Para Neujahr

Mögliches und Unmögliches zum Schutz der Privatsphäre
-
Technische Antworten auf die Vorratsdatenspeicherung

Gliederung

- Theoretische Grundlagen zur VDS
- Möglichkeiten zum Schutz der Privatsphäre
  - Mobilfunk
  - Elektronische Post
  - Country Shifting
- Projekt Tunnelendpunkt

VDS - Theorie

Vorratsdatenspeicherung ist die verdachtsunabhängige Speicherung der Verkehrs- und Standortdaten elektronischer Komunikationsvorgänge für eine Dauer von 6 Monaten.

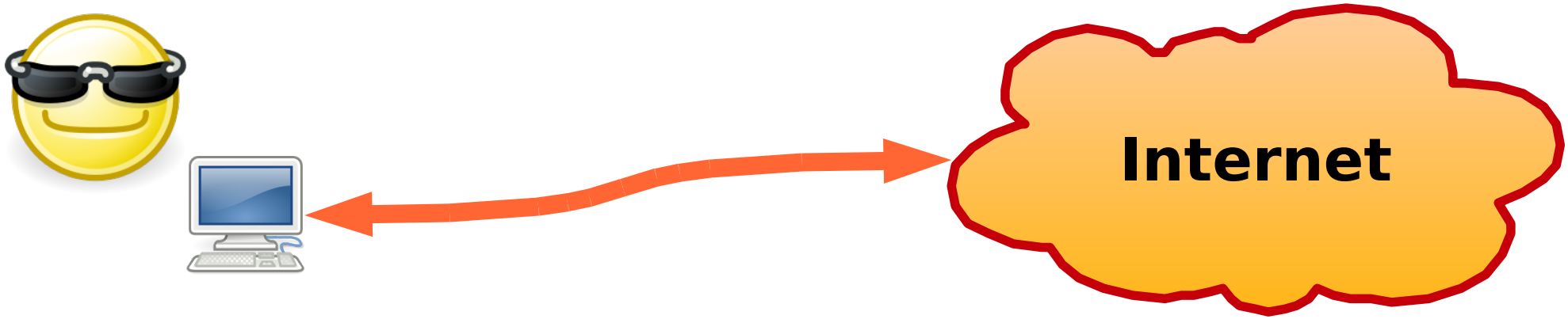
VDS - Theorie

- Gesetzliche Grundlage
  - Gesetz zur Neuregelung der Telekommunikations-überwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG
  - Verdachtslose Speicherung
- TKÜV
  - Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation
  - Verdachtsabhängige Speicherung

VDS - Theorie

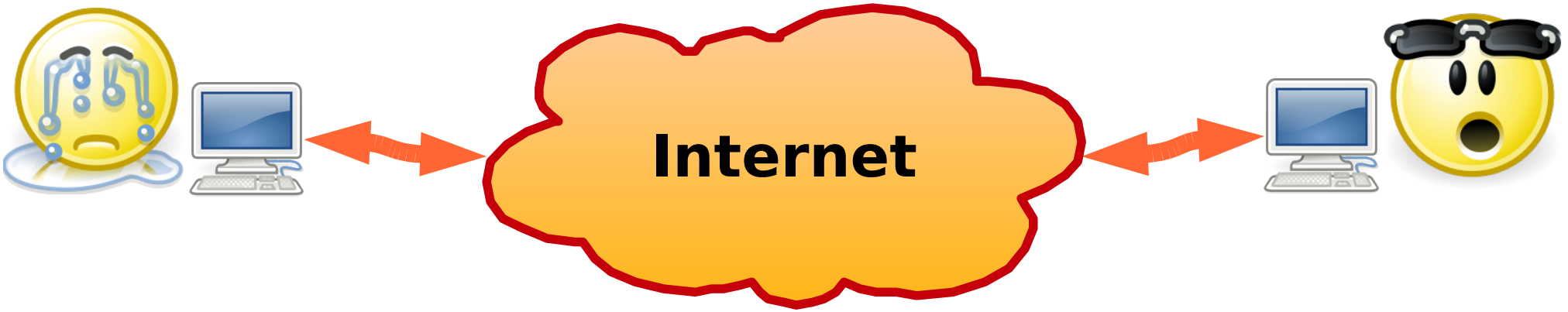
- Wer speichert?
  - Telekommunikationsanbieter
  - Internetprovider
- Wo werden die Daten gespeichert?
  - nicht bei einer Behörde
  - beim privatwirtschaftlichen Anbieter (also beim “Experten” vor Ort)

VDS – Internetzugang



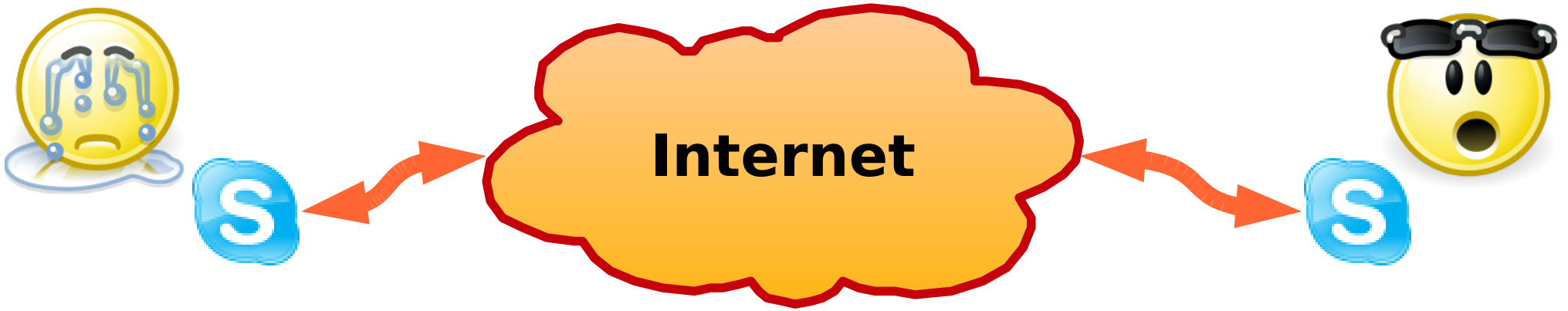
- Eindeutige Kennung des Anschlusses
- Datum und Uhrzeit von Beginn und Ende
- zugewiesene IP-Adresse

VDS – Elektronische Post



- E-Mail Adresse des Senders
- E-Mail Adresse aller Empfänger
- Jeder Zugriff auf das Postfach
  - Datum, Uhrzeit, Kennung, IP-Adresse
  - auch bei Nutzung eines Webinterfaces

VDS - IP-Telefonie



- Rufnummer/ Benutzerkennung der Teilnehmer
- bei Rufumleitung alle beteiligten Anschlüsse
- Beginn und Ende der Verbindung
- IP-Adresse
- genutzte Dienste

VDS - Mobilfunk

- Rufnummer/ Benutzerkennung der Teilnehmer
- bei Rufumleitung alle beteiligten Anschlüsse
- Beginn und Ende der Verbindung
- IMEI und IMSI
- Funkzelle (Standort)
- Aktivierungsdatum der Karte (P

auch f ür Kurznachrichten

VDS - Festnetz

- Rufnummer/ Benutzerkennung der Teilnehmer
- bei Rufumleitung alle beteiligten Anschlüsse
- Beginn und Ende der Verbindung

auch für Kurznachrichten

VDS - Ausnahmen

- Abgeordnete
- Geschlossene Benutzergruppen
  - sind von der VDS ausgenommen
  - Universitäten (im Einzelfall prüfen!)

VDS - Fazit

- Datenerhebung ähnlich wie bisher
- längere Speicherung der Daten
- verpflichtende Zuordnung
- Herausgabe der Daten

Zuordnung Daten ⟷ Person

VDS - Gegenmaßnahmen

- Strategien
  - Person unbekannt
    - Anonymisierung
  - Daten unbekannt
    - Datenvermeidung
    - Verschlüsselung
  - beides unbekannt

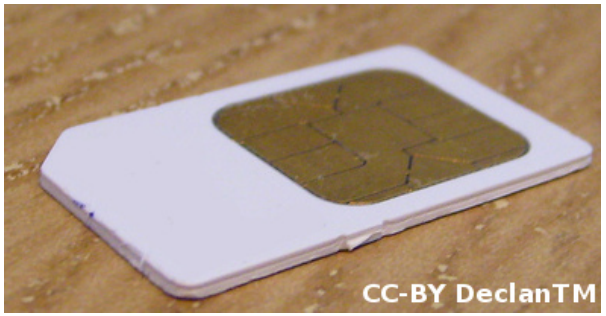
Mobilfunk

Mobilfunk

Die nun folgenden Überlegungen zum Thema Mobilfunk sollen theoretische Möglichkeiten aufzeigen. Die tatsächliche Umsetzung verstößt in deinem Land unter Umständen gegen Gesetze!

Mobilfunk

- Prepaidkarte kaufen
  - in einem nicht videoüberwachten Geschäft
  - Barzahlung
  - keine EC-Karte
  - keine Kundenkarte
  - keine Rabattkarten (Payback)
  - “Blisterverpackung” wählen
  - nicht vor Ort aktivieren!

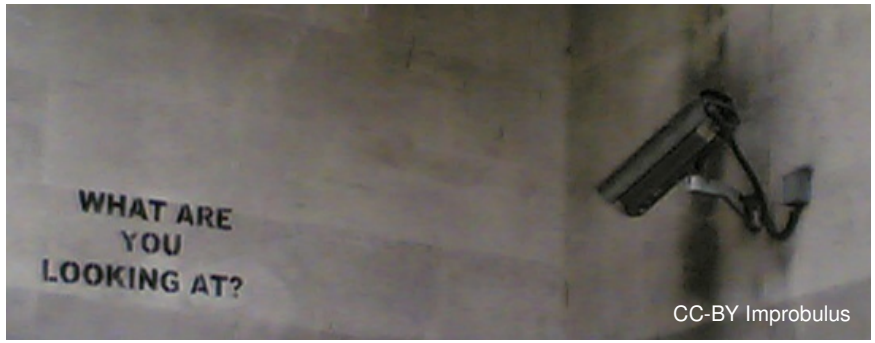


Mobilfunk

- Prepaidkarte aktivieren
  - per Telefon
    - Telefonzelle (Videoüberwachung?)
    - mit verstellter Stimme
  - per Internet
    - TOR
    - kein Referrer, keine Cookies
    - sauberer User-Agent
  - unter Angabe plausibler Daten
  - Hinweis: Personalausweisnummer

Mobilfunk

- Prepaidkarte aufladen
  - Barzahlung
  - Videoüberwachung?
  - keine EC-Karte
  - keine Kundenkarte
  - keine Rabattkarten (Payback)
  - idealerweise per Steuerbefehl
    - *100#01234567890# oder ähnlich



Mobilfunk

- Alternativen
  - bereits registrierte Karte anonym erwerben
  - ausländische, unregistrierte Karte
  - Tauschbörsen für Prepaidkarten

Mobilfunk

- Handy kaufen
  - Barzahlung
  - Videoüberwachung?
  - keine EC-Karte
  - keine Kundenkarte
  - keine Rabattkarten (Payback)
  - IMEI sollte nicht registriert werden
- gebrauchtes Handy kaufen
  - Käufer sollte dem Verkäufer unbekannt sein

Mobilfunk

- Mobilfunknutzung
  - Gerät nur bei Bedarf einschalten
  - Akku bei Nichtnutzung entnehmen
  - keine Klarnamen im Telefonbuch
    - Besser: nichts persönliches im Gerät speichern

Mobilfunk

- Mobilfunknutzung
  - niemals fremde Karte ins Gerät einlegen
  - Karte nie in ein anderes Gerät einlegen

Handy und Karte nicht trennen!

Mobilfunk

- Gegenargumente
  - bei jedem Ein- und Ausschalten werden Standort, Datum und Uhrzeit gespeichert
  - die Verkehrsdaten getätigter Anrufe werden weiterhin gespeichert
  - Profiling über angerufene Nummern und SMS
  - bei häufiger Nutzung: Bewegungsprofil
- Fazit
  - für den privaten Bereich ungeeignet
  - für konspirative Kräfte attraktiv

Elektronische Post

Elektronische Post

Betrieb eines eigenen Mailservers

Vorteile

- volle Kontrolle
- viel Speicherplatz
- beliebige Konfiguration

Nachteile

- Wartungsaufwand
- Spamfilterung
- Kosten
- Failback MX-Host?

Dies verhindert nur die Speicherung der auf der eigenen Seite anfallenden Daten!

Elektronische Post

- Protokollfrage
  - POP3
    - lokale Speicherung der Mails
    - lokale Datensicherheit?
  - IMAP
    - zentrale Speicherung der Mails
    - Datensicherheit auf dem Server?
- über TLS

Elektronische Post

- Alternativen
  - Nutzung von Anbietern ausserhalb der EU
  - Abrufen über verschlüsselte Verbindung
  - einer geschlossenen Benutzergruppe angehören

Elektronische Post

- Fazit
  - Inhalte sind besser geschützt
  - Verkehrsdaten entstehen an der Gegenstelle weiterhin
  - Elektronische Post hat und behält den Charakter einer “Postkarte”

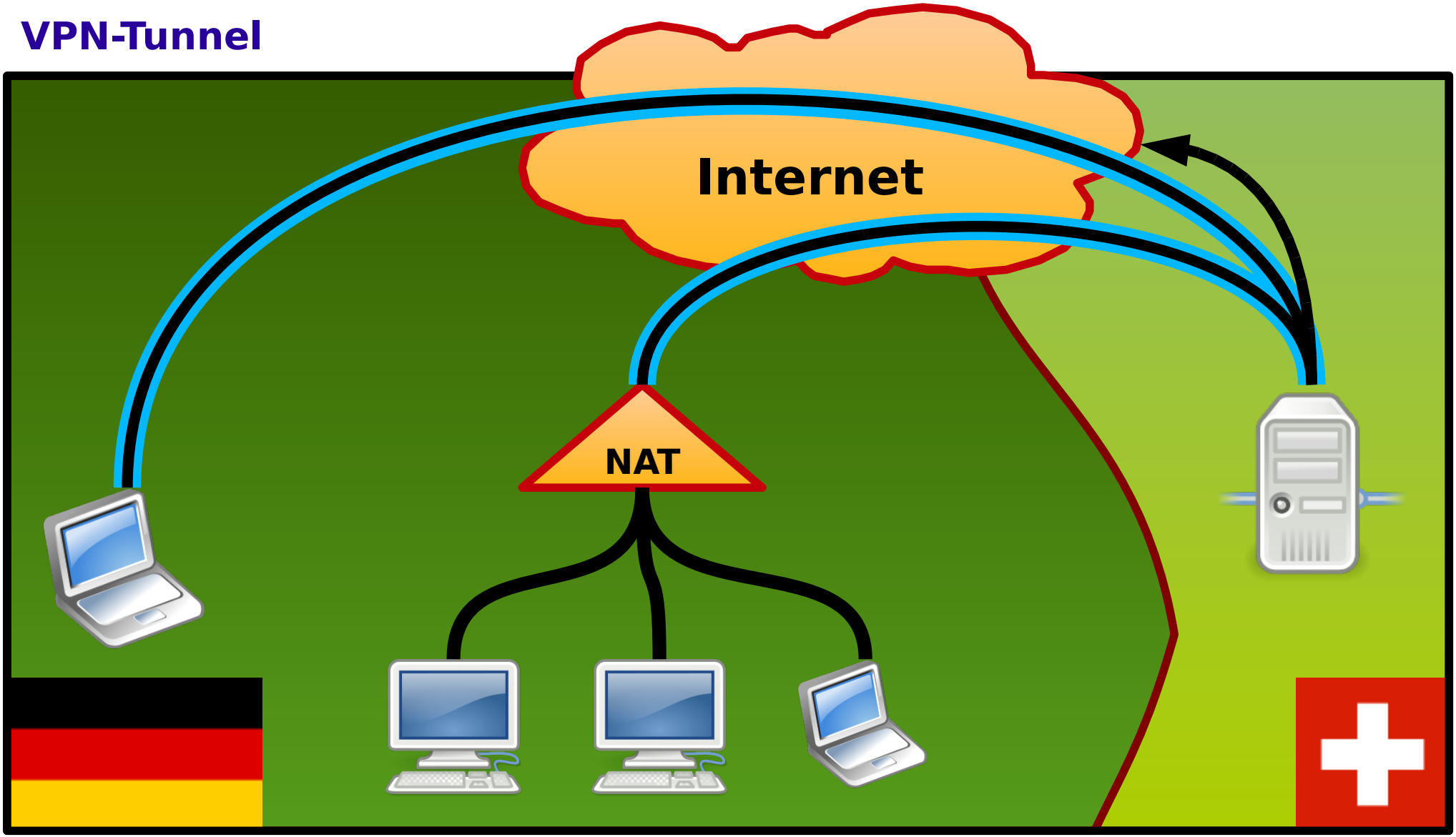
Country Shifting

Country Shifting

Country Shifting bezeichnet die Weiterleitung von Datenverkehr aus einem ungünstigen Rechtsraum in einen günstigeren Rechtsraum.

Country Shifting

VPN-Tunnel



Country Shifting

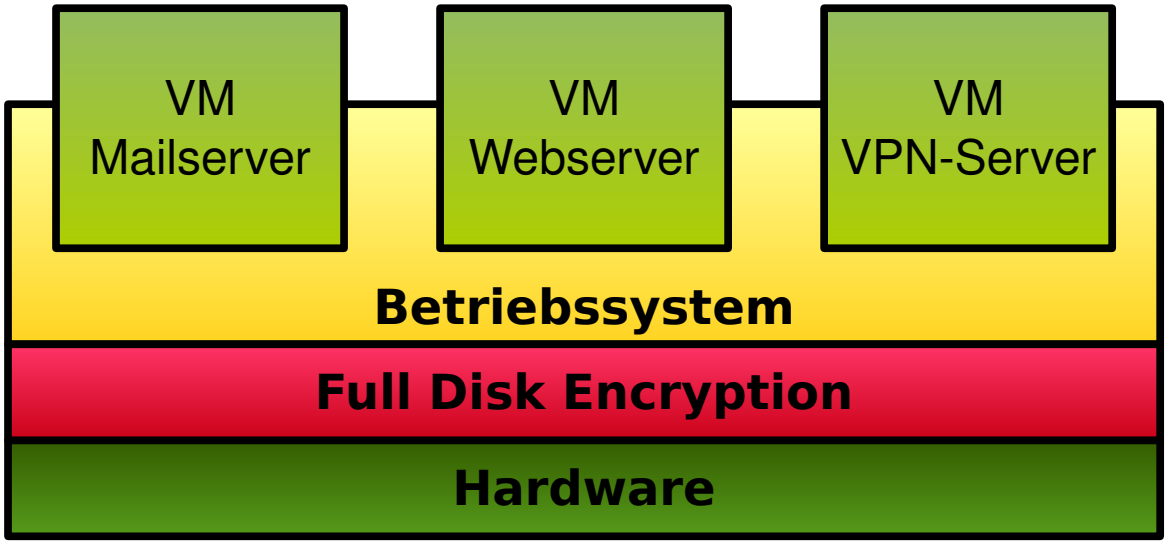
- Idee → Umsetzung
- Server Software
  - PPTP, IPSec, OpenVPN
- Server Hardware
  - HP Proliant DL 360
  - Ebay ~130€, zzgl. 25€ Versand
- Zielland Schweiz
  - gute Anbindung, ausserhalb EU
  - aber: kostenintensiv

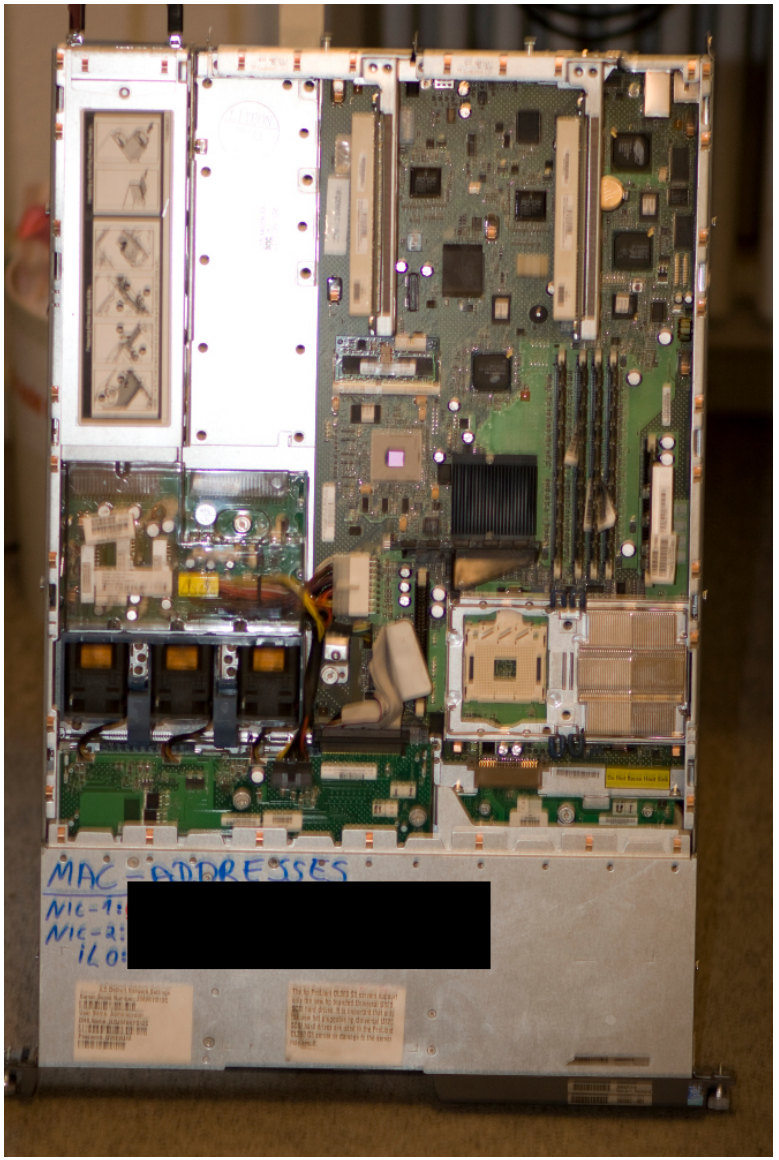
Country Shifting

- VPN Server Ergebnis
  - Nameserver
  - Source-NAT (Layer 3)
  - SSL-Verschlüsselung
  - UDP
- VPN Server Möglichkeiten
  - Proxy mit HTTP-Headerfilterung
  - Bridging (Layer 2)
  - TCP
  - ...

Country Shifting

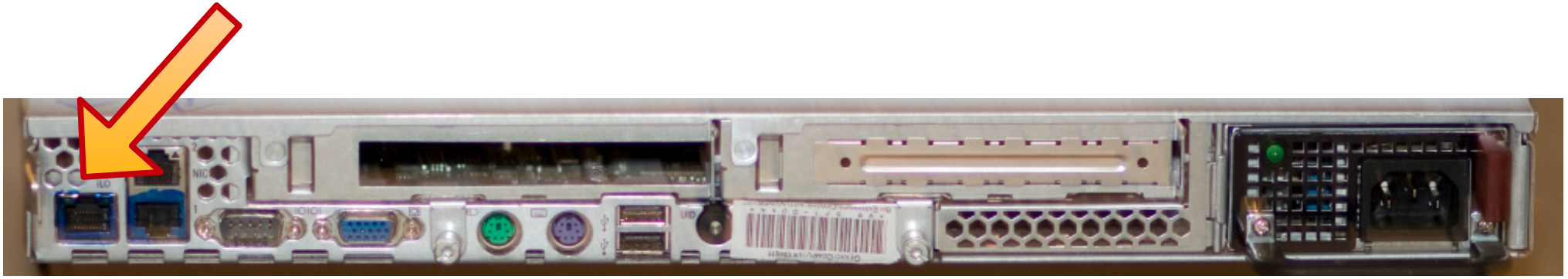
- Server Hardware
  - Intel XEON 2.4 GHz
  - 1 GB RAM
  - 2x 18 GB Festplatte (Raid 1)
- Virtualisierung





Country Shifting

- Augen auf beim Serverkauf
  - Zustand des Gerätes
  - Stromverbrauch
  - Virtualisierung
    - Virtualisierungserweiterung im Prozessor
    - “zu viel Arbeitsspeicher” gibt es nicht
  - Erste Hilfe (Remote Schnittstelle)

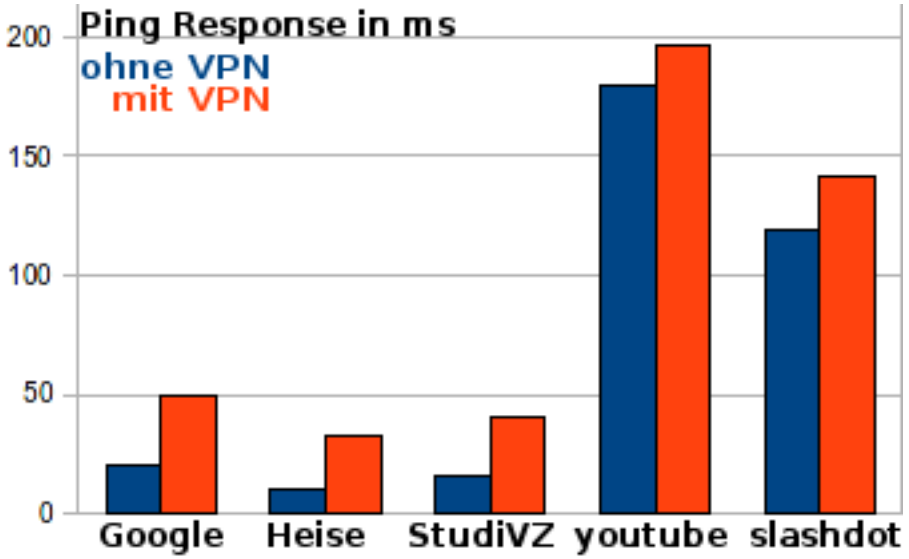


Country Shifting

- Wahl des Ziellandes
  - juristische Rahmenbedingungen
  - Kooperation mit deutschen Behörden/ EU
  - Währung (Wechselkursrisiko)
- Wahl des Rechenzentrums
  - sorgfältiger Tarifvergleich (Traffic, Strom)
  - Kosten für weitere IP-Adressen
  - tatsächlichen Standort des Servers vorher klären
  - Transportkosten

Country Shifting

- Erfahrungen
  - Surfen
    - leicht verzögert
  - Streaming
    - problemlos
  - IP-Telefonie
    - problemlos
  - Chatanwendungen (IM, IRC)
    - problemlos
  - Spiele
    - teilweise störende Verzögerungen



Country Shifting

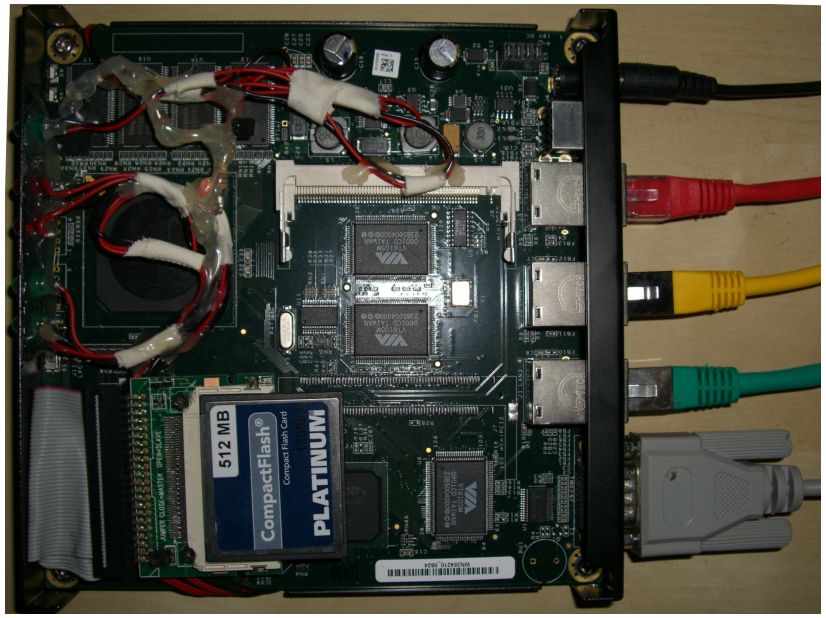
- Nachteile
  - höhere Latenz
  - doppeltes Datenaufkommen am Netzausstieg
  - statische IP
    - mangelnde Anonymität bei alleiniger Nutzung
    - “Diensteanbieter” bei gemeinsamer Nutzung
    - IP-Pool schwer zu realisieren

Country Shifting

- Fazit
  - Kostenintensiv (Gesamtkosten 635€)
  - für dauerhafte, private Nutzung nicht geeignet
  - zeitweise, gezielte Nutzung
- Alternativen
  - VPN-Anbieter
    - SwissVPN, Relakks, IPRedator, ...
  - TOR (je nach Standort des Exitnodes)


Para Neujahr

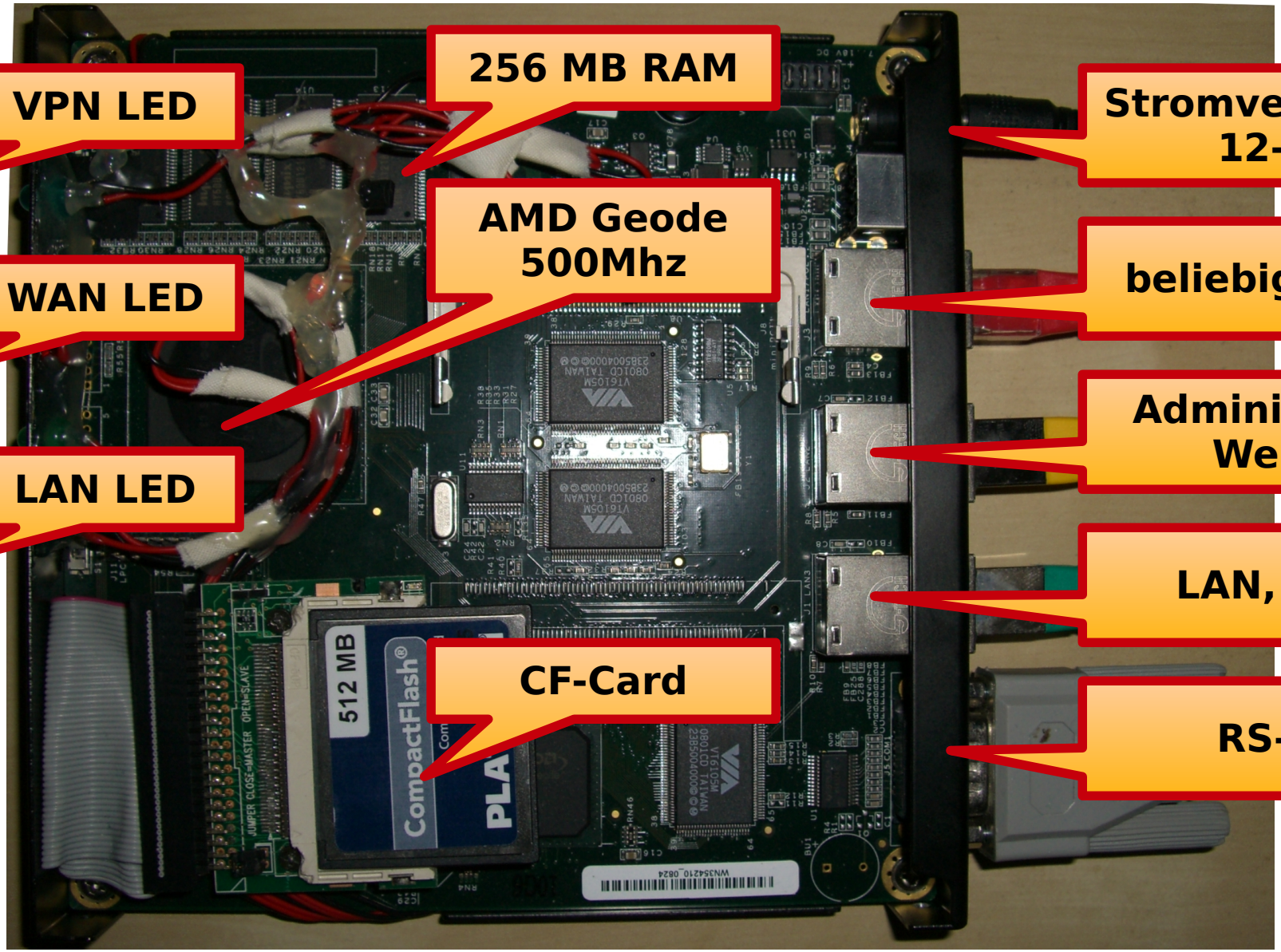
Tunnelende


512 MB
CompactFlash
Compact Flash Card
PLATINUM

Tunnelende

- Anforderungen
  - nicht proprietär
  - sicher
  - bezahlbar
  - einfache Bedienung
  - Eigenbau
- Umsetzung
  - PC Engines Board ALIX 2C3
  - CF-Card als Massenspeicher

Tunnelende



VPN LED

WAN LED

LAN LED

256 MB RAM

AMD Geode 500Mhz

CF-Card

Stromversorgung 12-18V

beliebiges WAN

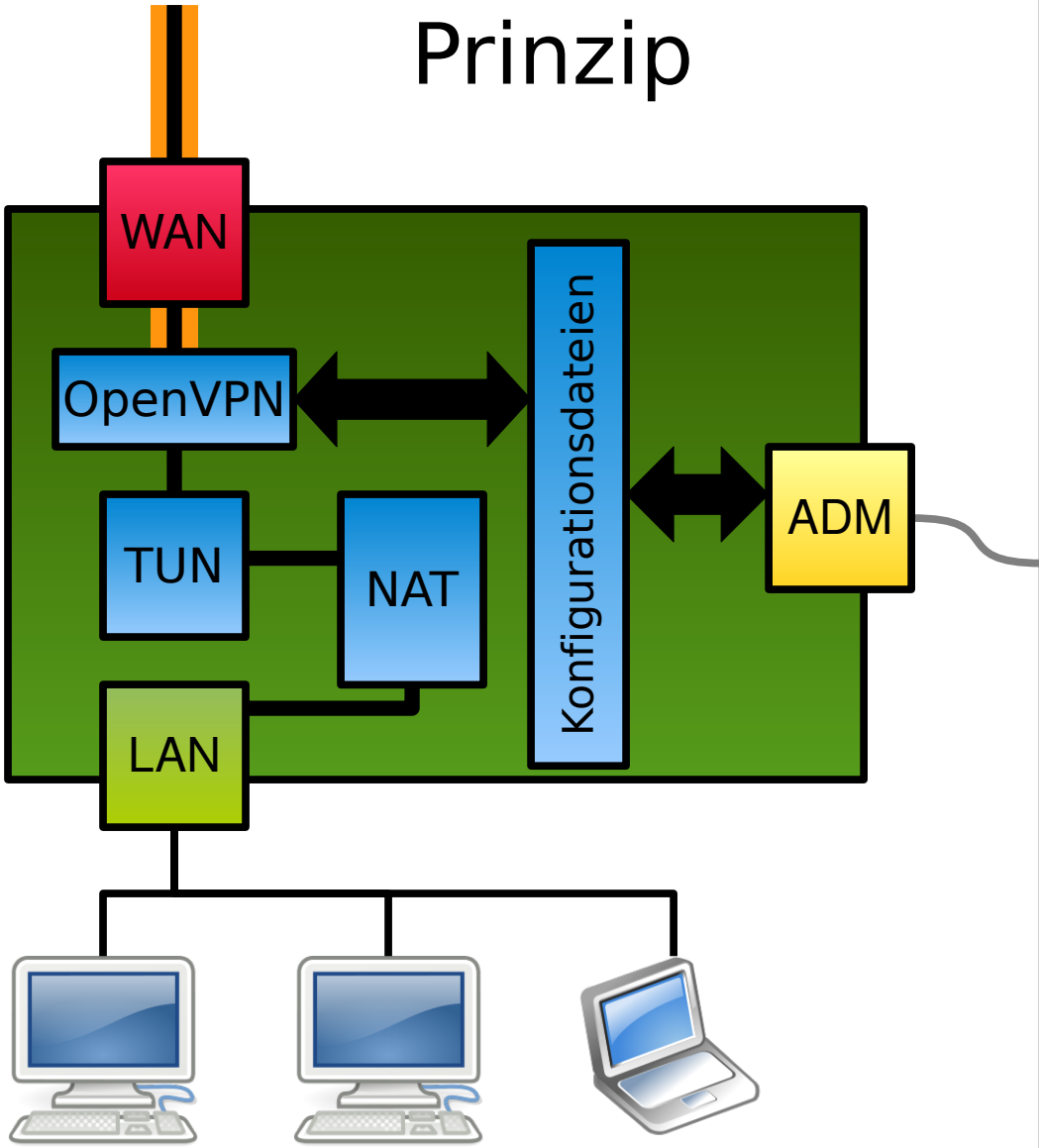
Administration Webgui

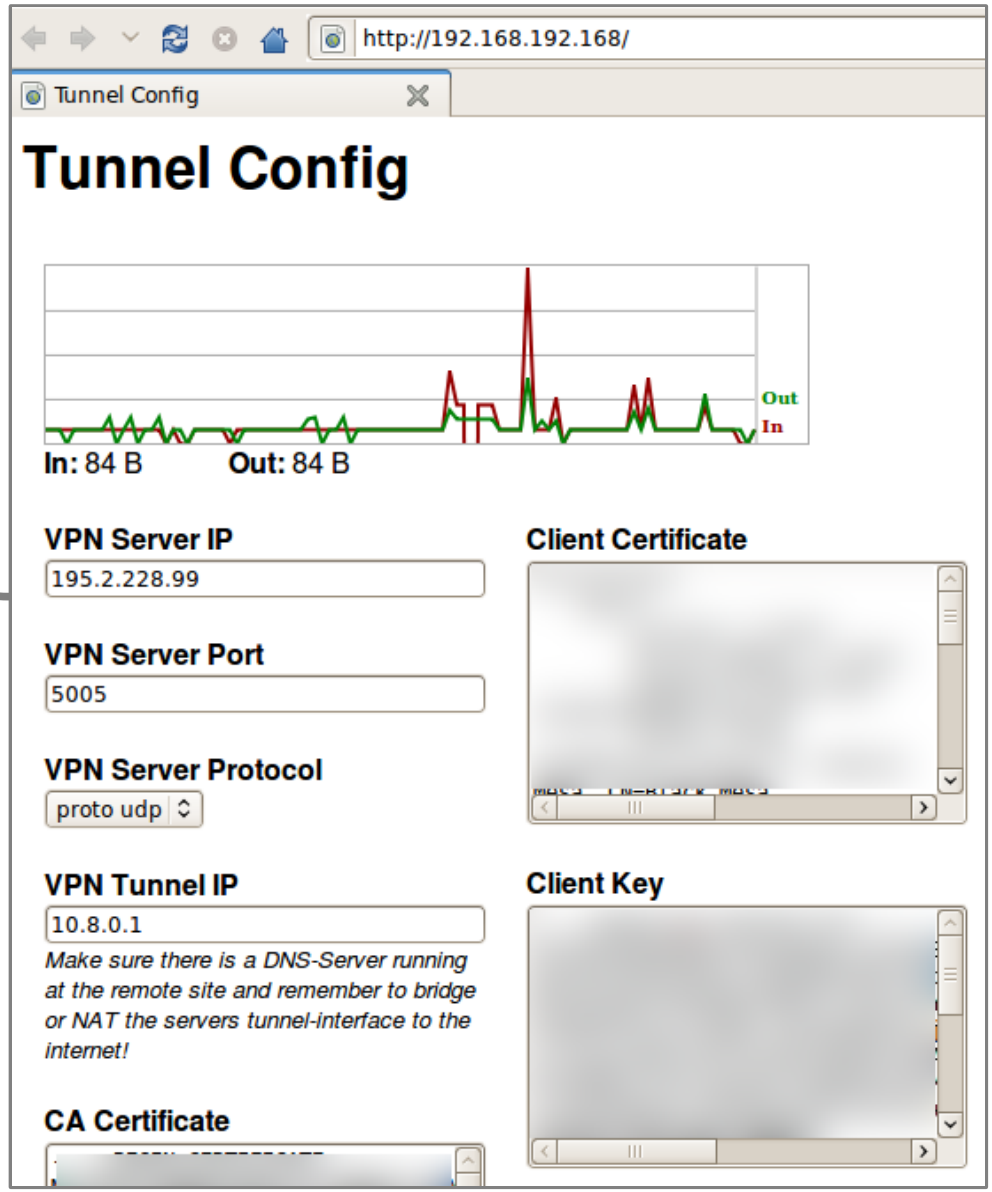
LAN, DHCP

RS-232

Tunnelende

Prinzip





Para Neujahr

Vielen Dank für Eure Aufmerksamkeit

Fragen?

weitere Informationen

- http://www.danluedtke.de/articles_tunnel.php

Quellen

- Grafiken: Flickr CC, Wikicommons, Gnome, Eigene
- RFCs, Manpages