OpenVPN - Der Versuch einer Einführung

Joel Garske, DuLUG, 2008.03

April 4, 2008

Es folgt...

1. Was ist ein VPN?
2. OpenVPN
3. Szenarien
4. Material

Was ist ein VPN? - Definition

"Ein Virtual Private Network (dt. virtuelles privates Netz; kurz VPN) ist ein reines Softwareprodukt (daher 'virtuell') und dient der Einbindung von entfernten Geräten eines benachbarten Netzes an das eigene (private) Netz, ohne dass die Netzwerke zueinander kompatibel sein müssen."

Wikipedia Artikel 'VPN' 03.2008

Was ist ein VPN? - Definition

Oder einfacher:

> *"Ein Virtual Private Network dient der Einbindung von entfernten Geräten an das eigene (private) Netz."*

Frei nach Wikipedia Artikel 'VPN' 03.2008

Wozu? - Anwendungsfälle

Beispielhafte Anwendungsfälle

- Aussendienst-Anbindung
- Standortvernetzung
- Wartungszugang
- IP-Telefonie
- Topologische Zentralisierung
- Rechte-Differenzierung in einem physischen Medium

Wozu? - Anwendungsfälle

Beispielhafte Anwendungsfälle

- Aussendienst-Anbindung
- Standortvernetzung
- Wartungszugang
- IP-Telefonie
- Topologische Zentralisierung
- Rechte-Differenzierung in einem physischen Medium

Wozu? - Anwendungsfälle

Beispielhafte Anwendungsfälle

- Aussendienst-Anbindung
- Standortvernetzung
- Wartungszugang
- IP-Telefonie
- Topologische Zentralisierung
- Rechte-Differenzierung in einem physischen Medium

Womit? - Verwendbare Software

Netzwerk-zentriert

- OpenVPN

Anwendungs-zentriert

Womit? - Verwendbare Software

Netzwerk-zentriert

- OpenVPN
- IPSec

Anwendungs-zentriert

Womit? - Verwendbare Software

Netzwerk-zentriert

- OpenVPN
- IPSec
- PPTP

Anwendungs-zentriert

Womit? - Verwendbare Software

Netzwerk-zentriert

- OpenVPN
- IPSec
- PPTP

Anwendungs-zentriert

- Remote Desktop

Womit? - Verwendbare Software

Netzwerk-zentriert

- OpenVPN
- IPSec
- PPTP

Anwendungs-zentriert

- Remote Desktop
- Application Services

Womit? - Verwendbare Software

Netzwerk-zentriert

- OpenVPN
- IPSec
- PPTP

Anwendungs-zentriert

- Remote Desktop
- Application Services
- 'SSL VPN'

Womit? - Verwendbare Software

Netzwerk-zentriert

- OpenVPN
- IPSec
- PPTP

Anwendungs-zentriert

- Remote Desktop
- Application Services
- 'SSL VPN'

Womit? - Verwendbare Software

Netzwerk-zentriert

- OpenVPN
- IPSec
- PPTP

Anwendungs-zentriert

- Remote Desktop
- Application Services
- 'SSL VPN'

OpenVPN

OpenVPN stellt sich vor:

> *"OpenVPN is a full-featured open source SSL VPN solution that accommodates a wide range of configurations[...]."*
>
> *"OpenVPN ist eine umfangreiche OpenSource VPN-Lösung, die ein breites Spektrum an Szenarien ermöglicht [...]."*

Eckdaten

- Open Source

Eckdaten

- Open Source
- basiert auf OpenSSL

Eckdaten

- Open Source
- basiert auf OpenSSL
- benutzt unter Linux TUN/TAP Kernel-API

Eckdaten

- Open Source
- basiert auf OpenSSL
- benutzt unter Linux TUN/TAP Kernel-API

Arbeitsweise von OpenVPN

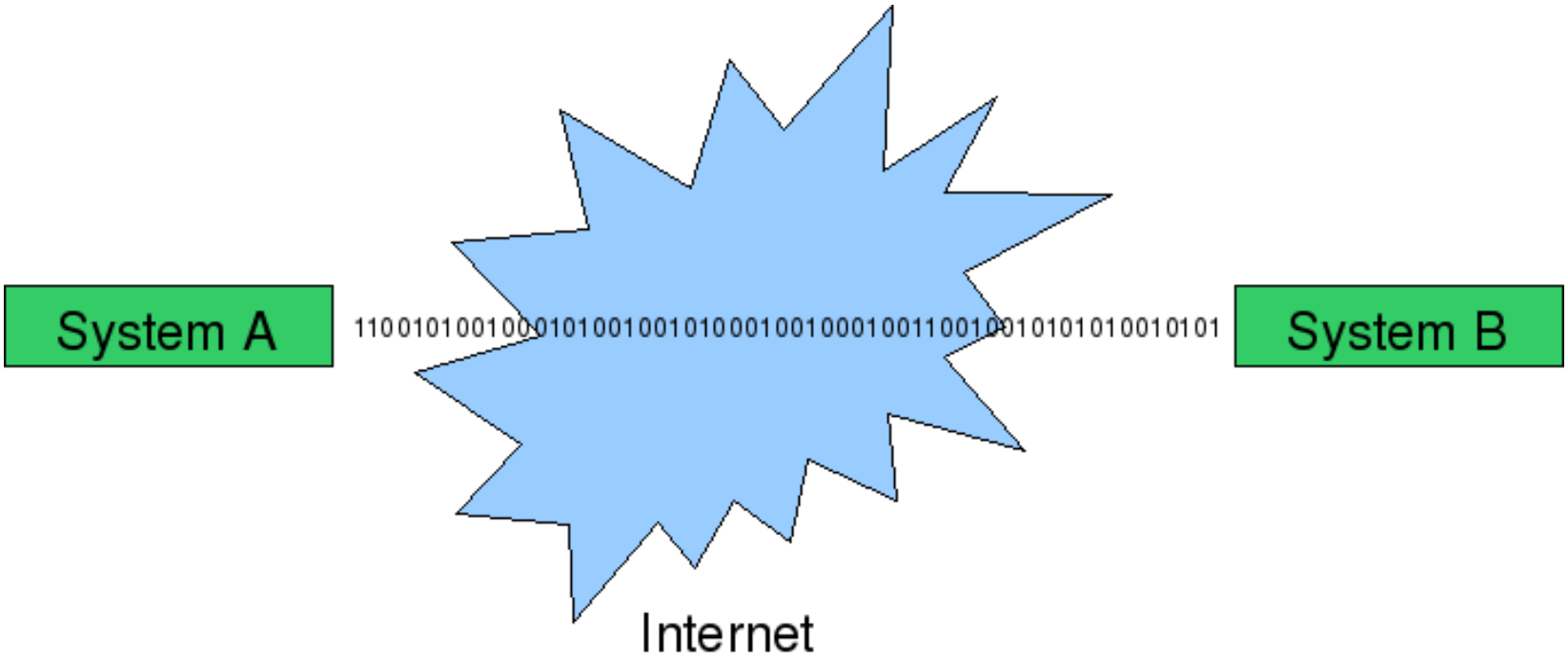

Figure: ungesicherte Kommunikation

Arbeitsweise von OpenVPN

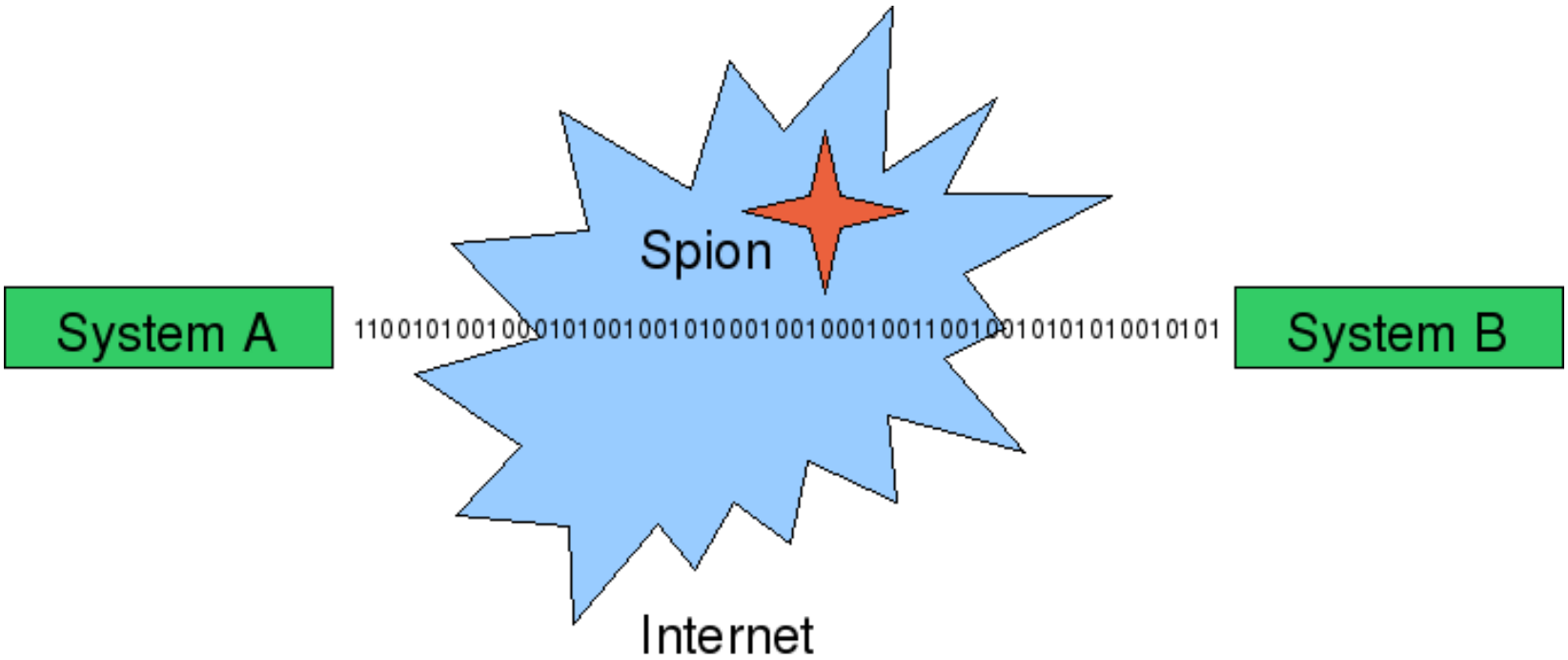

Figure: ungesicherte Kommunikation (ist doof)

Arbeitsweise von OpenVPN

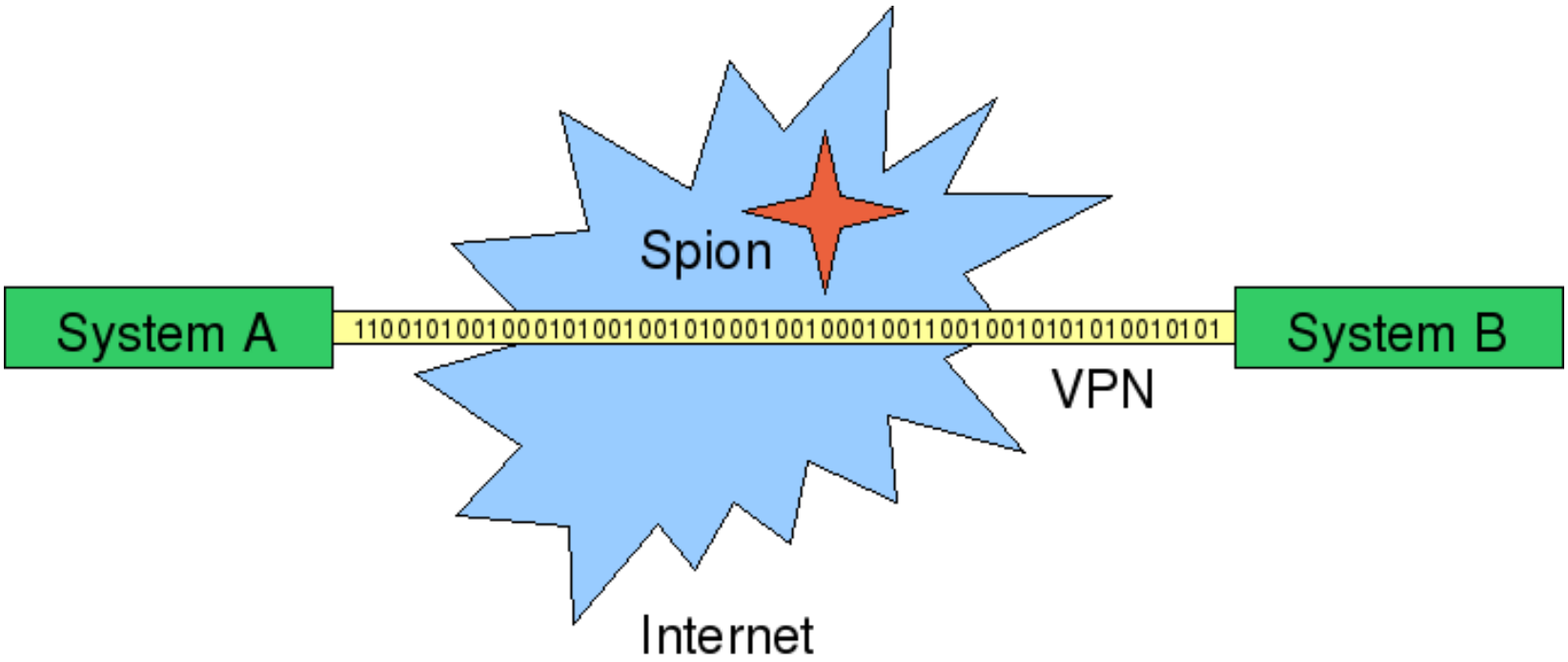

Figure: gesicherte Kommunikation (ist besser)

Möglichkeiten von OpenVPN

Figure: TCP/IP Schichten zweier Systeme

Möglichkeiten von OpenVPN

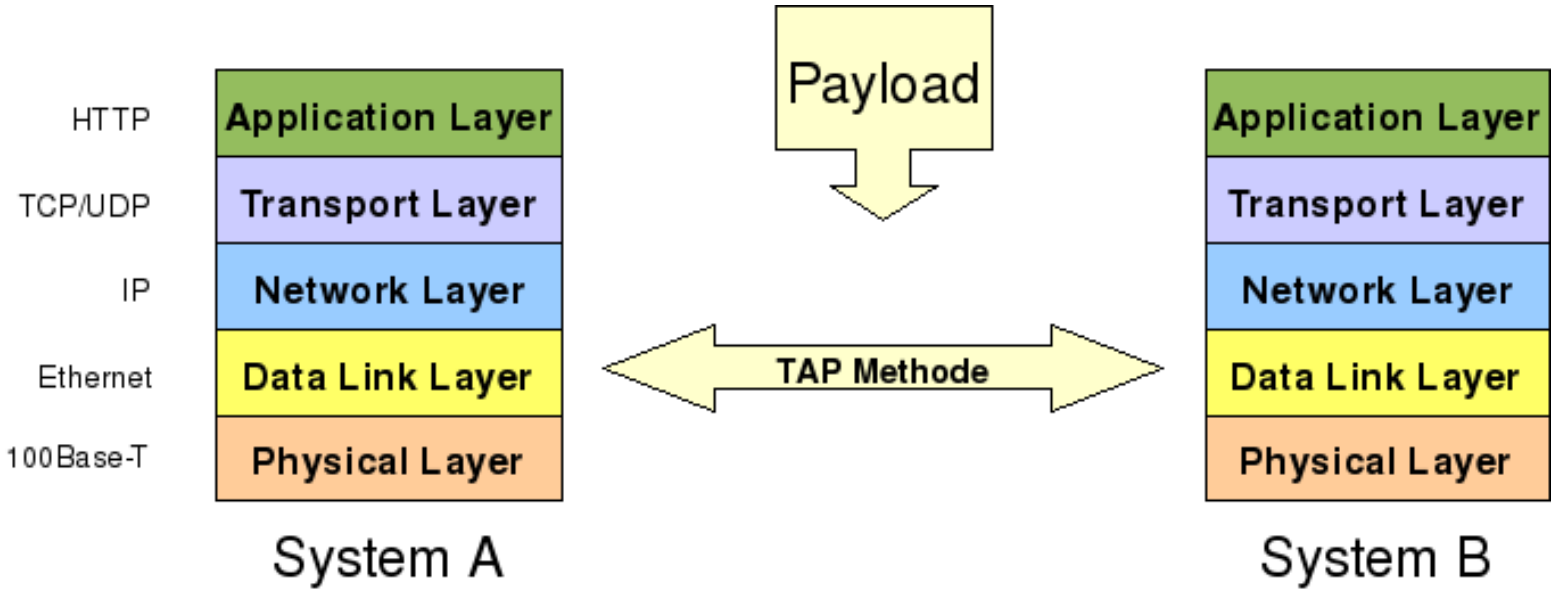

Figure: TAP-Methode auf TCP/IP- oder OSI-Layer 2

Möglichkeiten von OpenVPN

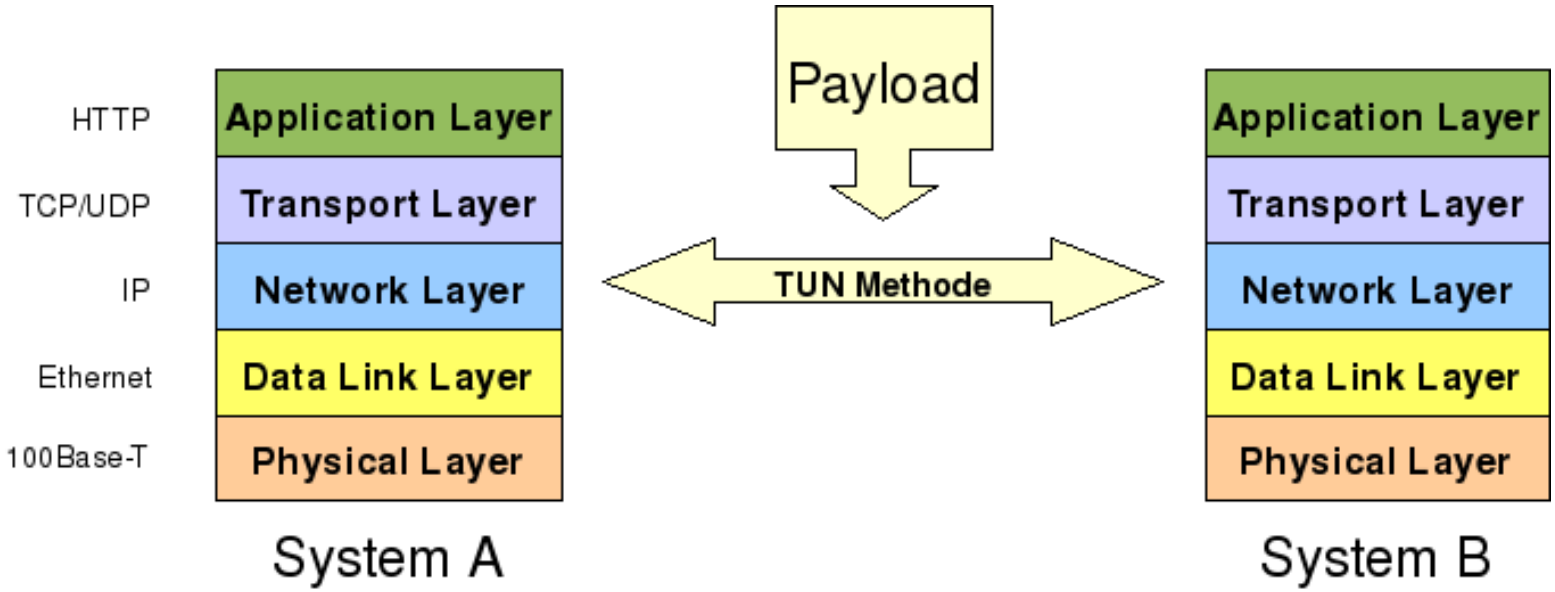

Figure: TUN-Methode auf TCP/IP- oder OSI-Layer 3

VPN-Szenarien

- Aussendienst - Host to Host
- Standortvernetzung - Net to Net

Host to Host - Topologie

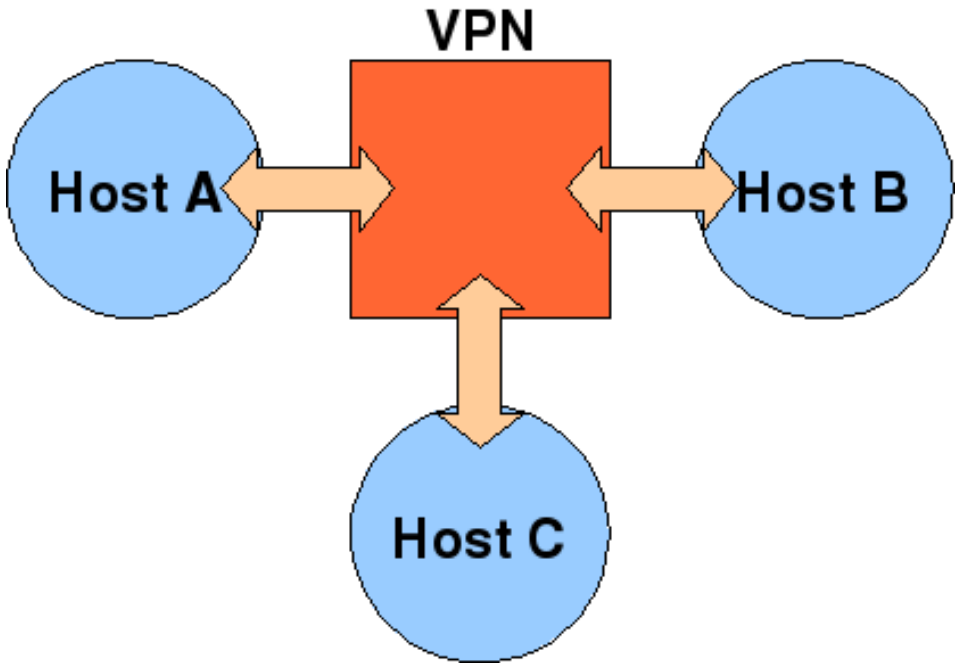

Figure: OpenVPN Host-to-Host Vernetzung mit TAP

Net to Net - Topologie

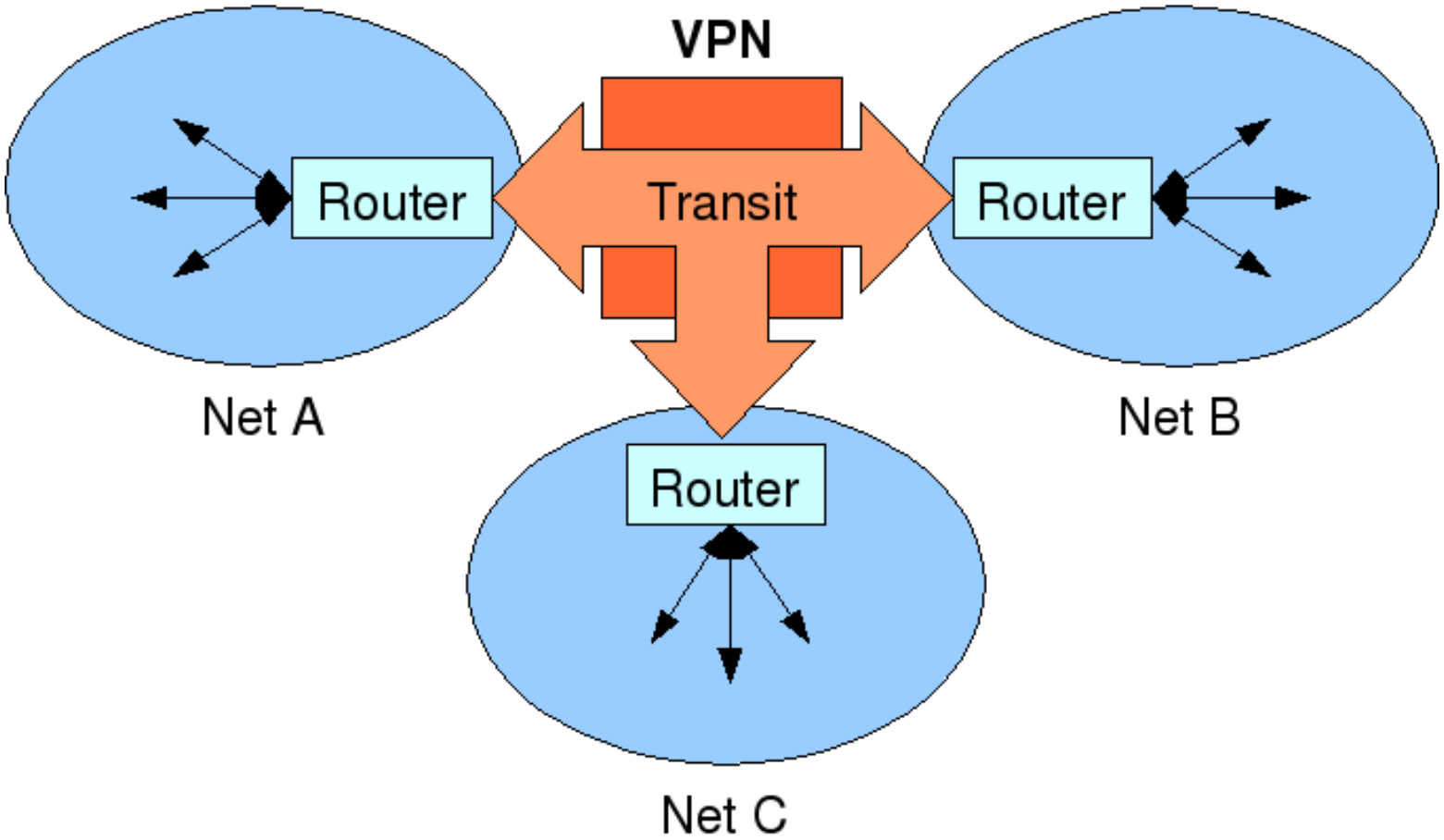

Figure: OpenVPN Net-to-Net Vernetzung mit TAP

Aufbau einer SSL PKI

Aufbau einer SSL PKI

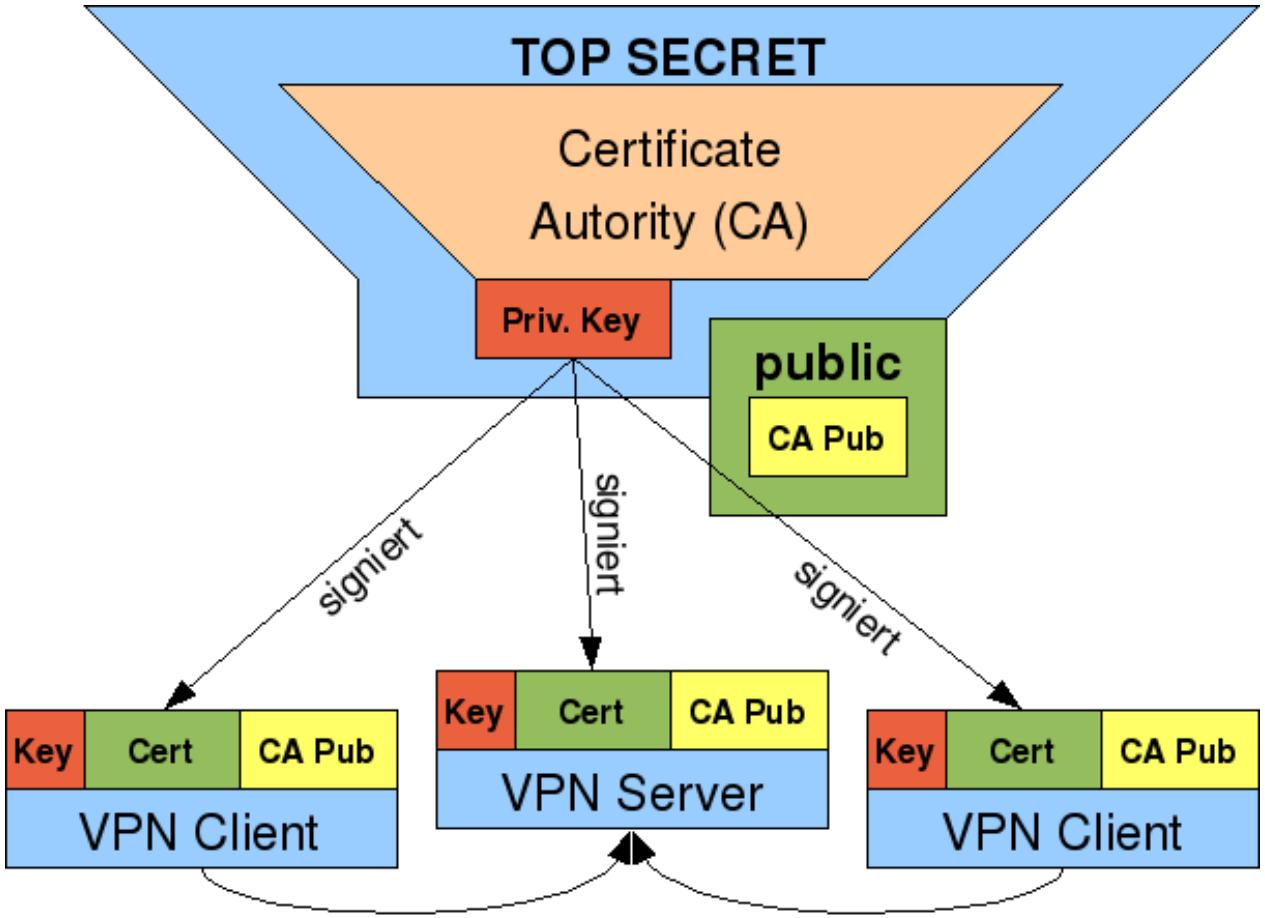

Figure: OpenSSL CA Aufbau als OpenVPN PKI

Erstellen einer SSL PKI mit easyRSA

Erstellen der CA

1. ./vars anpassen

Erstellen einer SSL PKI mit easyRSA

Erstellen der CA

1. ./vars anpassen
   - KEY_COUNTRY
   - KEY_PROVINCE
   - KEY_CITY
   - KEY_ORG
   - KEY_EMAIL
2. . ./vars

Erstellen einer SSL PKI mit easyRSA

Erstellen der CA

1. ./vars anpassen
   - KEY_COUNTRY
   - KEY_PROVINCE
   - KEY_CITY
   - KEY_ORG
   - KEY_EMAIL
2. . ./vars
3. ./clean-all

Erstellen einer SSL PKI mit easyRSA

Erstellen der CA

1. ./vars anpassen
   - KEY_COUNTRY
   - KEY_PROVINCE
   - KEY_CITY
   - KEY_ORG
   - KEY_EMAIL
2. . ./vars
3. ./clean-all
4. ./build-ca

Erstellen einer SSL PKI mit easyRSA

Erstellen der CA

1. ./vars anpassen
   - KEY_COUNTRY
   - KEY_PROVINCE
   - KEY_CITY
   - KEY_ORG
   - KEY_EMAIL
2. . ./vars
3. ./clean-all
4. ./build-ca

Erstellen einer SSL PKI mit easyRSA

Erstellen der Server- und Client-Keys

1. ./build-dh

Erstellen einer SSL PKI mit easyRSA

Erstellen der Server- und Client-Keys

1. ./build-dh
2. ./build-key-server server

Erstellen einer SSL PKI mit easyRSA

Erstellen der Server- und Client-Keys

1. ./build-dh
2. ./build-key-server server
3. ./build-key client1

Erstellen einer SSL PKI mit easyRSA

Erstellen der Server- und Client-Keys

1. ./build-dh
2. ./build-key-server server
3. ./build-key client1
4. ./build-key client2

Erstellen einer SSL PKI mit easyRSA

Erstellen der Server- und Client-Keys

1. ./build-dh
2. ./build-key-server server
3. ./build-key client1
4. ./build-key client2
5. ... and so on

Erstellen einer SSL PKI mit easyRSA

Erstellen der Server- und Client-Keys

1. ./build-dh
2. ./build-key-server server
3. ./build-key client1
4. ./build-key client2
5. ... and so on

Erstellen einer SSL PKI mit easyRSA

```
2008-03-28 13:05 ca.crt
2008-03-28 13:05 ca.key
2008-03-28 13:08 client1.crt
2008-03-28 13:08 client1.csr
2008-03-28 13:08 client1.key
2008-03-28 13:09 client2.crt
2008-03-28 13:09 client2.csr
2008-03-28 13:09 client2.key
2008-03-28 13:07 dh1024.pem
2008-03-28 13:04 index.txt
2008-03-28 13:04 serial
2008-03-28 13:08 server.crt
2008-03-28 13:08 server.csr
2008-03-28 13:08 server.key
```

Figure: Verzeichnis-Listing von ./keys

Konfiguration Server (TAP, Layer 2)

server.conf

1. server-bridge 10.0.0.1 255.0.0.0 10.0.0.2 10.255.255.254
2. dev tap
3. proto tcp
4. port 1194
5. ca /etc/openvpn/keys/ca.crt
6. cert /etc/openvpn/keys/server.crt
7. key /etc/openvpn/keys/server.key
8. dh /etc/openvpn/keys/dh1024.pem
9. client-to-client
10. ifconfig-pool-persist ipp.txt

Konfiguration Server (TAP, Layer 2)

server.conf

1. server-bridge 10.0.0.1 255.0.0.0 10.0.0.2 10.255.255.254
2. dev tap
3. proto tcp
4. port 1194
5. ca /etc/openvpn/keys/ca.crt
6. cert /etc/openvpn/keys/server.crt
7. key /etc/openvpn/keys/server.key
8. dh /etc/openvpn/keys/dh1024.pem
9. client-to-client
10. ifconfig-pool-persist ipp.txt

Konfiguration Server (TAP, Layer 2)

server.conf

1. server-bridge 10.0.0.1 255.0.0.0 10.0.0.2 10.255.255.254
2. dev tap
3. proto tcp
4. port 1194
5. ca /etc/openvpn/keys/ca.crt
6. cert /etc/openvpn/keys/server.crt
7. key /etc/openvpn/keys/server.key
8. dh /etc/openvpn/keys/dh1024.pem
9. client-to-client
10. ifconfig-pool-persist ipp.txt

Konfiguration Server (TAP, Layer 2)

server.conf

1. server-bridge 10.0.0.1 255.0.0.0 10.0.0.2 10.255.255.254
2. dev tap
3. proto tcp
4. port 1194
5. ca /etc/openvpn/keys/ca.crt
6. cert /etc/openvpn/keys/server.crt
7. key /etc/openvpn/keys/server.key
8. dh /etc/openvpn/keys/dh1024.pem
9. client-to-client
10. ifconfig-pool-persist ipp.txt

Konfiguration Server (TAP, Layer 2)

server.conf

1. server-bridge 10.0.0.1 255.0.0.0 10.0.0.2 10.255.255.254
2. dev tap
3. proto tcp
4. port 1194
5. ca /etc/openvpn/keys/ca.crt
6. cert /etc/openvpn/keys/server.crt
7. key /etc/openvpn/keys/server.key
8. dh /etc/openvpn/keys/dh1024.pem
9. client-to-client
10. ifconfig-pool-persist ipp.txt

Konfiguration Client (TAP, Layer 2)

client.conf

1. client
2. remote vpn.domain.tld 1194
3. resolv-retry infinite
4. dev tap
5. proto tcp
6. nobind
7. ca /etc/openvpn/keys/ca.crt
8. cert /etc/openvpn/keys/client1.crt
9. key /etc/openvpn/keys/client1.key

Konfiguration Client (TAP, Layer 2)

client.conf

1. client
2. remote vpn.domain.tld 1194
3. resolv-retry infinite
4. dev tap
5. proto tcp
6. nobind
7. ca /etc/openvpn/keys/ca.crt
8. cert /etc/openvpn/keys/client1.crt
9. key /etc/openvpn/keys/client1.key

Konfiguration Client (TAP, Layer 2)

client.conf

1. client
2. remote vpn.domain.tld 1194
3. resolv-retry infinite
4. dev tap
5. proto tcp
6. nobind
7. ca /etc/openvpn/keys/ca.crt
8. cert /etc/openvpn/keys/client1.crt
9. key /etc/openvpn/keys/client1.key

Konfiguration Client (TAP, Layer 2)

client.conf

1. client
2. remote vpn.domain.tld 1194
3. resolv-retry infinite
4. dev tap
5. proto tcp
6. nobind
7. ca /etc/openvpn/keys/ca.crt
8. cert /etc/openvpn/keys/client1.crt
9. key /etc/openvpn/keys/client1.key

Ausrollen des VPN

Schritte im Rollout

- Keyfiles kopieren

Ausrollen des VPN

Schritte im Rollout

- Keyfiles kopieren
- Configs kopieren

Ausrollen des VPN

Schritte im Rollout

- Keyfiles kopieren
- Configs kopieren
- IP auf Server-TAP-Interface konfigurieren

Ausrollen des VPN

Schritte im Rollout

- Keyfiles kopieren
- Configs kopieren
- IP auf Server-TAP-Interface konfigurieren

Weitere Schritte bei Net-to-Net

Ausrollen des VPN

Schritte im Rollout

- Keyfiles kopieren
- Configs kopieren
- IP auf Server-TAP-Interface konfigurieren

Weitere Schritte bei Net-to-Net

- Routen vom Server mit "push" an Clients pushen

Ausrollen des VPN

Schritte im Rollout

- Keyfiles kopieren
- Configs kopieren
- IP auf Server-TAP-Interface konfigurieren

Weitere Schritte bei Net-to-Net

- Routen vom Server mit "push" an Clients pushen
  - push "route 192.168.3.0 255.255.255.0 172.16.42.16 15"

Ausrollen des VPN

Schritte im Rollout

- Keyfiles kopieren
- Configs kopieren
- IP auf Server-TAP-Interface konfigurieren

Weitere Schritte bei Net-to-Net

- Routen vom Server mit "push" an Clients pushen
  - push "route 192.168.3.0 255.255.255.0 172.16.42.16 15"
- Routen auf Server in Routingtable eintragen

Ausrollen des VPN

Schritte im Rollout

- Keyfiles kopieren
- Configs kopieren
- IP auf Server-TAP-Interface konfigurieren

Weitere Schritte bei Net-to-Net

- Routen vom Server mit "push" an Clients pushen
  - push "route 192.168.3.0 255.255.255.0 172.16.42.16 15"
- Routen auf Server in Routingtable eintragen

Ausrollen des VPN

Schritte im Rollout

- Keyfiles kopieren
- Configs kopieren
- IP auf Server-TAP-Interface konfigurieren

Weitere Schritte bei Net-to-Net

- Routen vom Server mit "push" an Clients pushen
  - push "route 192.168.3.0 255.255.255.0 172.16.42.16 15"
- Routen auf Server in Routingtable eintragen

Material

- http://www.openvpn.net/ - OpenVPN
- http://www.openssl.org/ - OpenSSL Kryptographie
- http://openvpn.net/index.php/documentation/howto.html - HowTos zu OpenVPN

Herzlichen Dank...