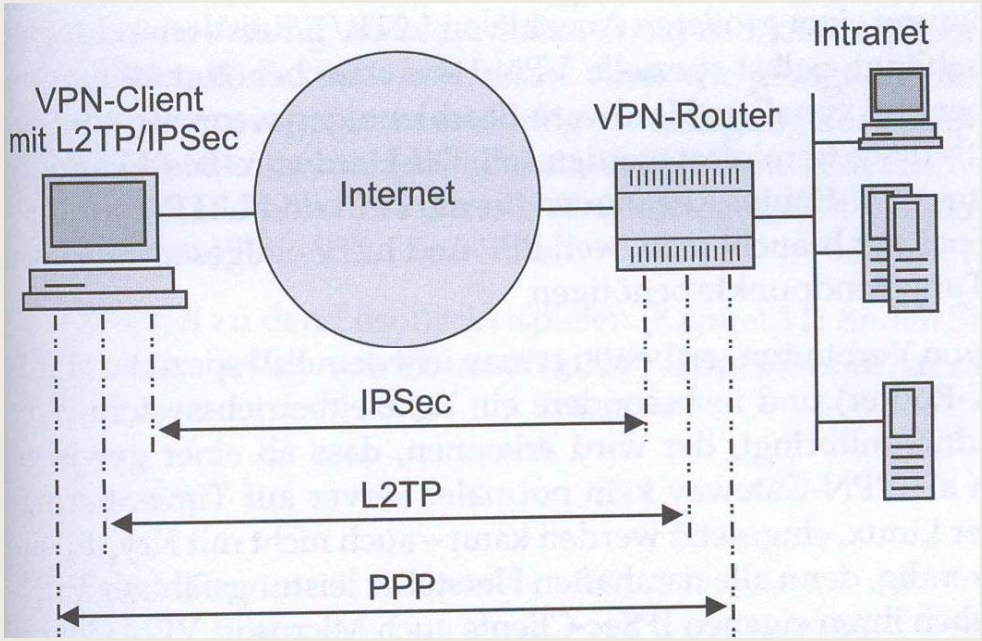
- umfassender Schutz für den Datenverkehr auf IP – Ebene
- Verschlüsselungsalgorithmen: DES, Triple DES, AES
- Nachteil: Nutzung von symmetrischen Schlüsselverfahren
- Schutz vor Veränderung und Authentizität eines Datenpaketes mit Hilfe des Hash-based-Message-Authentification Codes
- Schutz vor Denial-of-Service-Angriffen, Replay-Angriffen und Man-in-the-Middle-Angriffen implementiert

SSL = Secure Socket Layer

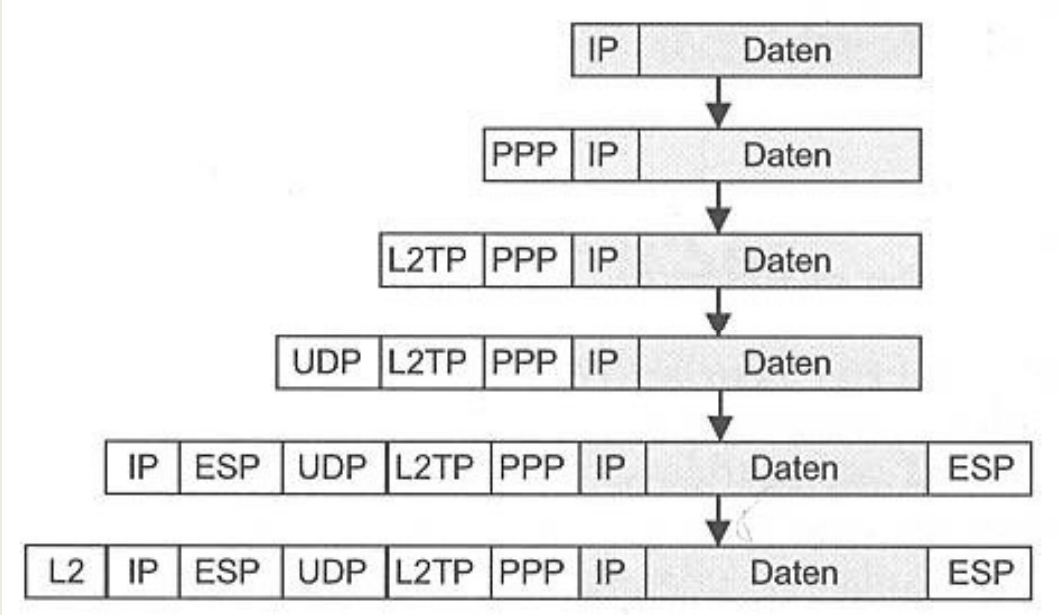
- von Netscape für HTTP entwickelt
- Datenverschlüsselung erfolgt mit DES oder AES
- Datenintegrität und Authentizität wird durch die selben Hashfunktionen wie bei IPSec gewährleistet
- Schlüsselmanagement erfolgt z.B. mit RSA
- keine freie Kombination der Verschlüsselungsverfahren
- kein Schutz vor Denial-of-Service Angriffen

L2TP + IPSec

- Verwendung von Microsoft seit Windows 2000
- Vorteile beider Verfahren werden kombiniert



Manfred Lipp: Kombination L2TP / IPSec in VPN Aufbau und Sicherheit, Seite 313



Manfred Lipp: Datenverkapselung in L2TP / IPSec in VPN Aufbau und Sicherheit, Seite 314

Vielen Dank für Ihre Aufmerksamkeit

ENDE

FRAGEN ?