



Was leistet ein VPN?

Hanno 'Rince' Wagner, Chaos Computer Club Stuttgart

Über den CCCS / über den Vortragenden

Über den CCCS:

regelmäßige Treffen seit Sommer 2001

Seit Oktober 2003 monatliche Vortragsreihe

Spaß am Gerät, aber Gefahren beachten und abwägen

Informieren statt abschrecken.

Über mich:

Seit September 1993 im Netz aktiv

(Mail, News, IRC; Relay Parties, CCC, Fitug, EDRI)

Heute: CCC(S), Datenschleuder, CSISAC Steering Committee

Agenda

- Wofür brauche ich ein VPN?
- Was ist ein VPN
- Welche Arten von VPN gibt es?
- VPN-Anbieter?
- Unterschied zu TOR?
- Erfahrungen

Wofür brauche ich ein VPN?

- Anwendungsfälle:
 - Ich möchte nicht, dass meine Eltern mitlesen was ich mache
 - Ich möchte nicht, dass mein Provider mitliest was ich mache
 - Ich möchte als Firma sicherstellen, dass nur vertrauenswürdige Personen in mein Netz kommen
 - Ich möchte zwei Standorte miteinander verbinden
 - Ich möchte im Netz pseudonym surfen
 - Oder auch ganz profan: Ich möchte Netflix USA sehen
 - Ich möchte Roadwarrior sein

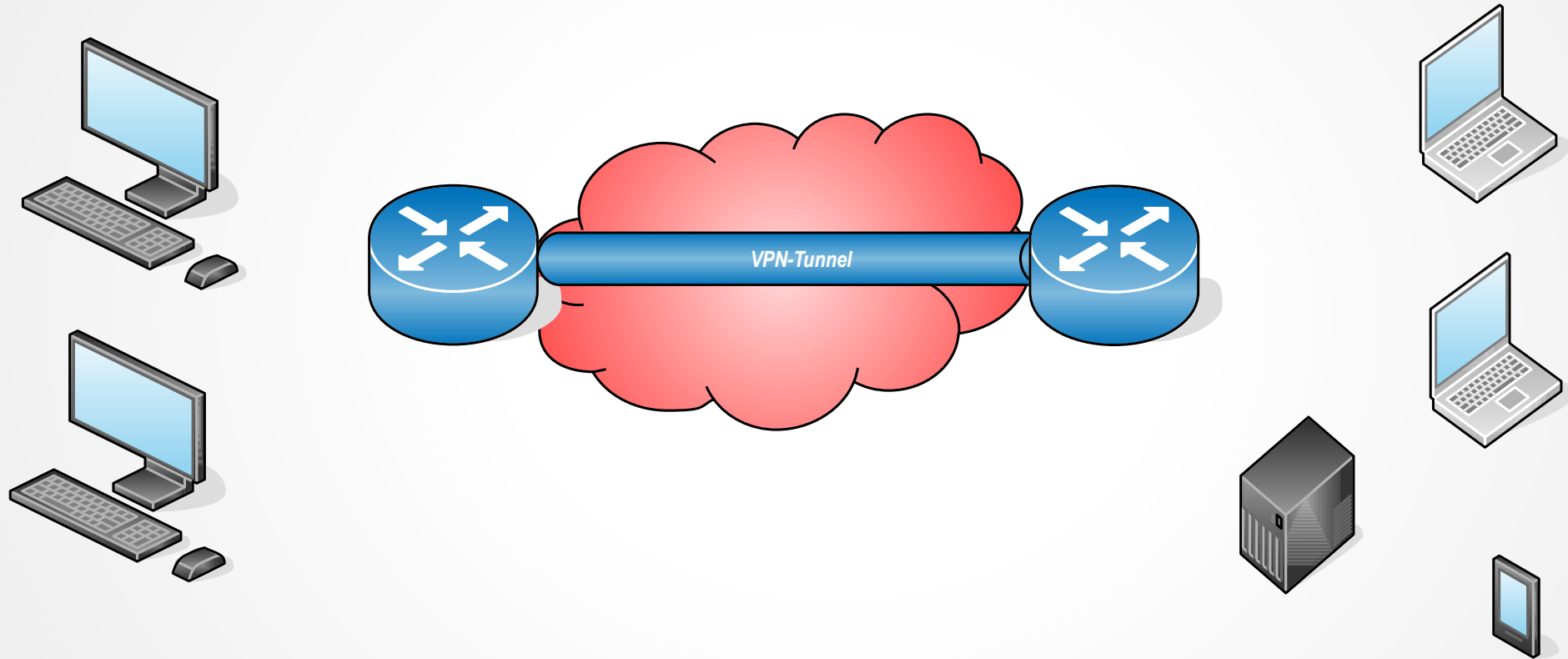
Was ist ein (klassisches) VPN?

- Ein VPN ist eine Verbindung von Punkt A zu Punkt B
- Es wird ein Tunnel zwischen diesen beiden Punkten erstellt
- Der Verkehr zwischen diesen beiden Punkten wird verschlüsselt und die Carrier dazwischen können den Inhalt nicht einsehen (und demzufolge nicht verändern)

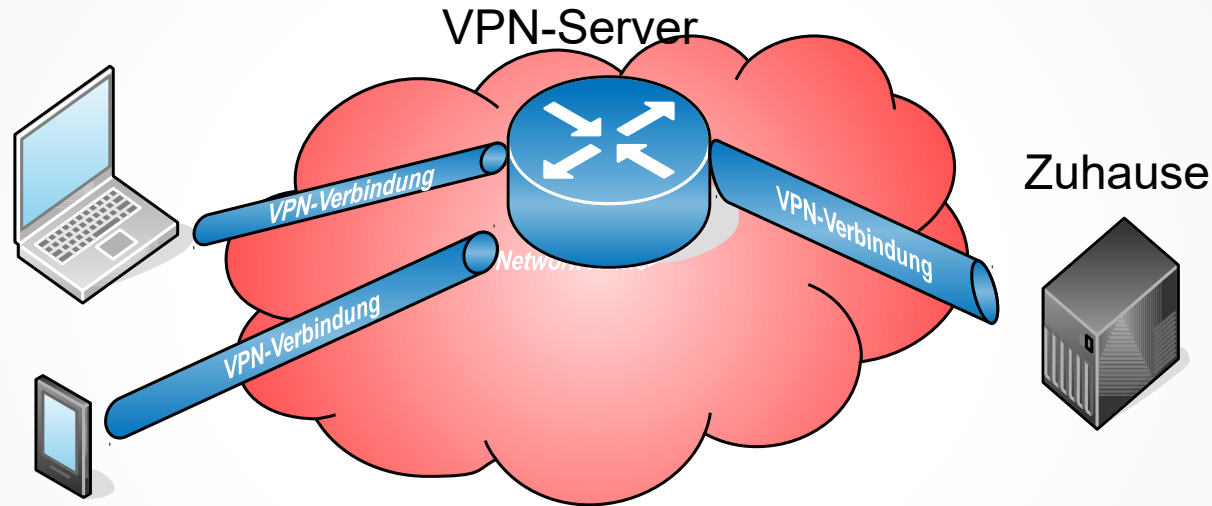
Was ist ein (klassisches) VPN?

- Über diesen Tunnel können ganze Netzwerke miteinander verbunden werden.
- Es können aber auch „nur“ zwei Rechner miteinander verbunden werden. Oder ein Laptop und ein Netzwerkspeicher.

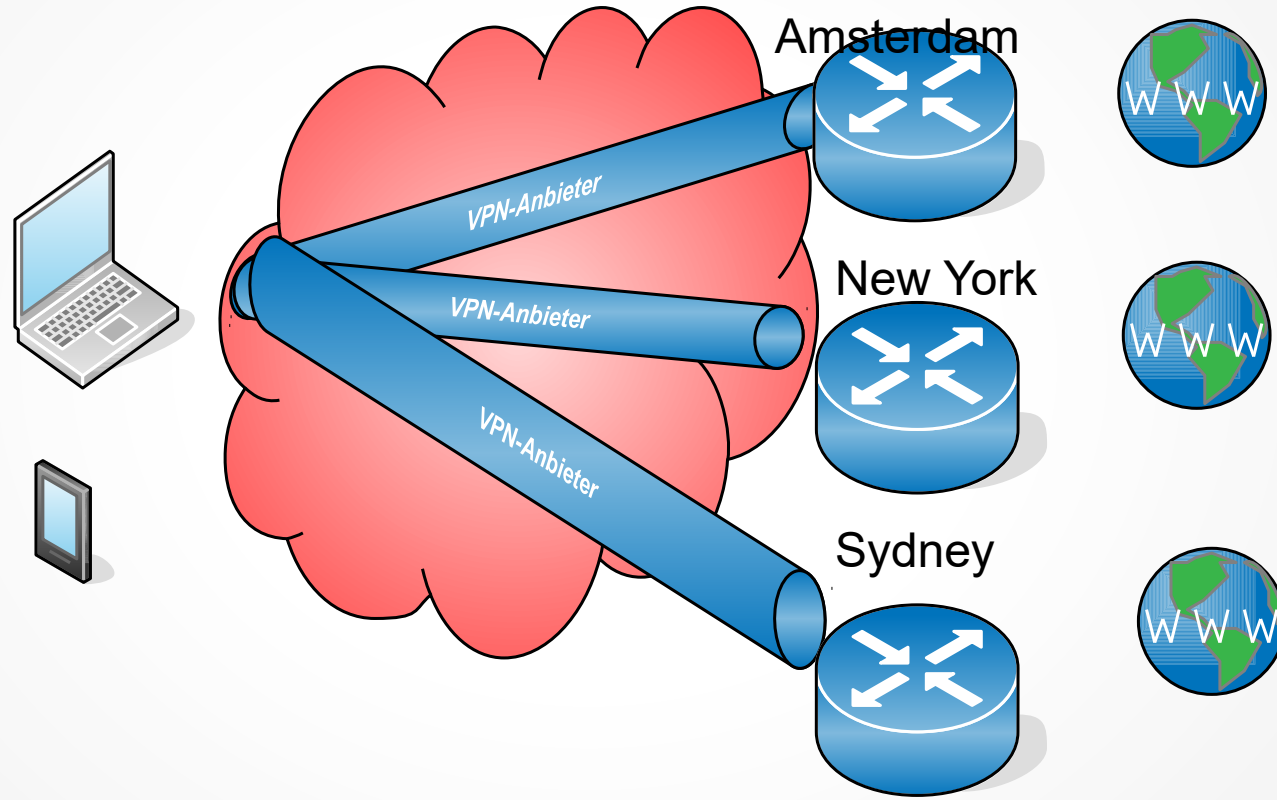
Was ist ein (klassisches) VPN?



Was ist ein (klassisches) VPN?



Was ist ein VPN mit Provider?



Was ist ein VPN?

- Es gibt verschiedene VPN-Software
 - OpenVPN
 - IPSec
 - WireGuard

Was braucht man?

- Ein Konzept: Man muss überlegen was alles über das VPN gehen soll: Sämtlicher Traffic? Nur CIFS-/NFS-Laufwerke? Nur SSH-Verbindungen? DNS-Abfragen?
- Software: Ein VPN ist wie ein neues Netzwerk. Dafür müssen beide Endpunkte dieselbe Software nutzen und sich dadurch verstehen.
- Konfiguration: VPNs müssen auf beiden Seiten konfiguriert werden: Je nach Software und Komplexität muss man nicht nur Schlüssel erstellen (für die Verschlüsselung) sondern auch das Netzwerk definieren.

VPN-Anbieter?

- Inzwischen werden VPNs über das Fernsehen und Youtube-Shots beworben
- Der Anbieter stellt den Endpunkt sowie oftmals vorkonfigurierte Software für den Nutzer bereit.
- Meistens gibt es OpenVPN-Verbindungen, aber auch IPSec wird angeboten
- Beworben wird Anonymität und ein besseres Gefühl.
- Aber: Man muss dem Anbieter vertrauen! Wie ist dies gerechtfertigt?

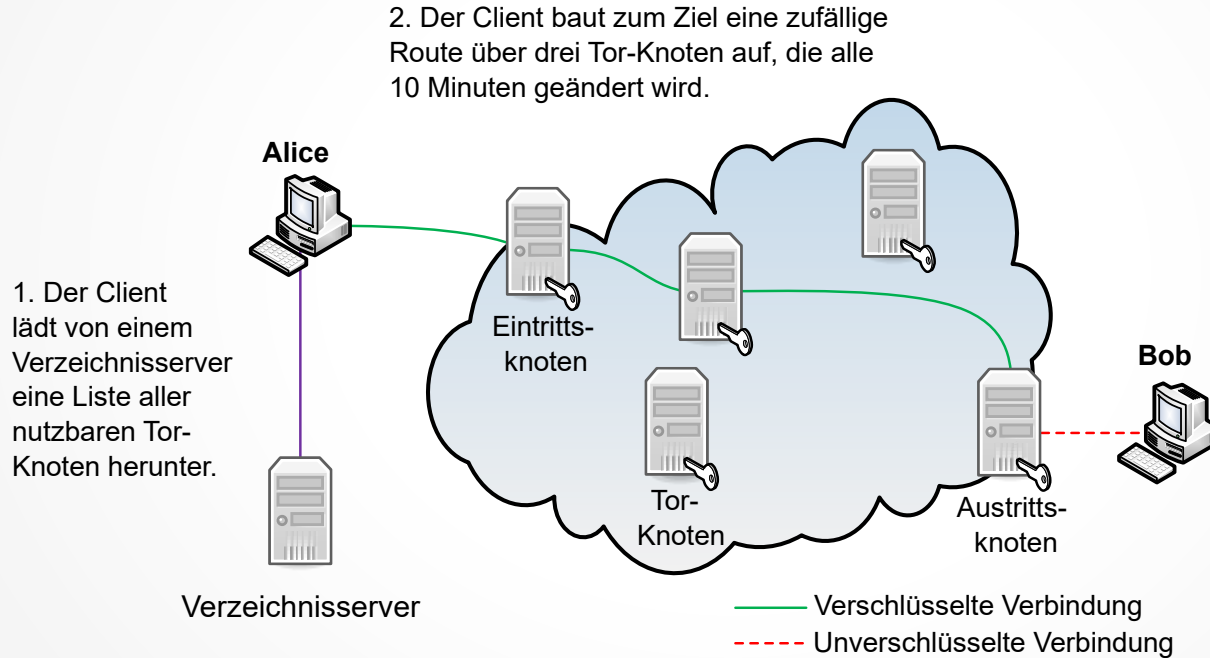
VPN-Anbieter?

- Gewerbliche VPN-Anbieter unterstützen dabei, dass der eigene Telekom-Provider nicht sehen kann, wohin man surft.
- Für Webseiten sehe ich aus, als ob ich von woanders komme.
- Zumindest wenn ich alles richtig konfiguriere!
- Aber: Der VPN-Provider sieht weiterhin alles, was aus dem Tunnel kommt.
- Und: Facebook (sowie anderen Webseiten) ist egal, von wo ich mich einlogge – wenn ich mich einlogge, kennen sie mich und können mich weiterhin tracken, auch über VPNs hinweg.

Was ist TOR?

- Tor ist ein spezielles VPN
- Hier geht der Verkehr über mehrere Knotenpunkte
- Jeder Knotenpunkt kennt nur seinen Vor- und Nachgänger, aber nicht mehr.
- Dein Traffic wird über mindestens 3 Knotenpunkte gelenkt. Damit wird sichergestellt das kein Knoten alle zur Identifikation notwendigen Informationen besitzt.
- Alle 10 Minuten werden die Verbindungen geändert
- Damit wird der Verkehr anonymisiert

Was ist TOR?



Was ist SPN?

- SPN steht für „safing private network“
- Nutzt das TOR-Prinzip
- Kann Anwendungen „individuell“ routen
- Kann Geo-Blocking automatisiert verhindern(?)
- Teil der Portmaster-Firewall
- Hat aber für den Zugriff ein Accounting, also gibt es irgendwo einen Server der einen Account einem Nutzer zuordnen kann, selbst wenn man für den Traffic anonymisierte Tokens verwendet.

Die Fritzbox kann auch VPN?

- Fritzboxen bieten auch ein VPN für den Heimnutzer an.
- Heutzutage benötigt man dafür ein Konto bei dem Hersteller (AVM). Dann konfiguriert man auf seiner Fritzbox einen Benutzer und ein Passwort und wählt einen (weltweit eindeutigen) Namen für die Fritzbox.
- Für Linux und MacOS kann man mit „vpnc“ (Cisco VPN-Client) arbeiten, unter Windows benötigt man Fremdsoftware. Es gibt aber Anleitungen im Netz.
- Auch mit dem Handy kann man so auf das Heimnetz zugreifen.

Der Roadwarrior

- Der Roadwarrior möchte meistens sein eigenes VPN haben: Er hat Dienste zuhause, aber auch im Netz Cloud-Systeme, die er vertrauenswürdig ansprechen möchte.
- Dafür baut er ein VPN-Netz auf, in dem sich die verschiedenen Geräte / Netze einwählen. Ein Der VPN-Server vergibt die Tunnel-IP-Adressen, je nach Architektur geht der gesamte Traffic über den Server oder die Systeme meshen und verteilen den Traffic.
- So etwas wird zB gerne für Backups gemacht. Oder auch um überall Debian-Pakete bauen zu können ;)
- Es gibt inzwischen mobile Router (mit Akku), die für diesen Einsatz (linux-basiert) gebaut sind. Diese verbinden sich direkt nach dem Einloggen beim Telekom-Provider mit dem VPN-Server, spannen ein WLAN auf welches man nutzt und kümmern sich um die Sicherheit der Verbindung. Einer davon heisst ähnlich wie ein Maultier...

Erfahrungen

- Wenn das VPN kostengünstig angeboten wird, womit verdient der Anbieter sein Geld?
- Der Anbieter sieht am Tunnelendpunkt natürlich alle Daten die wir verschicken – er kann sehen welche Webseiten wir besuchen. Im Zweifelsfall eigene Tracker mit einbauen. Oder eigene Werbung.
- Es gab schon mehrfach Anbieter, die mitloggen obwohl sie in der Werbung behaupten dies nicht zu tun.
- Um nur seinen Heimserver zu erreichen, sind einfache, selbstgebaute VPNs gut nutzbar. Für komplexere Aufgaben (Roadwarrior) braucht man Verständnis der Technik und auch mehr Erfahrung wie man das VPN so konfiguriert dass es auch richtig funktioniert.
- Auch das Web verändert sich. Seitdem Browser interaktiv sind und Scripte ausführen kann auch hierüber die Anonymität verlorengehen wenn das Script ungewöhnliche Verbindungen aufbauen darf oder durch Fehler aufbauen kann.
- Wenn man nur bestimmte Dienste nutzen will, reicht eventuell ein SSH-Forwarding aus?

Empfehlungen

- Ich empfehle keinen Anbieter ;)
- Man kann aber daran ablesen ob ein Anbieter seriös ist, ob es ihn
 - Schon länger gibt
 - Keine oder wenige negative Berichte in der Presse (nicht soziale Medien)
 - Gesundes Geschäftsmodell

Fragen?

Danke für die
Aufmerksamkeit



Nächsten Monat

Am 13.04.2023

stellen sich befreundete Gruppen vor:

Java User Group (JUGS)

no-spy.org