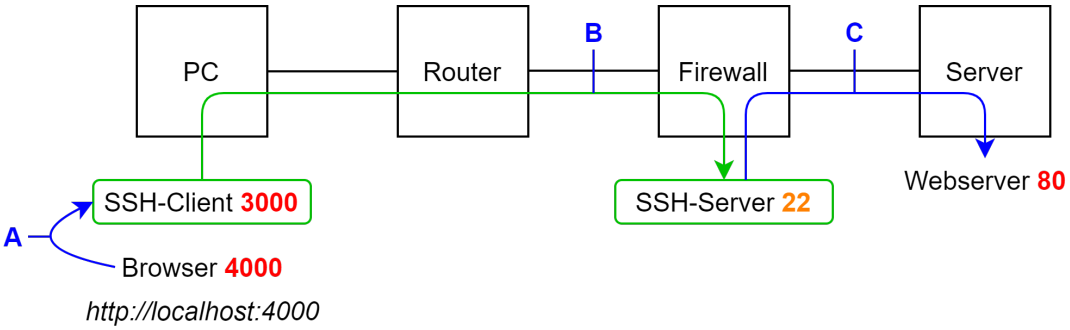
SSH-Tunnel

→ Ein SSH-Tunnel macht den Zugriff auf einen Server möglich, der ohne Tunnel durch z.B. eine Firewall blockiert wird. Die Verbindung ist verschlüsselt.

Beispiel: Ich möchte auf einen Server zugreifen, werde aber durch eine Firewall blockiert.



A	Quell-MAC-PC Ziel-MAC-PC	Quell-IP-PC Ziel-IP-PC	Quell-Port 4000 Ziel-Port 3000	**GET**
B	Quell-MAC-R Ziel-MAC-FW	Quell-IP-PC Ziel-IP-FW	Quell-Port 3000 Ziel-Port 22	*III*
C	Quell-MAC-FW Ziel-MAC-Server	Quell-IP-FW Ziel-IP-Server	Quell-Port FW* Ziel-Port 80	**GET**

** vom BS generiert*

1. Zwischen dem SSH-Client und dem SSH-Server wird ein Tunnel aufgebaut

2. Das Datenpaket wird zunächst vom Browser an den SSH-Client gesendet. (**A**)

3. Der SSH-Client leitet das Datenpaket an den SSH-Server weiter. Der HTTP-Header ist verschlüsselt. (**B**)

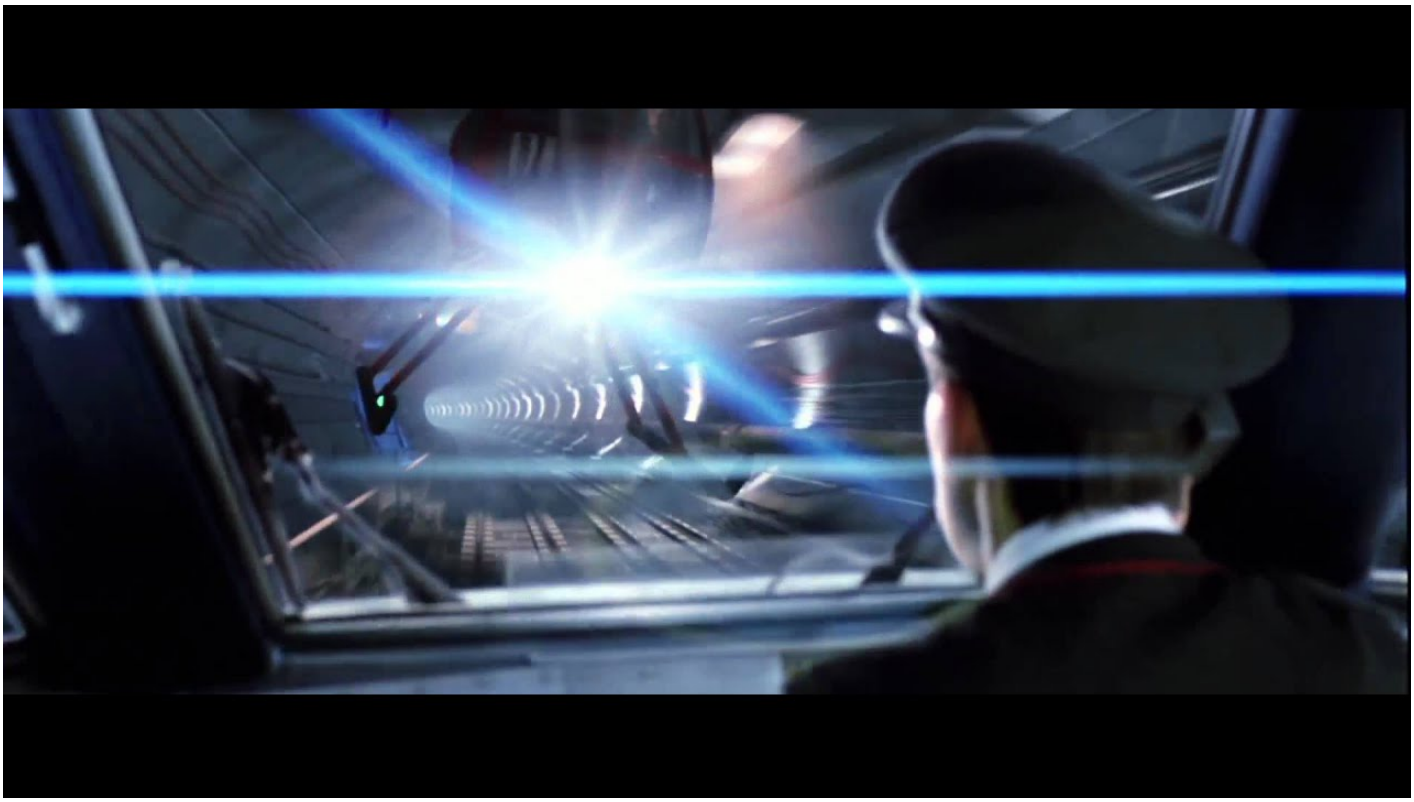
4. Der SSH-Server leitet das Datenpaket an die Destination weiter. Das Datenpaket ist nicht mehr verschlüsselt. (**C**)

→ Bei der Rückantwort vom Server werden die Daten vom SSH-Server wieder zum SSH-Client und von dort zum Browser weitergeleitet.

> **Beispiel Autobahntunnel**: Über der Autobahn fliegt ein Hubschrauber zur Beobachtung des Verkehrs. Die Autos die auf der Autobahn fahren sind hier die Datenpakete. Solange die

Autos nicht durch den Tunnel fahren kann der Hubschrauber die Autos beobachten.

Sobald die Autos in den Tunnel einfahren hat der Hubschrauber keine Möglichkeit mehr die Autos zu beobachten. Vorausgesetzt wir befinden uns nicht in Mission Impossible.



Revision #10
Created 19 January 2022 10:29:03 by Martin Tienken
Updated 23 February 2022 08:06:34 by Martin Tienken