1. Firewall-Technologien einsetzen

   (a) OSI-Modell

   (b) Proxy einsetzen

   (c) eigene DNS-Tabelle

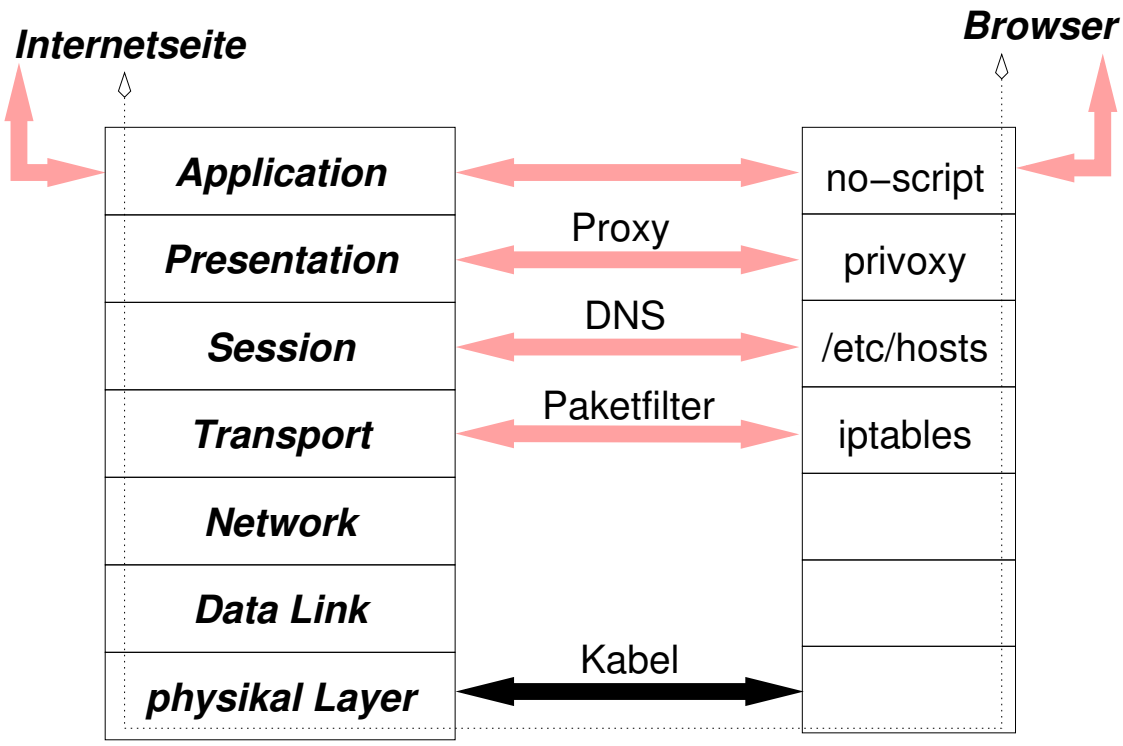
   (d) iptables-Firewall (Linux-Router, Fritzbox m. Erw.)

2. Firefox konfigurieren

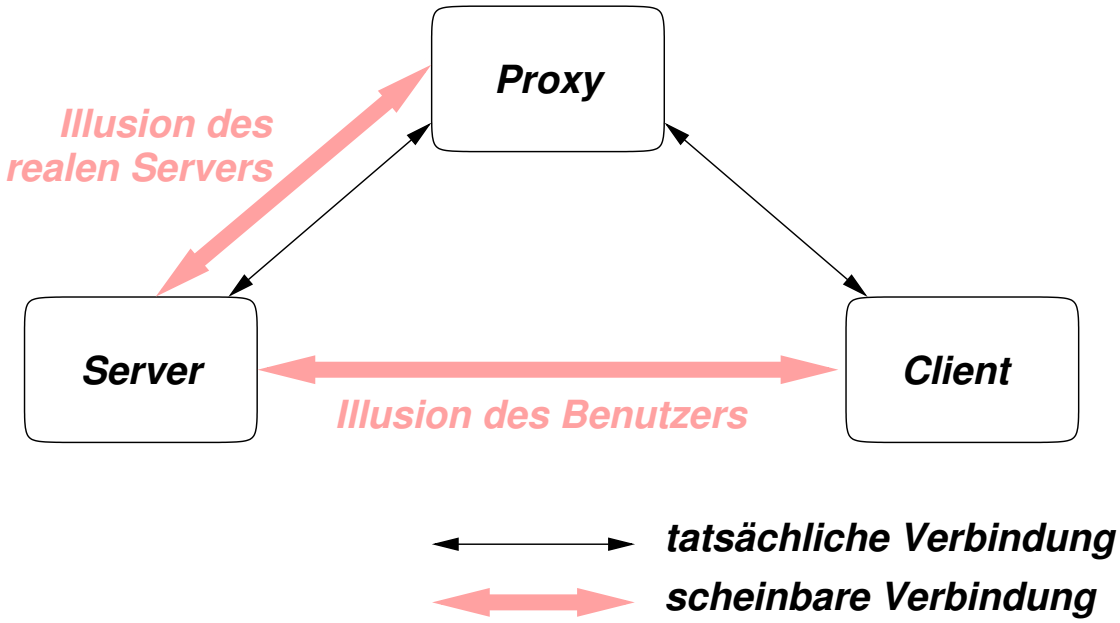
   (a) dedizierte Profile benutzen

   (b) about:config

   (c) Auditing der Verbindungen



Firewall-Funktionalität kann in verschiedenen Schichten implementiert sein – aber SSL macht privoxy unbrauchbar.



Proxy == Stellvertreter, Vermittler – kann unerlaubte/unerwünschte Anfragen des Clients verhindern

- ein Profil für ein Dienst (Internetbanking, Ebay, Facebook, Google/Downloads/Surfen)

- Zugriff aufs Internet kann in jedem Profil anders definiert/beschränkt werden

- Datensammler können nur ihre eigenen Cookies lesen

- jedes Profil enthält ein-eindeutige Nutzer-ID

- ID kann auch über Browser-Agent erkannt werden
  - Betriebssystem
  - Architektur
  - Browser-Version (Proxy oder Profil)
  - IP-Adresse (VPN, Tor)

- firefox --new-instance --no-remote -P

- .local/share/applications/alacarte-made-20.desk

1. installieren proxy-pac.js

2. Browser-Konsole: zeigen was im Hintergrund passiert

3. about:config

   (a) browser.fixup.alternate.enabled

   (b) browser.newtabpage.activity-stream.impressio

   (c) captivedetect.canonicalURL

   (d) datareporting.healthreport.infoURL

   (e) toolkit.telemetry.cachedClientID

1. Download von: https://noscript.net/getit/#late
   stable
   https://addons.mozilla.org/en-US/firefox/addon

2. URL kopieren und mit wget herunterladen

3. für jedes Profil einzeln installieren

4. Berechtigung zur Ausführung von Javascript
   pro Seite erlauben

A time marker:

Don't talk more than .