Jakob Metzger

VPN & IPsec

Sichere Kommunikation
im Internet

Übersicht

Motivation

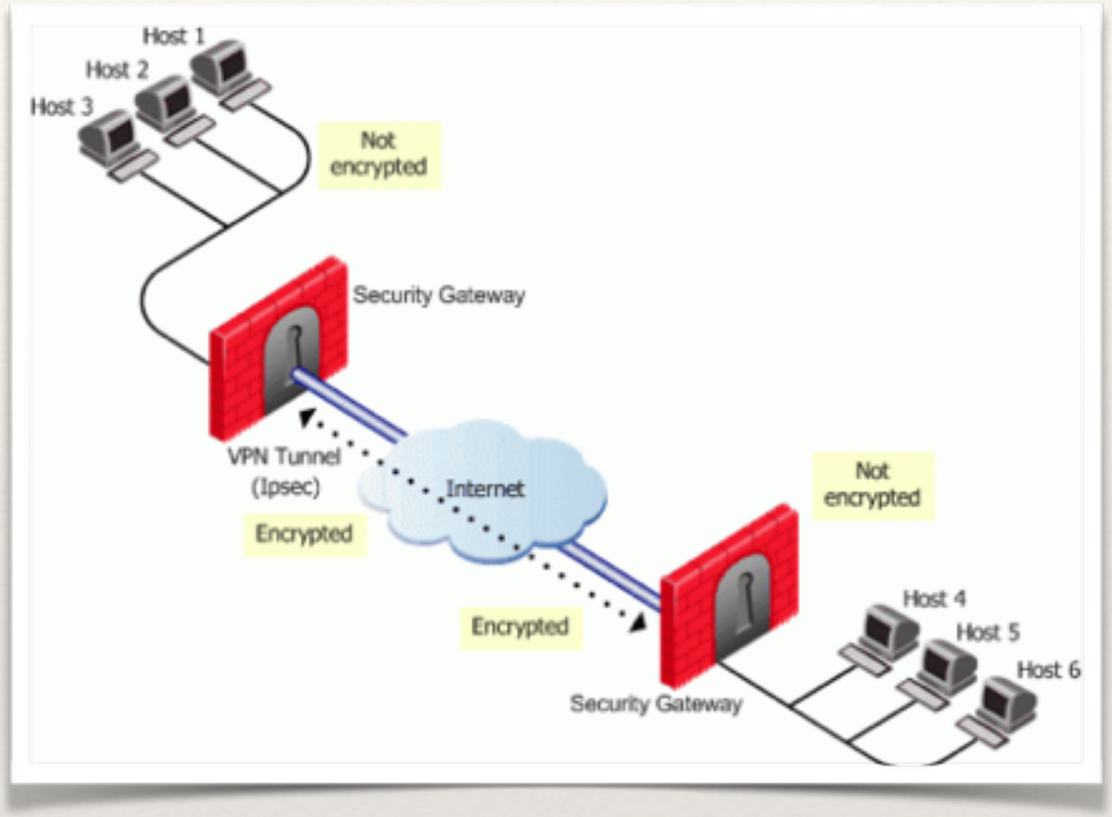
- Verbindung mehrerer lokaler Netzwerke an verschiedenen Standorten (z.B. Universitäten, Firmen mit Außenstellen)
- Ursprüngliche Lösung: „Leased Lines“; physikalische Verbindung der Netzwerke durch gemietete Standleitungen
- Probleme:
  - Sehr teuer
  - Schlechte Skalierung
  - Keine großen Distanzen (Kontinente)
  - Nicht flexibel (Home Offices, Außendienst)
- Neue Lösung:
  - Öffentliches Netzwerk (Internet) als „Verlängerungskabel“ nutzen
  - ABER: Öffentliche Netze sind nicht sicher! Daten können gelesen und manipuliert werden

Ziele/Eckpfeiler

- 1. Vertraulichkeit
  - Daten dürfen nur von Kommunikationspartnern eingesehen werden
- 2. Authentizität
  - Identität der Kommunikationspartner muss überprüft werden
- 3. Integrität
  - Es muss sichergestellt werden, dass keine Daten manipuliert wurden

Konzept

- Sichere Verbindung zwischen zwei Punkten durch „Tunneling“
- Durch Einkapselung und Verschlüsselung von Daten wird ein privater Datentunnel (im öffentlichen Netz) erstellt
- Identität beider Punkte wird sichergestellt
- Daten werden auf Integrität überprüft
- Kompatible Software wird benötigt
- Keine spezielle Hardware erforderlich
- Implementierung von verwendeten Protokollen abhängig (VPN ist kein Protokoll)



Konzept

- Durch VPN wird aus Subnetzen ein virtuelles Netzwerk gebildet
- Alle Beteiligten können agieren, als befänden sie sich im selben LAN (Zugriff auf alle Netzwerkressourcen, z.B. Drucker, Dateien usw.)
- Zwei Typen:
  - Site-to-site (zwei Standorte/Netzwerke)
  - Remote Access (Fernzugriff auf Netzwerk)

Protokolle

- Beliebte Protokolle:
  - PPTP (Point-to-point Tunneling Protocol)
  - L2F (Layer 2 Forwarding)
  - L2TP (Layer 2 Tunneling Protocol)
  - **IPsec (Internet Protocol Security)**
  - Weitere, z.B. SSL-VPN, MPLS

Anwendungen von VPN

- Verbinden von Firmennetzwerken und Standorten
- Fernzugriff für Home Offices und Außendienst
- Sichere Kommunikation
- Anonymität, Verschleierung der Identität
  (Zugriff auf Internet über angesteuertes VPN-Gateway führt zu geänderter IP)

Was ist IPsec?

- Protokoll-Suite für gesicherte Kommunikation
- Modulare Protokolle und Algorithmen
- Arbeitet auf Layer 3 (Network) im OSI-Modell
- Ist in IPv6 integriert
- Komponenten:
  - Security Associations (SA)
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
  - Internet Key Exchange (IKE)

Vorteile von IPsec für VPN

- Die Ziele von VPN werden von IPsec erfüllt:
  - Vertraulichkeit durch Verschlüsselung der Daten
  - Integrität durch Prüfsummen oder Hash-Werte
  - Authentizität durch Signaturen und Zertifikate
- Pakete können uneingeschränkt durch IP Netzwerke gesendet werden

Ablauf von IPsec

- 1. Security Policies (muss bereits vorhanden sein)
- 2. Anfrage zur Kommunikation wird gesendet
- 3. Mit dem IKE Protokoll werden in zwei Phasen beide Endpunkte authentifiziert und eine Vereinbarung über die verwendeten Parameter getroffen (Security Associations werden gebildet)
- 4. Über den so erstellten Tunnel werden Daten übertragen
- 5. Der Tunnel wird terminiert

Security Policy

- Anwender von IPSec müssen über eine Security Policy verfügen, die folgendes definiert:
  - Welche Verschlüsselungsalgorithmen?
  - Welche Algorithmen für Hashing?
  - Was für Zertifitikate?
  - Welche Schlüssellängen?
  - Wie lange sind Schlüssel gültig?
  - Mit wem wird kommuniziert?
- Kommunikationspartner müssen sich koordinieren und aushandeln, welche Algorithmen und Parameter sie verwenden (Security Associations)
- Security Policies werden statisch in einer Datenbank gespeichert

Security Associations

- SAs sind eine Sammlung von Parametern, die für eine sichere Verbindung benötigt werden
- Jede SA wird vor dem Aufbau der Verbindung zwischen beiden Endpunkten ausgehandelt
- Eine SA kann durch drei Parameter identifiziert werden:
  - Security Parameter Index (SPI)
  - Ziel IP-Adresse
  - ID des Sicherheitsprotokolls (AH oder ESP)
- SAs sind unidirektional (Sender und Empfänger haben eigene)
- SAs werden mit dem IKE Protokoll automatisch erzeugt

Internet Key Exchange

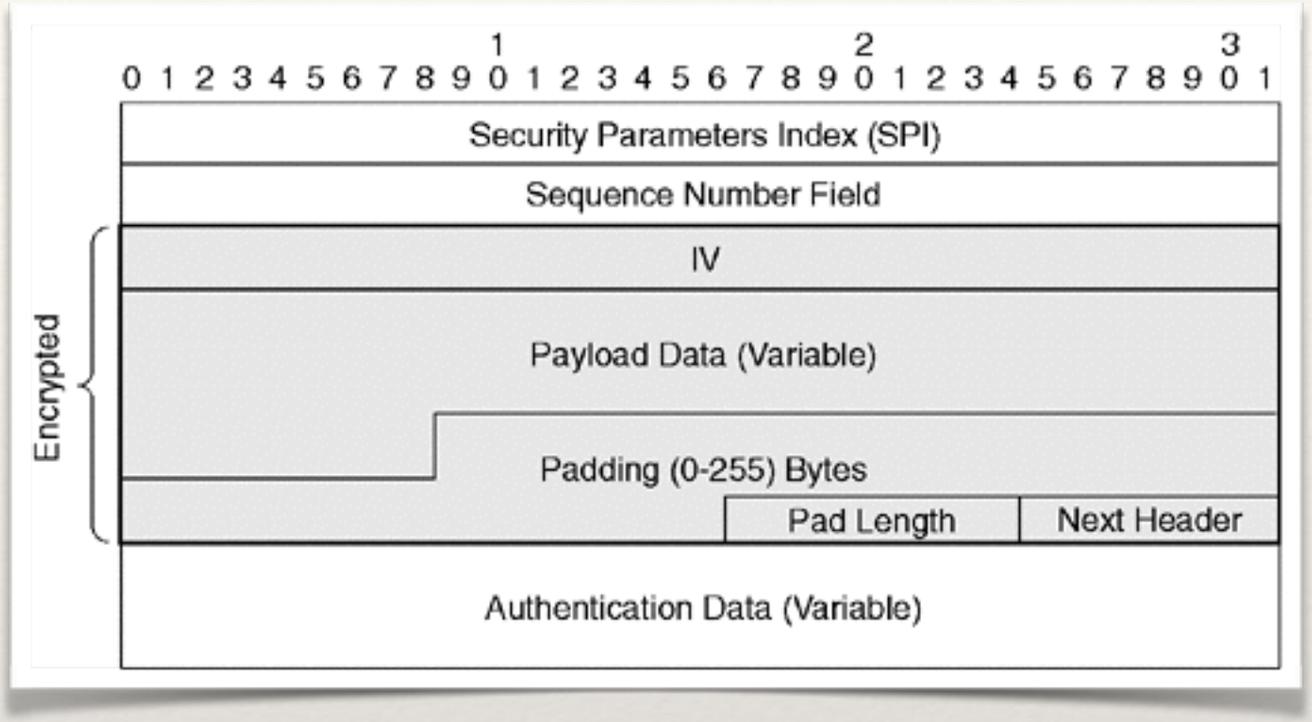
- Protokoll zum Aushandeln von SAs und Austauschen von Schlüsseln (für Authentifizierung und Verschlüsselung)
- Phase 1:
  - Die zu verwendende SA für IKE wird ausgehandelt (bidirektional)
  - Gegenseitiges Authentifizieren anhand der ausgehandelten SA
  - Mit dem Diffie-Hellmann-Algorithmus wird ein gemeinsamer Schlüssel erzeugt („Shared Secret“)
  - Jetzt besteht eine vorläufig gesicherte Verbindung für Phase 2 („Management Channel/Tunnel“)
- Phase 2:
  - Die zu verwendende SA für IPsec wird ausgehandelt (unidirektional)
  - Anhand des zuvor erzeugten Schlüssels werden neue Schlüssel für IPSec erzeugt und ausgetauscht
  - Jetzt besteht ein gesicherter IPsec Tunnel zwischen beiden Punkten, Daten können ausgetauscht werden

Authentication Header

- Stellt Authentizität und Integrität eines Datenpakets in IPsec sicher
- Enthält Datenfelder für die Identifizierung einer SA (Security Parameter Index), eine Sequenznummer (Replay Protection) und das Ergebnis einer Integritätsprüfung (Prüfsumme)
- Ist bereits veraltet, da hier keine Verschlüsselung stattfindet (und Probleme mit NAT)!

Encapsulating Security Payload

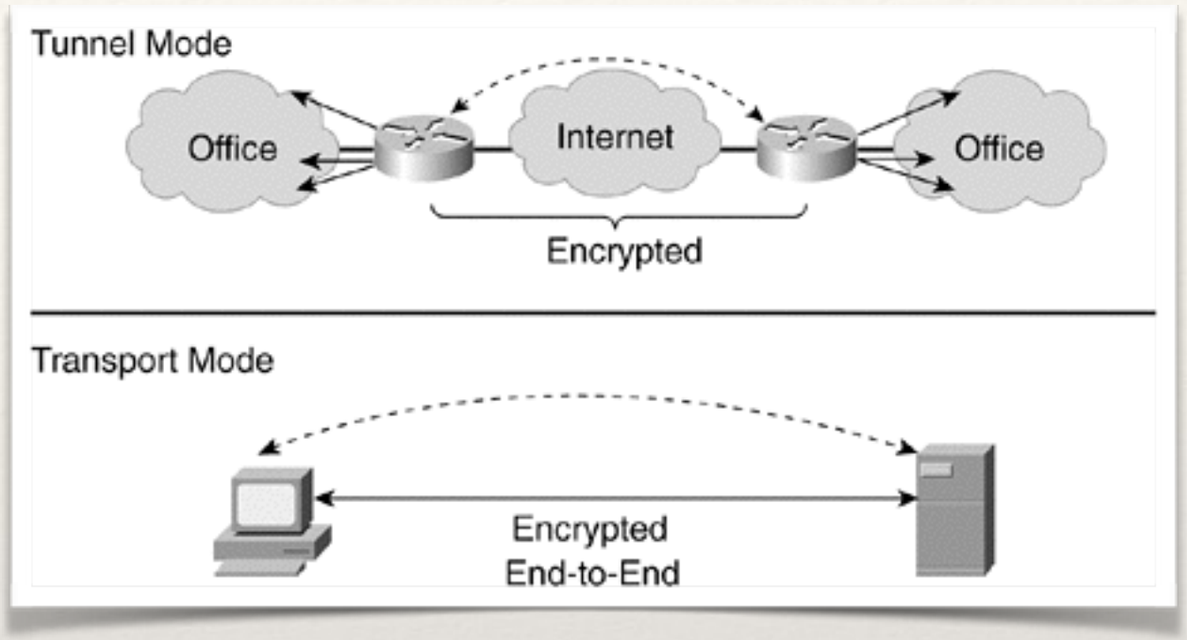
- Alternative zu AH (bevorzugt)
- Verschlüsselt Daten, bietet Integrität und Authentizität durch Prüfsummen



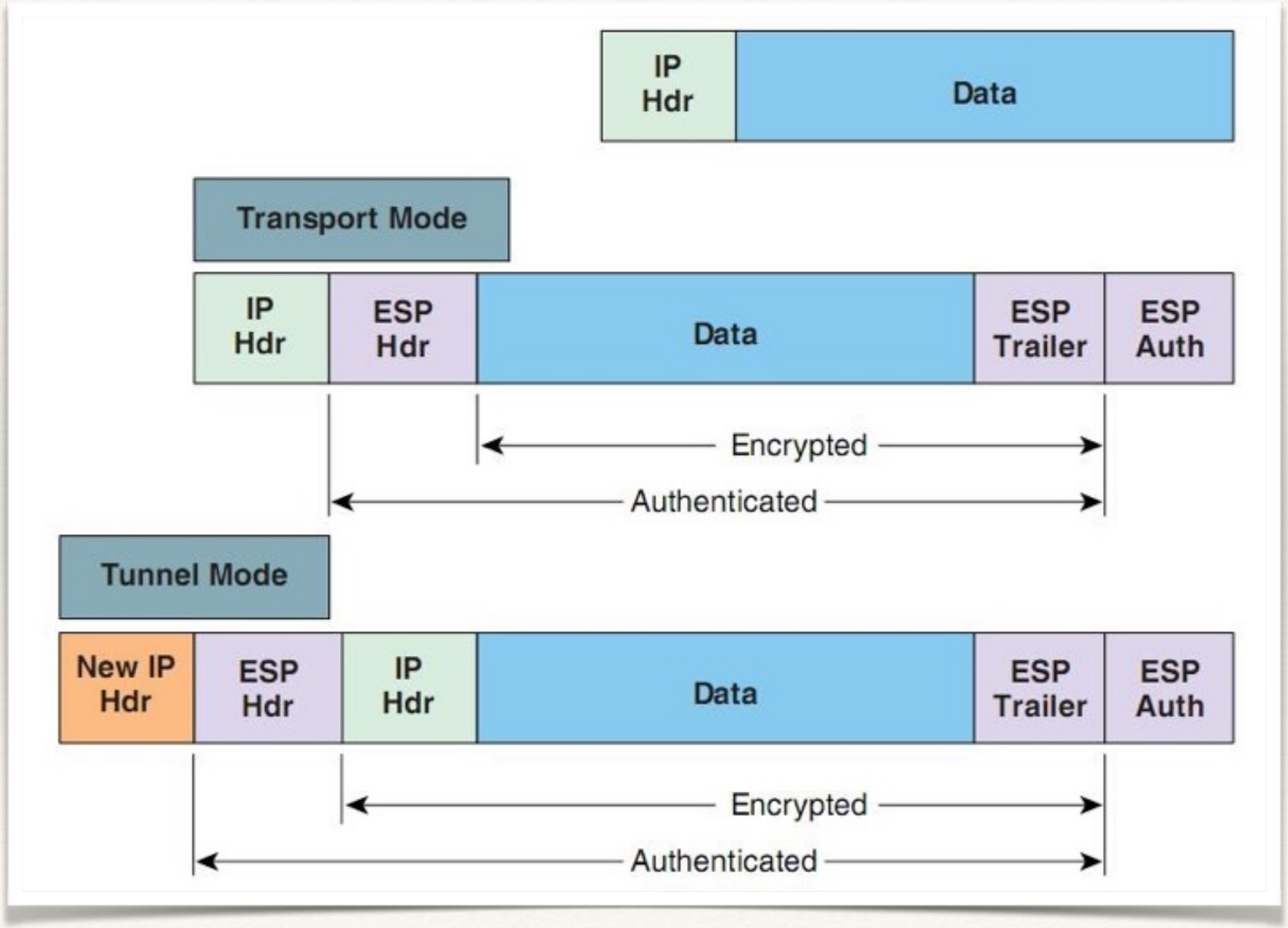
- Payload ist vollständig verschlüsselt
- Padding füllt Payload für Verschlüsselung auf bestimmte Bytezahl auf
- Authentication ist optional (aber empfohlen)

Modi von IPsec

- Tunnel Mode
  - Das gesamte IP-Paket (inklusive IP-Header) wird verschlüsselt und als Datenfeld in neues IP-Paket integriert
  - Das Gesamtpaket wird größer
  - Wird für Site-to-Site VPNs benutzt
- Transport Mode
  - IPsec Header wird in ein bestehendes IP-Paket integriert
  - Kleinere Paketgröße als im Tunnel Mode
  - Wird für Remote Access VPNs benutzt



Modi von IPsec



Vielen Dank für die Aufmerksamkeit!

Jakob Metzger

Quellen

- RFC 4301 (https://tools.ietf.org/html/rfc4301)
- APNIC Training eLearning Class „IPsec Basics 19 Mar 2014“ (https://www.youtube.com/watch?v=gnUIgSvx3OE)
- Cisco SIMOS course „Understanding AH vs ESP and ISKAKMP vs IPSec in VPN tunnels“ (https://www.youtube.com/watch?v=rwu8__GG_rw)
- Watchguard Fireware XTM Web UI Help (http://www.watchguard.com/help/docs/webui/xtm_11/en-US/index.html#cshid=en-US/mvpn/general/ipsec_vpn_negotiations_c.html)
- Wikipedia Eintrag zu IPsec (http://de.wikipedia.org/wiki/IPsec)