Virtual Private Network

340282366920938463463374607431768211456

VPN steht für Virtual Private Network
Was ist VPN? die Frage die eigentlich sehr schwer und doch kann Sie einfach erklärt werden. Die Frage richtet sich auf ein komplexes Themengebiet

Man nehme IP Pakete ,packe Sie ein ,verändere den IP-Header ,lege einen Hash- und Verschlüsselungs-Algorithmus darüber , schicke sie durchs Internet und packte Sie wieder aus.

Hierzu eine kurze Erklärung.

- **IPsec** (Kurzform für **Internet Protocol Security**) ist eine **Protokoll-Suite**, die eine gesicherte Kommunikation über potentiell unsichere IP-Netze wie das Internet (Space) ermöglichen soll.

- IPSec bietet die höchste Sicherheit für alle Daten.

- IPSec beschreibt, wie verschiedene Verschlüsselungstechniken genutzt werden können, um gesicherte Verbindungen zwischen Gegenstellen herzustellen.

- IPSec stellt als Standard sicher, dass die verschiedenen Komponenten problemlos miteinander funktionieren.

- IPSec ist ein Paket von Protokollen zur Gewährleistung der Vertraulichkeit, Integrität und Authentizität.

  - Vertraulichkeit: Durch ein Kryptoverfahren , z.B. mit AES, werden die Daten verschlüsselt
  - Integrität: Durch ein Hash-Verfahren, z.B. MD5, werden die Daten vor Manipulationen geschützt
  - Authentizität: Es erfolgt eine Prüfung des Kommunikationspartners, z.B. über ein Passwort

- IKE (Internet Key Exchange) wird vom IPSec für den Verbindungsaufbau und das Schlüsselmanagement verwendet.
- Der erste Schritt einer IPSEC-Kommunikation ist die Aushandlung einer SA.

- Die SA definiert alle Informationen, die zur sicheren Datenübertragung zwischen zwei Kommunikationspartnern erforderlich sind:

Security Associations (SAs)

Kommunikationspartner treffen eine gemeinsame Sicherheitsvereinbarung über den Schutz des Datentransfers:

- Kommunikationsendpunkte
- Kryptographische Verfahren
- Schlüsselmaterial
- Integrität der Daten
- Angaben über die Lebensdauer der Schlüssel

- Der IKE Verbindungsaufbau teilt sich in zwei Phasen auf:

IKE Phase 1 (IKE):

– Herstellen einer gesicherten Verbindung zweier Gegenstellen (Gateways)

– Zwischen zwei Gateways existiert genau eine SA der Phase 1, die definiert, wie die Gateways gesichert miteinander kommunizieren können.

IKE Phase 2 (IPsec):

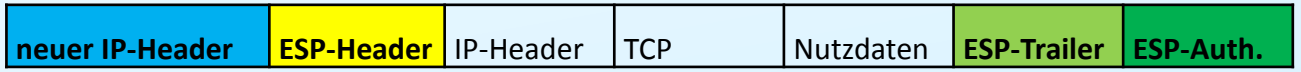
– Aushandlung des Tunnels für die Nutzdaten. Hierbei definieren die ausgehandelten SAs die Kommunikation zwischen bestimmten Netzen.

– Pro Netzwerkkombination wird jeweils eine eingehende und eine ausgehende Phase 2 Aushandlung durchgeführt.

Nach Aushandlung der SAs (Security Associations) in IKE Phase 2 wird das Protokoll ESP benutzt, um letztendlich die verschlüsselten Daten zu transportieren. ESP hat keinen Port, da es ein OSI Layer 3 Protokoll ist.

Originales IP-Paket

ESP im Tunnel-Modus



- Das ist VPN, die Daten werden mit AES 256Bit verschlüsselt (Advanced Encryption Standard), bis jetzt sind keine Schwachstellen bekannt.
- Um einen gängigen 256-bit AES-Schlüssel zu knacken würde ein Computer, der pro Sekunde eine Milliarde Schlüssel durchprobieren kann, über **10 hoch 60 Jahre** benötigen.
- Alles was in Agentenfilmen zu sehen ist und Entschlüsselung betrifft, ist reines Hollywood, das sollte nicht mit einem Brute-Force-Angriff verwechselt werden, bei dieser Methode werden Schlüssel ausprobiert.

Anzahl der möglichen Schlüssel

- Bei einem 128 Bit Schlüssel ist jede der 2^{128} möglichen Kombinationen als Schlüssel zulässig.
- 2^{128} als Zahl ausgeschrieben ist:
- 340282366920938463463374607431768211456
- Das ist die Zahl vom Anfang ☺