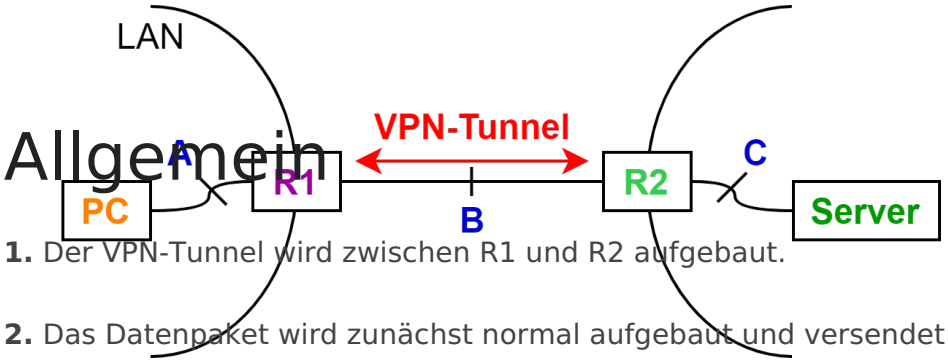
VPN by Falko

VPN

→ VPN (Virtual Private Network) wird benötigt, um die Verbindung zwischen zwei Routern zu verschlüsseln. Dabei wird der originale IP-Header verschleiert.

Beispiel: Im Homeoffice greife ich mit meinem PC aus meinem lokalen Netzwerk per VPN auf das Unternehmensnetz bzw. einen Server im Unternehmensnetz zu.



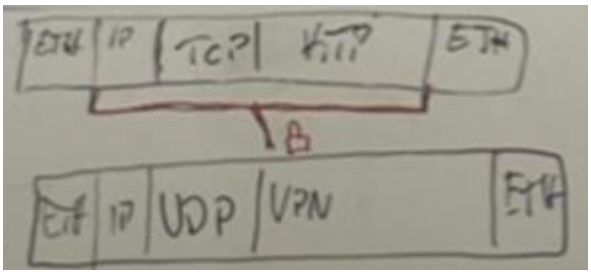
Allgemein

1. Der VPN-Tunnel wird zwischen R1 und R2 aufgebaut.

2. Das Datenpaket wird zunächst normal aufgebaut und versendet:

A	Quell-MAC	Ziel-MAC	Quell-IP	Ziel-IP
	PC	R1	PC	Server

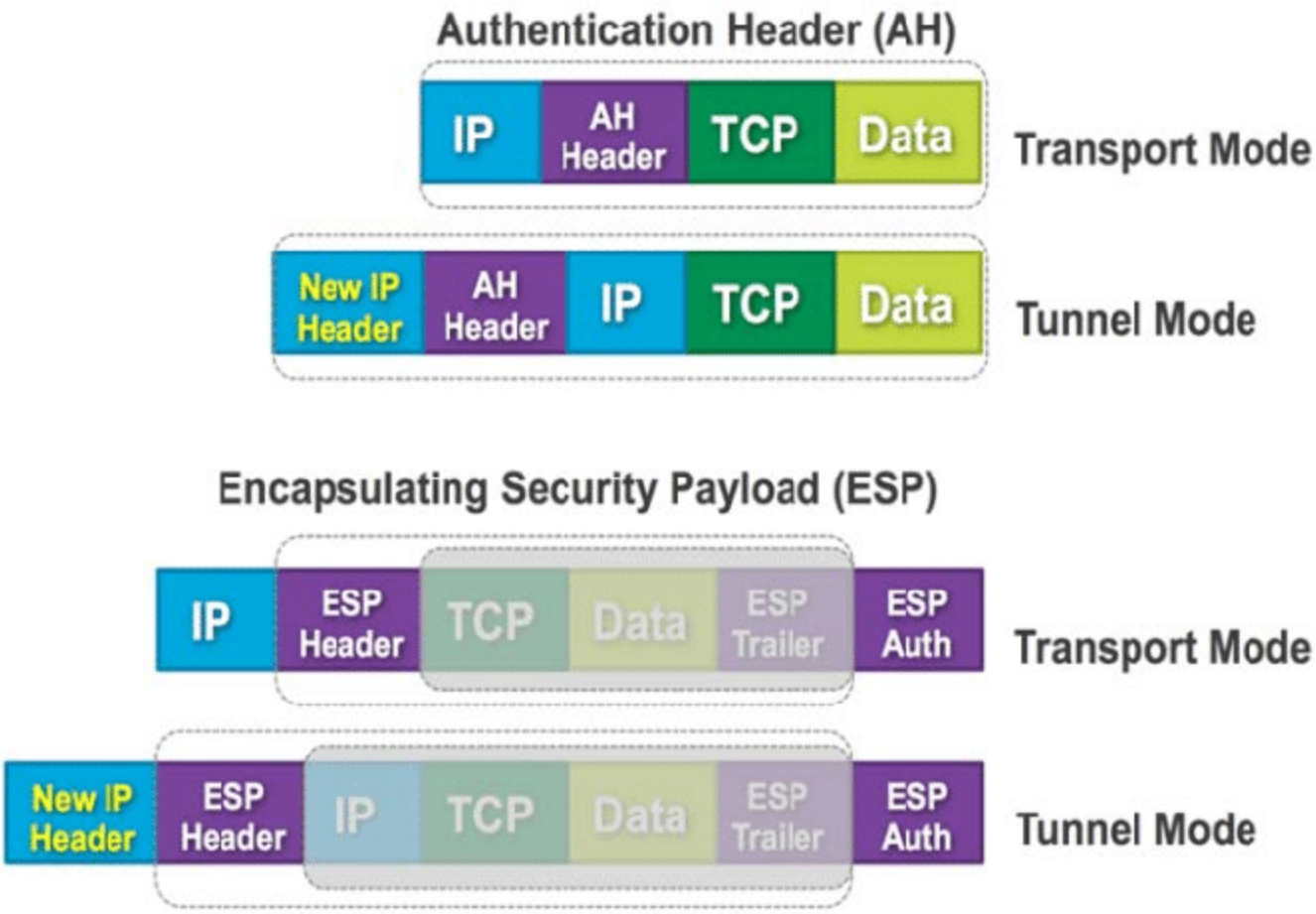
3. Auf R1 wird das gesamte Datenpaket verschlüsselt. Es wird ein neuer IP-Header generiert und vor den verschlüsselten Teil gesetzt.



4. Auf R2 wird der IPneu-Header wieder abgeschnitten und die Payload entschlüsselt.

IPsec VPN (ESP)

Dies ist eine konkrete Implementierung eines VPNs (wir brauchen nur ESP nicht AH)



→ Da der verschlüsselte Teil immer eine bestimmte Länge haben muss (ein Vielfaches von 32 Bit) wird er um ein **Padding**, eine entsprechend lange zufällige Zeichenfolge ergänzt.

Revision #1
Created 13 March 2022 10:43:51 by Falko Tschernay
Updated 13 March 2022 10:56:07 by Falko Tschernay