

# Virtual Private Network mit OpenVPN

The screenshot shows the OpenVPN website homepage. At the top is the OpenVPN logo and a 'Follow us' button with a Twitter icon. The main heading reads 'Your private path to access network resources and services securely'. Below this are three columns: 'VPN Service' with icons for 'PROTECTION', 'ENCRYPTION', and 'PRIVACY'; 'VPN Solution' with a globe and arrows; and 'Community' with a group of people. A banner below these columns states 'OpenVPN has you protected against the OpenSSL Heartbleed vulnerability'. The 'Downloads' section features icons for 'FOR YOUR PC', 'FOR YOUR MAC', 'FOR YOUR ANDROID', and 'FOR YOUR IPHONE/IPAD'. The footer contains a navigation menu with links like 'About', 'Jobs', 'News', 'Contact', 'Partners', 'Support', 'Privacy Policy', and 'Terms of Use', along with copyright information for 2002-2014 OpenVPN Technologies, Inc.

© by T. Kling (kling@gds2-verw.de) P. Kraut (kraut@gds2.de), 2015. This work is licensed under the **Creative Commons Attribution-NonCommercial-ShareAlike 2.0 License**. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-sa/2.0/de/>



# Virtual Private Network ?!?

Ziele sicherer Kommunikation:

**Vertraulichkeit, Authentisierung, Integrität**

VPN verbindet Rechner und/oder Netzwerke miteinander, indem es andere (öffentliche) Netze als Transportweg nutzt.

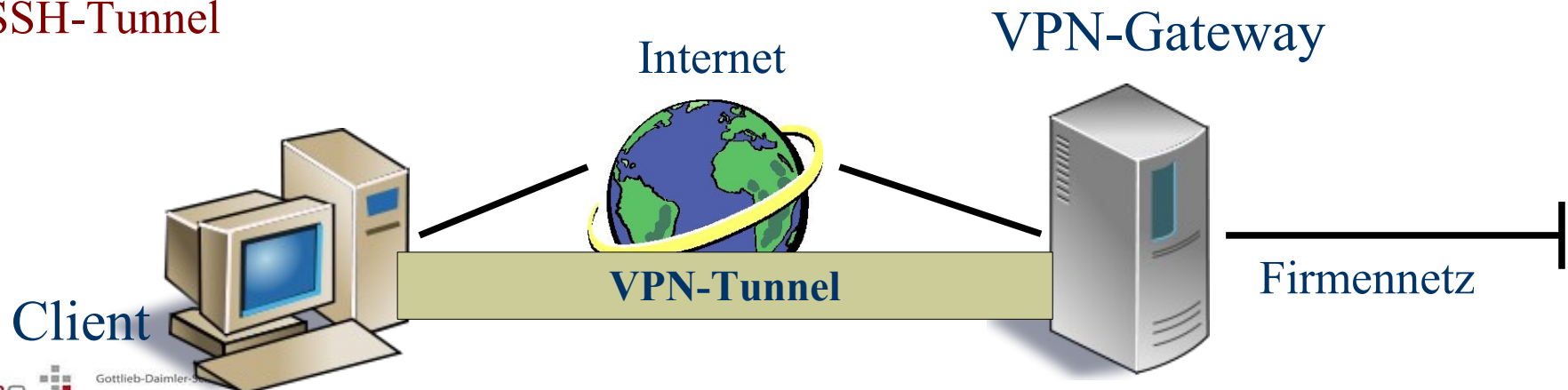
Varianten:

**PPTP**

**IPSec**

**SSL-VPN**

**SSH-Tunnel**



# VPN Typen

- ◆ End-to-Site-VPN (Host-to-Gateway-VPN / Remote-Access-VPN, Road Warrior)



- ◆ Site-to-Site-VPN (LAN-to-LAN-VPN / Gateway-to-Gateway-VPN / Branch-Office-VPN)



- ◆ End-to-End-VPN (Host-to-Host-VPN / Remote-Desktop-VPN)



# OpenVPN - Übersicht

♦ „Dass das freie VPN-Tool einen derart großen Funktionsumfang mit einer simplen Konfiguration bei gleichzeitig hoher Sicherheit kombiniert, scheint wie die Quadratur des Kreises“

( Linux-Magazin 05/09 )

## ♦ Implementierung eines SSL-basierten VPN

- Anwendungsneutralität
- „Sichere“ Netzwerkerweiterung bzgl. OSI Layer 2 und 3
- 2 Betriebsmodi: Routing (TUN) und Bridging(Tap)
- Arbeitet über die Transportprotokolle TCP und UDP

## ♦ Authentifizierung erfolgt auf Basis von:

- Benutzername/Passwort
- Zertifikatsbasiert
- (PreShared Keys)

# TUN/TAP???

Routing-Modus	Bridging-Modus
<ul style="list-style-type: none"><li>▶ TUN-Device</li><li>▶ eine Verbindung zwischen zwei Gegenstellen</li><li>▶ Um auf andere Geräte zuzugreifen, benötigt man Kenntnisse über Netzwerkrouting.</li><li>▶ weniger Netzwerktraffic</li><li>▶ nur IP-Protokoll</li><li>▶ arbeitet auf Schicht 3 im OSI-Modell</li></ul>	<ul style="list-style-type: none"><li>▶ TAP-Device</li><li>▶ eine Verbindung zwischen Netzwerken</li><li>▶ höherer Netzwerktraffic (auch Broadcast-Anfragen usw. werden übertragen)</li><li>▶ Auch andere Protokolle sind möglich.</li><li>▶ arbeitet auf Schicht 2 im OSI-Modell</li></ul>

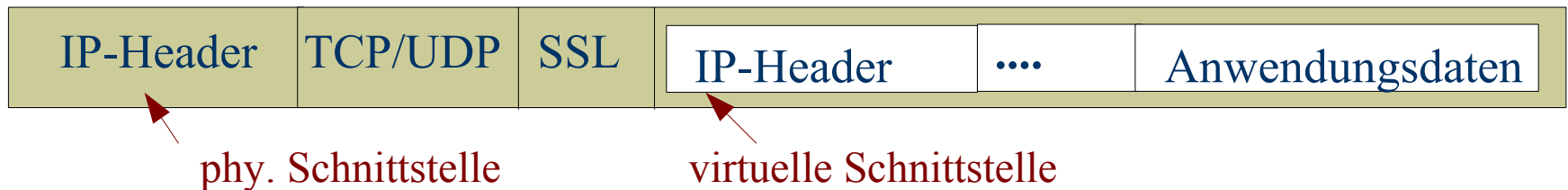
(Quelle: OpenVPN, Das Praxisbuch, Dirk Becker, Galileo Computing )

# OpenVPN installieren

- ◆ Installationspakete sind in der Regel in den Softwarerepositories der verschiedenen Linuxdistributionen vorhanden.
- ◆ Installation aus den Sourcedateien von [www.openvpn.net](http://www.openvpn.net)
- ◆ Unterstützung der virt. Netzwerkschnittstellen tun/tap in aktuellen Betriebssystemkernen bereits enthalten.
- ◆ Für Windows/Mac stehen ebenfalls entsprechende Programmpakete (inkl. OpenVPN-GUI) zur Verfügung. Diese beinhalten auch den benötigten win32tap-Treiber für die virtuelle Netzwerkschnittstelle.
- ◆ Hilfen zur Installation und Konfiguration:
  - <http://www.openvpn.net/index.php/open-source/documentation/howto.html>
  - <http://wiki.openvpn.eu>

# Virtuelle Netzwerkschnittstellen: Das Tunnelprinzip

- ◆ Ansatz von OpenVPN:
  - Nutzt die sogenannten virtuellen Netzwerkschnittstellen und
  - verknüpft diese mit einer Verschlüsselung im Userspace des OS.
  - virt. Schnittstellen bilden die Verknüpfung zwischen den über den Tunnel übertragenen Daten, dem OpenVPN-Prozess und dem OS.
- ◆ Protokollverschachtelung in Tunneln mit einem Trick:
  - IP-Paket als Payload eines IP-Pakets.
  - virtuelle Netzwerkschnittstellen sind Endpunkte des Tunnels.



# Der erste Tunnel End to END (unverschlüsselt)

Virtueller  
Netzwerkadapter

Virtuelle  
Verbindung  
Tunnel

phys. Verbindung

Physikalischer  
Netzwerkadapter  
Host 1

Host 2

```
openvpn --dev tun0 --remote 192.168.2.10 --ifconfig 10.10.10.2 10.10.10.1
```

```
C:\>openvpn --dev tun0 --remote 192.168.2.20 --ifconfig 10.10.10.1 10.10.10.2 --verb 3
```

```
Sat Oct 18 11:26:23 2014 ***** WARNING *****: all encryption and authentication features disabled -- all data will be tunneled as cleartext
Sat Oct 18 11:26:23 2014 Notified TAP-Windows driver to set a DHCP IP/netmask of 10.10.10.1/255.255.255.252 on interface
99D445BA> [DHCP-serv: 10.10.10.2, lease-time: 31536000]
Sat Oct 18 11:26:23 2014 Successful ARP Flush on interface [3] (6995F2B1-C758-42DD-A4D1-A9B399D445BA)
Sat Oct 18 11:26:23 2014 UDPv4 link local (bound): [undef]
Sat Oct 18 11:26:23 2014 UDPv4 link remote: [AF_INET]192.168.2.20:1194
Sat Oct 18 11:26:33 2014 Peer Connection Initiated with [AF_INET]192.168.2.20:1194
Sat Oct 18 11:26:39 2014 TEST ROUTES: 0/0 succeeded len=0 ret=1 a=0 u/d=up
Sat Oct 18 11:26:39 2014 Initialization Sequence Completed
```



# Workshop I

- ◆ Installation von OpenVPN auf Ihrem Laptop oder bereitgestellte VM (VM danach neu starten).
- ◆ Aufbau eines unverschlüsselten Tunnels aus der Kommandozeile heraus (Befehl – vergleiche letzte Folie) zu einem Partner.
- ◆ Test der VPN-Verbindung durch einen Ping zur Gegenseite (virtuelles Interface).
- ◆ **Analyse der zu den Pings gehörigen Netzwerkpakete mit Wireshark → IP-Paket im IP-Paket !!!**
- ◆ Überprüfen der zusätzlichen Einträge in der Routingtabelle der Rechner nach dem Aufbau der VPN-Verbindung.

# Mitschnitt ping

```
C:\Windows\system32>ping 10.10.10.2
```

```
Ping wird ausgeführt für 10.10.10.2 mit 32 Bytes Daten:  
Antwort von 10.10.10.2: Bytes=32 Zeit<1ms TTL=64
```

```
9 0.99861500 192.168.2.10 192.168.2.20 UDP 102 source port: 1194 destination port: 1194
```

```
+ Frame 9: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0  
+ Ethernet II, Src: VMware_7c:e0:e9 (00:0c:29:7c:e0:e9), Dst: VMware_13:0b:59 (00:0c:29:13:0b:59)  
+ Internet Protocol Version 4, Src: 192.168.2.10 (192.168.2.10), Dst: 192.168.2.20 (192.168.2.20)  
+ User Datagram Protocol, Src Port: 1194 (1194), Dst Port: 1194 (1194)  
+ Data (60 bytes)
```

```
0000 00 0c 29 13 0b 59 00 0c 29 7c e0 e9 08 00 45 00 ..).Y.. )|....E.  
0010 00 58 04 82 00 00 80 11 b0 a4 c0 a8 02 0a c0 a8 .X.....  
0020 02 14 04 aa 04 aa 00 44 70 a3 45 00 00 3c 04 81 .....D p.E.<..  
0030 00 00 80 01 0e 2a 0a 0a 0a 01 0a 0a 0a 02 08 00 .....*..  
0040 14 5c 03 00 36 00 61 62 63 64 65 66 67 68 69 6a .\..6.ab cdefghij  
0050 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 klmnopqr stuvwabc  
0060 64 65 66 67 68 69 defghi
```

## Oder mit Decode as IPv4

```
9 0.99861500 10.10.10.1 10.10.10.2 ICMP 102 Echo (ping) request
```

```
+ Frame 9: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0  
+ Ethernet II, Src: VMware_7c:e0:e9 (00:0c:29:7c:e0:e9), Dst: VMware_13:0b:59 (00:0c:29:13:0b:59)  
+ Internet Protocol Version 4, Src: 192.168.2.10 (192.168.2.10), Dst: 192.168.2.20 (192.168.2.20)  
+ User Datagram Protocol, Src Port: 1194 (1194), Dst Port: 1194 (1194)  
+ Internet Protocol Version 4, Src: 10.10.10.1 (10.10.10.1), Dst: 10.10.10.2 (10.10.10.2)  
+ Internet Control Message Protocol
```

# Mitschnitt FTP

No.	Time	Source	Destination	Protocol	Length	Info
8	22.4389010	192.168.2.10	192.168.2.20	UDP	82	Source port: 1194 Destination port: 1194
9	22.4407910	192.168.2.20	192.168.2.10	UDP	124	Source port: 1194 Destination port: 1194
10	22.4426380	192.168.2.10	192.168.2.20	UDP	98	Source port: 1194 Destination port: 1194
11	22.4434730	192.168.2.20	192.168.2.10	UDP	115	Source port: 1194 Destination port: 1194
12	22.4448530	192.168.2.10	192.168.2.20	UDP	103	Source port: 1194 Destination port: 1194
13	22.4466140	192.168.2.20	192.168.2.10	UDP	102	Source port: 1194 Destination port: 1194
14	22.4486070	192.168.2.10	192.168.2.20	UDP	88	Source port: 1194 Destination port: 1194
<div> <div>+</div> <div>Frame 9: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface 0</div> </div>						
<div> <div>+</div> <div>Ethernet II, Src: vmware_c0:38:94 (00:0c:29:c0:38:94), Dst: vmware_04:8f:cc (00:0c:29:04:8f:cc)</div> </div>						
<div> <div>+</div> <div>Internet Protocol Version 4, Src: 192.168.2.20 (192.168.2.20), Dst: 192.168.2.10 (192.168.2.10)</div> </div>						
<div> <div>+</div> <div>User Datagram Protocol, Src Port: 1194 (1194), Dst Port: 1194 (1194)</div> </div>						
<div> <div>+</div> <div>Data (82 bytes)</div> </div>						

## Mit Decode as IPv4

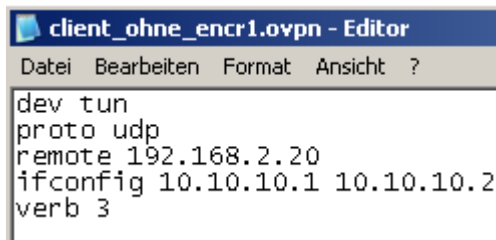
No.	Time	Source	Destination	Protocol	Length	Info
9	22.4407910	10.10.10.2	10.10.10.1	FTP	124	Response: 220 3Com 3Cdaemon FTP Server Version 2.0
10	22.4426380	10.10.10.1	10.10.10.2	FTP	98	Request: USER anonymous
11	22.4434730	10.10.10.2	10.10.10.1	FTP	115	Response: 331 User name ok, need password
12	22.4448530	10.10.10.1	10.10.10.2	FTP	103	Request: PASS anon@localhost
13	22.4466140	10.10.10.2	10.10.10.1	FTP	102	Response: 230 User logged in
14	22.4486070	10.10.10.1	10.10.10.2	FTP	88	Request: SYST
<div> <div>+</div> <div>Frame 9: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface 0</div> </div>						
<div> <div>+</div> <div>Ethernet II, Src: vmware_c0:38:94 (00:0c:29:c0:38:94), Dst: vmware_04:8f:cc (00:0c:29:04:8f:cc)</div> </div>						
<div> <div>+</div> <div>Internet Protocol Version 4, Src: 192.168.2.20 (192.168.2.20), Dst: 192.168.2.10 (192.168.2.10)</div> </div>						
<div> <div>+</div> <div>User Datagram Protocol, Src Port: 1194 (1194), Dst Port: 1194 (1194)</div> </div>						
<div> <div>+</div> <div>Internet Protocol Version 4, Src: 10.10.10.2 (10.10.10.2), Dst: 10.10.10.1 (10.10.10.1)</div> </div>						
<div> <div>+</div> <div>Transmission Control Protocol, Src Port: 21 (21), Dst Port: 1438 (1438), Seq: 1, Ack: 1, Len: 42</div> </div>						
<div> <div>+</div> <div>File Transfer Protocol (FTP)</div> </div>						

# Mit OpenVPN GUI

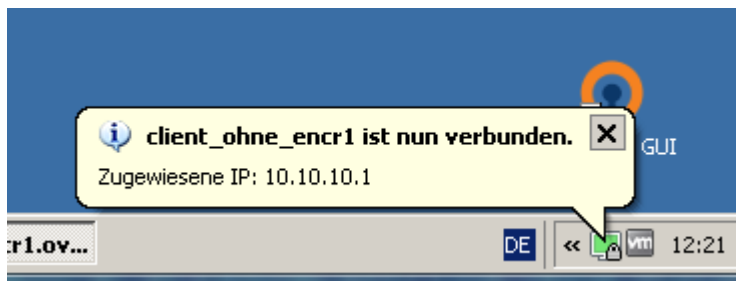
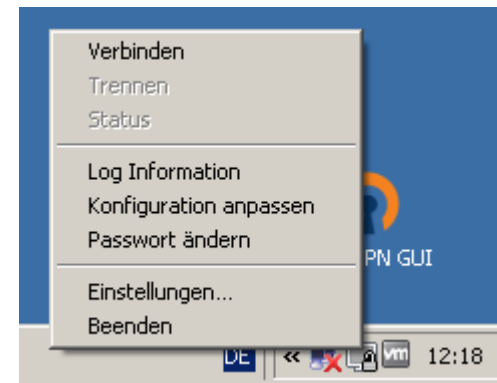
- ◆ Statt Kommandozeile kann man auch mit den .ovpn Dateien im Verzeichnis

C:\Program Files\OpenVPN\config (32-bit Windows)

C:\Program Files (x86)\OpenVPN\config (64-bit Windows)  
arbeiten.

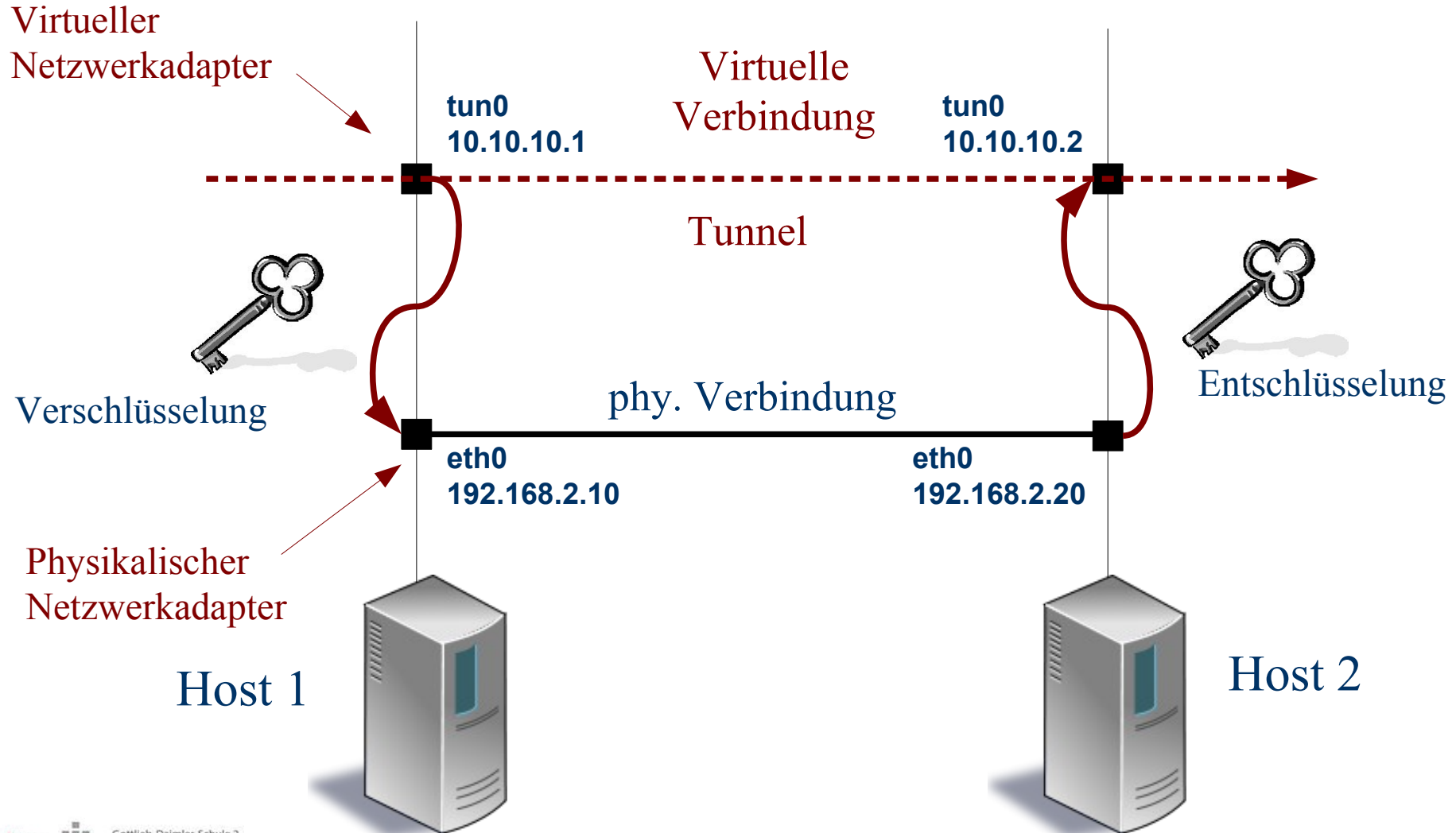


```
client_ohne_encr1.ovpn - Editor
Datei Bearbeiten Format Ansicht ?
dev tun
proto udp
remote 192.168.2.20
ifconfig 10.10.10.1 10.10.10.2
verb 3
```



Workshop II  
Mit OpenVPN GUI  
verbinden

# Funktionsweise mit Verschlüsselung



# PreShared Key - Authentifizierung und Verschlüsselung des Datentransports

- ◆ Verwenden einer symmetrische Verschlüsselung!
- ◆ Erzeugen eines gemeinsamen Schlüssels:  
`openvpn --genkey --secret static.key`
- ◆ „Sicherer“ Austausch dieses Schlüssels!?!
- ◆ Vorteil - Sehr einfache Einrichtung!

Konfigurationsdateien<sup>1)</sup> (Textdatei) im Verzeichnis *config*:

host1.ovpn:

```
dev tun
remote 192.168.2.20
ifconfig 10.10.10.1 10.10.10.2
secret static.key
```

host2.ovpn:

```
dev tun
remote 192.168.2.10
ifconfig 10.10.10.2 10.10.10.1
secret static.key
```

1) Aus dem Unterverzeichnis *samples* kann auch eine Beispieldatei kopiert und angepasst werden.

# Workshop III

- ◆ Erzeugung eines gemeinsamen Secret-Key
- ◆ Konfigurationsdateien auf dem jeweiligen Host erzeugen
- ◆ Start der VPN-Verbindung aus der GUI heraus
- ◆ Verschlüsselter Datentransport mit Wireshark überprüfen
- ◆ FTP Anmeldung mit Wireshark auf der physik. und virtuellen Netzkarte aufzeichnen
- ◆ Optional: Installation eines Webservers (Apache) auf einem Host. Den Webserver so konfigurieren, dass er **nur Verbindungsanfragen am virtuellen Tunnelinterface annimmt.** Webserver vom zweiten Host „durch den Tunnel“ kontaktieren.

# Wireshark Mitschnitt ping

6	0.00043800	192.168.2.10	192.168.2.20	UDP	142	Source port: 1194	Destination port: 1194
Frame 6: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0							
Ethernet II, Src: vmware_7c:e0:e9 (00:0c:29:7c:e0:e9), Dst: vmware_13:0b:59 (00:0c:29:13:0b:59)							
Internet Protocol Version 4, Src: 192.168.2.10 (192.168.2.10), Dst: 192.168.2.20 (192.168.2.20)							
User Datagram Protocol, Src Port: 1194 (1194), Dst Port: 1194 (1194)							
Data (100 bytes)							
Data: 711adc0a9a8137470a55faf9a44f26c0ebc0760c1d59b081...							
[Length: 100]							
0000	00 0c 29 13 0b 59 00 0c	29 7c e0 e9 08 00 45 00	..Y.. } ....E.				
0010	00 80 07 a8 00 00 80 11	ad 56 c0 a8 02 0a c0 a8	.....V.....				
0020	02 14 04 aa 04 aa 00 6c	a8 df 71 1a dc 0a 9a 81	.....l..q.....				
0030	37 47 0a 55 fa f9 a4 4f	26 c0 eb c0 76 0c 1d 59	7G.U...O &...v..Y				
0040	b0 81 23 fe e6 d1 9b 78	75 1b 0c 15 0c 79 8f e8	..#....x u...y..				
0050	2c f1 b8 dd cb 3a ff d7	6e 1f 91 98 4a c2 fa 13	,....:.. n...J...				
0060	9d 68 6e 9a 78 05 06 df	e0 95 f9 8c c7 06 9a e5	.hn.x... ..				
0070	99 46 48 0a eb 1c e2 a6	41 52 c1 f5 52 c9 00 c5	.FH.... AR..R...				
0080	4a b7 32 5d f7 b1 68 9b	02 2d 3f d1 02 f2	]2]..h. .-?...				



# Wireshark FTP Anmeldung auf beiden Karten mitgeschnitten

60	11.3240540	10.10.10.1	10.10.10.2	FTP	70 Request: USER anonymous
61	11.3283760	10.10.10.2	10.10.10.1	FTP	87 Response: 331 User name ok, need password
62	11.3288750	10.10.10.1	10.10.10.2	FTP	75 Request: PASS anon@localhost
63	11.3311200	10.10.10.2	10.10.10.1	FTP	74 Response: 230 User logged in
64	11.3312790	10.10.10.1	10.10.10.2	FTP	60 Request: SYST
65	11.3344490	10.10.10.2	10.10.10.1	FTP	73 Response: 215 UNIX Type: L8
66	11.3349860	10.10.10.1	10.10.10.2	FTP	60 Request: FEAT
67	11.3399000	10.10.10.2	10.10.10.1	FTP	76 Response: 211- Feature listing
68	11.5373820	10.10.10.1	10.10.10.2	TCP	54 1059+21 [ACK] Seq=50 Ack=137 Win=64104 Len=0
69	11.5404270	10.10.10.2	10.10.10.1	FTP	88 Response: MDTM
70	11.5539030	10.10.10.1	10.10.10.2	FTP	59 Request: PWD
71	11.5590730	10.10.10.2	10.10.10.1	FTP	84 Response: 257 "/" is current directory
72	11.5744610	10.10.10.1	10.10.10.2	FTP	62 Request: TYPE I
73	11.5809250	192.168.2.10	192.168.2.20	UDP	134 Source port: 1194 Destination port: 1194
74	11.5822520	192.168.2.20	192.168.2.10	UDP	142 Source port: 1194 Destination port: 1194
75	11.5856750	192.168.2.10	192.168.2.20	UDP	126 Source port: 1194 Destination port: 1194
76	11.5900250	192.168.2.20	192.168.2.10	UDP	166 Source port: 1194 Destination port: 1194
77	11.5951710	192.168.2.10	192.168.2.20	UDP	126 Source port: 1194 Destination port: 1194
78	11.5993520	192.168.2.10	192.168.2.20	UDP	134 Source port: 1194 Destination port: 1194

- ⊞ Frame 75: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0
- ⊞ Ethernet II, Src: Vmware\_04:8f:cc (00:0c:29:04:8f:cc), Dst: Vmware\_c0:38:94 (00:0c:29:c0:38:94)
- ⊞ Internet Protocol Version 4, Src: 192.168.2.10 (192.168.2.10), Dst: 192.168.2.20 (192.168.2.20)
- ⊞ User Datagram Protocol, Src Port: 1194 (1194), Dst Port: 1194 (1194)

## ⊞ Data (84 bytes)

Data: a5876b21e939668edf7464cd117b74896e1e0909f850eb3a...

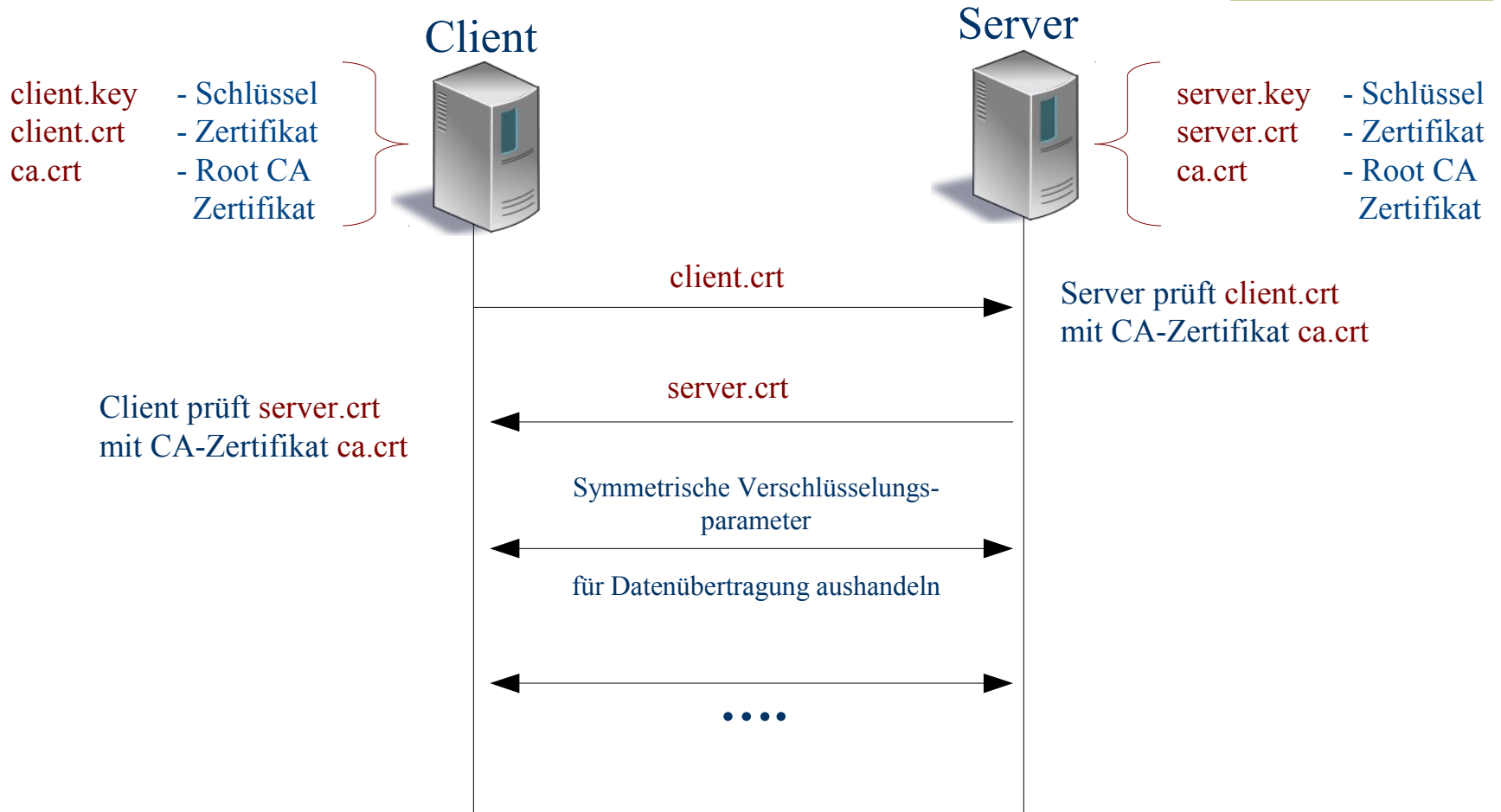
[Length: 84]

Warum sieht man trotz Verschlüsselung noch Namen und Passwort

# Schlüsselaustausch mit Transport Layer Security

- ◆ Zertifikatsbasierte Authentifizierung über TLS-Protokoll.
- ◆ SSL ursprünglich von Netscape beschriebenes Protokoll:
  - Ziel: Absicherung von HTTP-Verbindungen
  - Versionen SSLv1, SSLv2 bis SSLv3
- ◆ SSL setzt auf ein Transportprotokoll auf (TCP/UDP).
- ◆ SSL wegen vieler Schwachstellen nicht mehr zu empfehlen
- ◆ TLS (RFC 2246) basiert auf SSLv3:
  - TLS bietet Fallback auf SSLv3 (Kom. zw. TLS-Hosts und SSL-Clients).
  - Authentifizierung bei TLS gegenüber SSL mit Zertifikaten Pflicht.

# Verbindungsaufbau



# Zertifikatserstellung

- ◆ Aufbau einer PKI
- ◆ OpenVPN bietet mit EasyRSA bereits vorgefertigte Skripte zur Erstellung der CA, Server- und Clientzertifikate (OpenSSL-Paket muß hierfür installiert sein) Vorgehensweise unter:
  - <http://www.openvpn.net/index.php/open-source/documentation/howto.html#pki>
  - <http://wiki.openvpn.eu> → Erzeugen einer PKI mit EasyRSA
  - VPN Motta Osemann
- ◆ CA- und Zertifikatserstellung (PKI-Verwaltung) direkt mit OpenSSL, oder entsprechenden grafischen Frontends wie z.B. XCA, Mobilefish.
- ◆ Eigene Zertifikatsverwaltung in den div. Distributionen, in den OpenVPN enthalten ist (Zeroshell, IPFire, PfSense etc.)

# Schlüssel und Zertifikate

## #Benötigte Zertifikate der CA und des Servers selbst

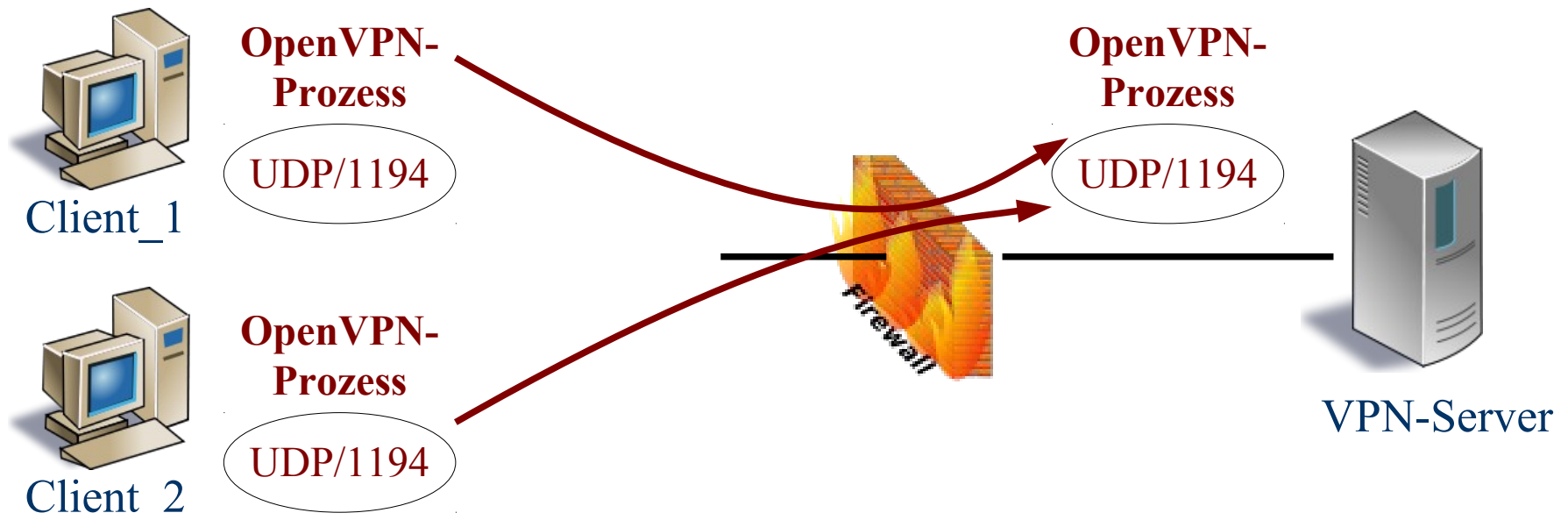
```
ca      /etc/openvpn/keys/ca.crt
cert    /etc/openvpn/keys/server.crt
key     /etc/openvpn/keys/server.key
dh      /etc/openvpn/keys/dh1024.pem
```

## #Benötigte Zertifikate der CA und des Clients

```
ca      /etc/openvpn/keys/ca.crt
cert    /etc/openvpn/keys/client.crt
key     /etc/openvpn/keys/client.key
```

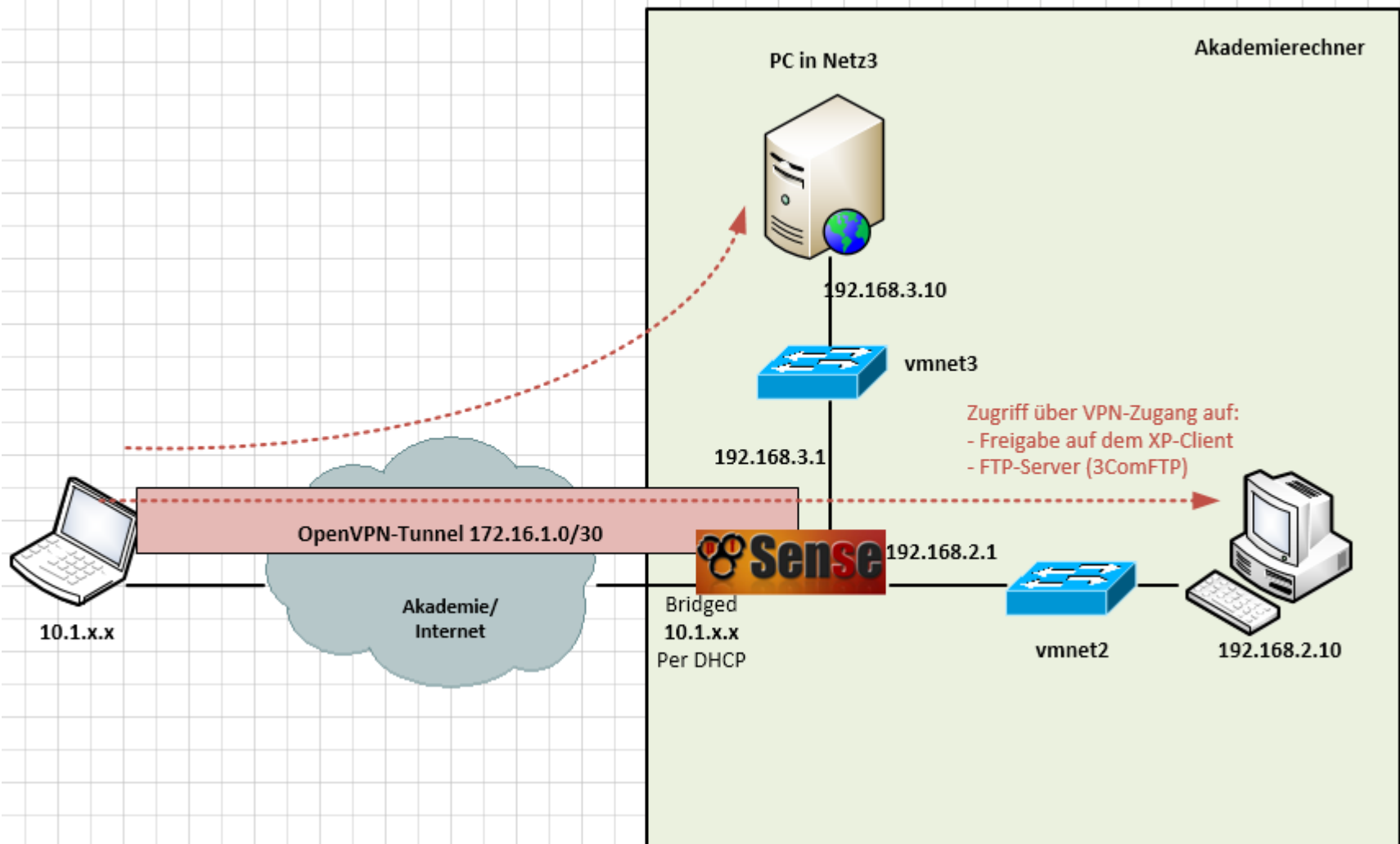
So sieht es z.B. nach der Erstellung mit easy-rsa aus

# Betriebsmodi: Server Mode




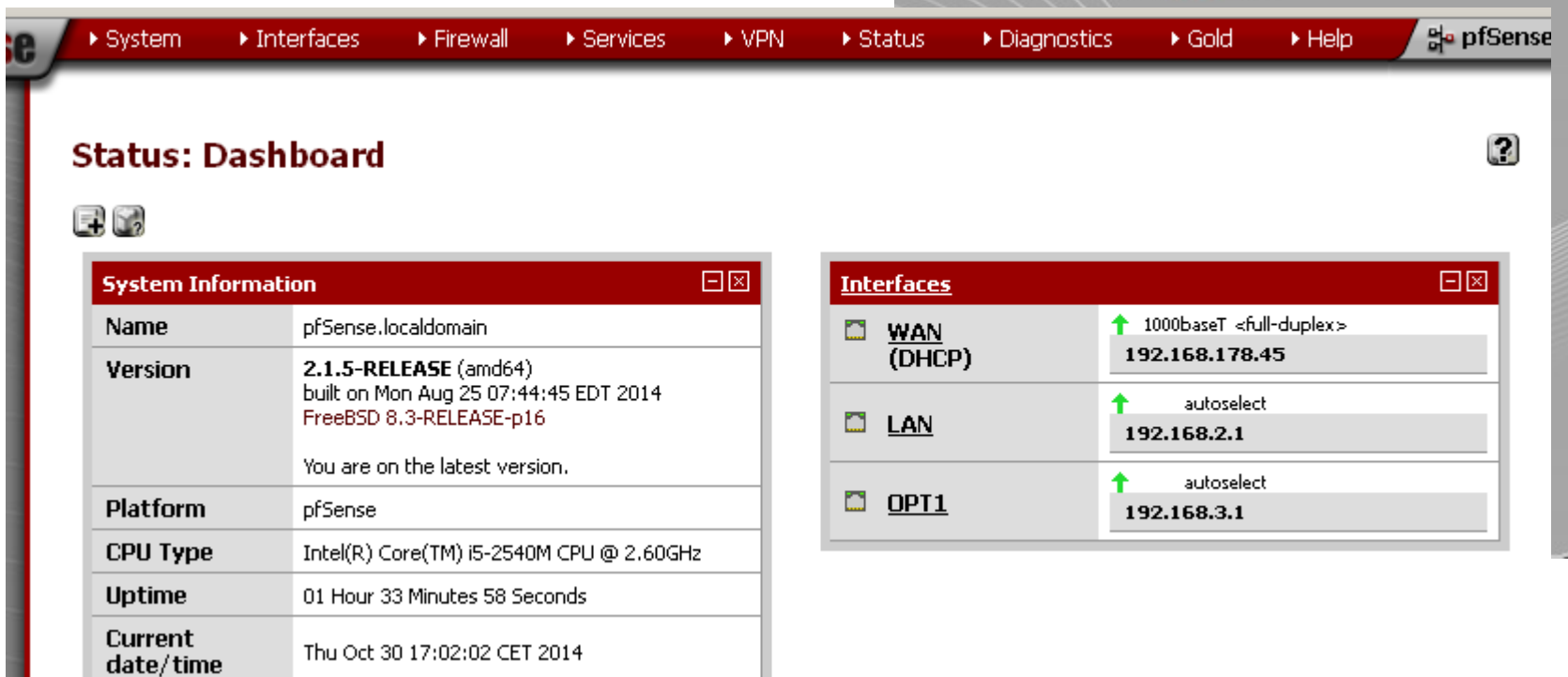
- Ansatz für Remote-Access-Verbindungen
- Ein Prozess auf dem Server verwaltet alle VPN-Verbindungen
- Point-to-Multipoint Modus

# Beispielnetz – OpenVPN mit pfSense



# Anmeldung pfSense

- ♦ Mit PC aus vmnet2 und <https://192.168.2.1>
- ♦ Falls selbst installiert admin und Passwort pfsense
- ♦ Fertige VM hat Passwort 12345

The screenshot shows the pfSense web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled "Status: Dashboard" and contains two expandable panels. The "System Information" panel displays details about the pfSense instance, including its name, version (2.1.5-RELEASE), platform, CPU type, uptime, and current date/time. The "Interfaces" panel shows the configuration for three network interfaces: WAN (DHCP), LAN, and OPT1, each with its assigned IP address and status.

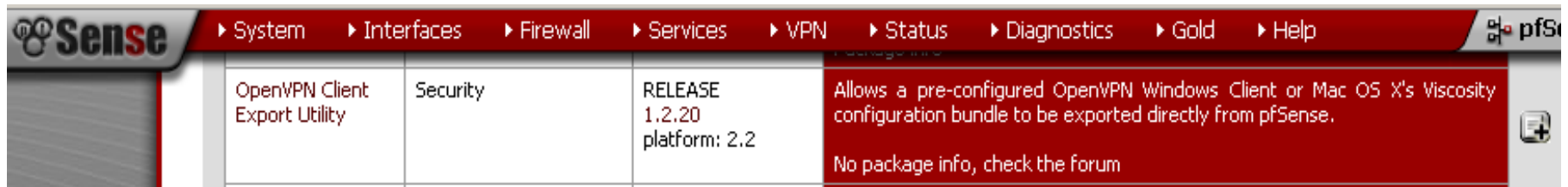
System Information	
Name	pfSense.localdomain
Version	2.1.5-RELEASE (amd64) built on Mon Aug 25 07:44:45 EDT 2014 FreeBSD 8.3-RELEASE-p16  You are on the latest version.
Platform	pfSense
CPU Type	Intel(R) Core(TM) i5-2540M CPU @ 2.60GHz
Uptime	01 Hour 33 Minutes 58 Seconds
Current date/time	Thu Oct 30 17:02:02 CET 2014

Interfaces	
WAN (DHCP)	↑ 1000baseT <full-duplex> 192.168.178.45
LAN	↑ autoselect 192.168.2.1
OPT1	↑ autoselect 192.168.3.1



# Zusatzpaket installieren

- ◆ Unter System – Packages – Available Packages
- ◆ Open VPN Client Export Utility auswählen und mit Confirm installieren



- ◆ Paket wird zum Herunterladen der Schlüssel und Zertifikate benötigt

# CA erzeugen

## ◆ VPN – OpenVPN - Wizards

**OpenVPN Remote Access Server Setup Wizard**

**Select an Authentication Backend Type**

Type of Server:  NOTE: If you are unsure, leave this set to "Local User Access."

**Create a New Certificate Authority (CA) Certificate**

<b>Descriptive name:</b>	<input type="text" value="CA_GDS2"/> <small>A name for your reference, to identify this certificate. This is the same as common-name field for other Certificates.</small>
<b>Key length:</b>	<input type="text" value="2048 bit"/> <small>Size of the key which will be generated. The larger the key, the more security it offers, but larger keys are generally slower to use.</small>
<b>Lifetime:</b>	<input type="text" value="3650"/> <small>Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)</small>
<b>Country Code:</b>	<input type="text" value="DE"/> <small>Two-letter ISO country code (e.g. US, AU, CA)</small>
<b>State or Province:</b>	<input type="text" value="BadenW"/> <small>Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).</small>
<b>City:</b>	<input type="text" value="Sindelfingen"/> <small>City or other Locality name (e.g. Louisville, Indianapolis, Toronto).</small>
<b>Organization:</b>	<input type="text" value="GDS2"/> <small>Organization name, often the Company or Group name.</small>
<b>E-mail:</b>	<input type="text" value="admin@gds2.de"/> <small>E-mail address for the Certificate contact. Often the e-mail of the person generating the certificate (i.e. You.)</small>

# Server Zertifikat erzeugen



## OpenVPN Remote Access Server Setup Wizard

### Create a New Server Certificate

<b>Descriptive name:</b>	<input type="text" value="VPNServer"/> A name for your reference, to identify this certificate. This is also known as the certificate's "Common Name."
<b>Key length:</b>	<input type="text" value="2048 bits"/> Size of the key which will be generated. The larger the key, the more security is offers, but larger keys are generally slower to use.
<b>Lifetime:</b>	<input type="text" value="3650"/> Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)
<b>Country Code:</b>	<input type="text" value="DE"/> Two-letter ISO country code (e.g. US, AU, CA)
<b>State or Province:</b>	<input type="text" value="BadenW"/> Full State of Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).
<b>City:</b>	<input type="text" value="Sindelfingen"/> City or other Locality name (e.g. Louisville, Indianapolis, Toronto).
<b>Organization:</b>	<input type="text" value="GDS2"/> Organization name, often the Company or Group name.
<b>E-mail:</b>	<input type="text" value="admin@gds2.de"/> admin@gds2.de the e-mail of the person generating the certificate (i.e. You.)

Create new Certificate




## General OpenVPN Server Information

<b>Interface:</b>	<div>WAN ▾</div> <p>The interface where OpenVPN will listen for incoming connections (typically WAN.)</p>
<b>Protocol:</b>	<div>UDP ▾</div> <p>Protocol to use for OpenVPN connections. If you are unsure, leave this set to UDP.</p>
<b>Local Port:</b>	<div> 1194</div> <p>Local port upon which OpenVPN will listen for connections. The default port is 1194. Leave this blank unless you need to use a different port.</p>
<b>Description:</b>	<div> VPN Zugang Mitarbeiter</div> <p>A name for this OpenVPN instance, for your reference. It can be set however you like, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff").</p>

## Cryptographic Settings

<b>TLS Authentication:</b>	<input checked="" type="checkbox"/> Enable authentication of TLS packets.
<b>Generate TLS Key:</b>	<input checked="" type="checkbox"/> Automatically generate a shared TLS authentication key.
<b>TLS Shared Key:</b>	<div></div> <p>Paste in a shared TLS key if one has already been generated.</p>
<b>DH Parameters Length:</b>	<div>2048 bit ▾</div> <p>Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. As with other such settings, the larger values are more secure, but may be slower in operation.</p>
<b>Encryption Algorithm:</b>	<div>AES-256-CBC (256-bit) ▾</div> <p>The method used to encrypt traffic between endpoints. This setting must match on the client and server side, but is otherwise set however you like. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips.</p>
<b>Hardware Crypto:</b>	<div>No Hardware Crypto Acceleration ▾</div> <p>The hardware cryptographic accelerator to use for this VPN connection, if any.</p>

## Tunnel Settings

<b>Tunnel Network:</b>	 172.16.1.0/24 This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients. (see Address Pool)
<b>Redirect Gateway:</b>	<input type="checkbox"/> Force all client generated traffic through the tunnel.
<b>Local Network:</b>	 192.168.2.0/24 This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. You may leave this blank if you don't want to add a route to the local network through this tunnel on the remote machine. This is generally set to your LAN network.
<b>Concurrent Connections:</b>	 10 Specify the maximum number of clients allowed to concurrently connect to this server.
<b>Compression:</b>	No Preference Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.
<b>Type-of-Service:</b>	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
<b>Inter-Client Communication:</b>	<input checked="" type="checkbox"/> Allow communication between clients connected to this server.
<b>Duplicate Connections:</b>	<input type="checkbox"/> Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.

## Client Settings

# Alles übernehmen

Windows shares. This is typically an Active Directory Domain Controller, designated WINS server, or Samba server.

Advanced:

```
push "route 192.168.2.0 255.255.255.0"
Enter any additional options you would like to add to the OpenVPN server configuration here, separated by a semicolon. (EXAMPLE: push "route 10.0.0.0 255.255.255.0")
```

# Fertig (CA , Server Zertifikate und Konfiguration erstellt)

## OpenVPN Remote Access Server Setup Wizard

### Firewall Rule Configuration

Firewall Rules control what network traffic is permitted. You must add rules to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

### Traffic from clients to server

Firewall Rule:

☒ Add a rule to permit traffic from clients on the Internet to the OpenVPN server process.

### Traffic from clients through VPN

## OpenVPN Remote Access Server Setup Wizard

### Configuration Complete!

Your configuration is now complete.

To be able to export client configurations, browse to System->Packages and install the OpenVPN Client Export package.

Finish

# Benutzer hinzufügen



System Interfaces Firewall Services VPN Status Diagnostics Gold Help

## System: User Manager

Users

Groups

Settings

Servers

Username

admin

System

Defined by	USER	
Disabled	<input type="checkbox"/>	
Username	<input type="text" value="kraut"/>	
Password	<input type="password" value="....."/>	
	<input type="password" value="....."/> (confirmation)	
Full name	<input type="text" value="Peter Kraut"/> User's full name, for your own information only	
Expiration date	<input type="text" value="10/25/2024"/> Leave blank if the account shouldn't expire, otherwise enter the expiration date in the following format: mm/dd/yyyy	
Group Memberships	<div><div>Not Member Of</div><div>Member Of</div></div>	
	<div><div><input type="text" value="admins"/></div><div> </div><div><input type="text"/></div></div>	
	Hold down CTRL (pc)/COMMAND (mac) key to select multiple items	
Certificate	<div><div>Descriptive name</div><div>Certificate authority</div><div>Key length</div><div>Lifetime</div></div> <div><div><input type="text" value="VPNCert Kraut"/></div><div><input type="text" value="CA_GDS2"/></div><div><input type="text" value="2048"/> bits</div><div><input type="text" value="3650"/> days</div></div>	
Authorized keys	<input type="checkbox"/> Click to paste an authorized key.	
IPsec Pre-Shared Key	<input type="text"/>	
<input type="button" value="Save"/>		

# Client Dateien Downloaden



## OpenVPN: Client Export Utility

Server Client Client Specific Overrides Wizards Client Export Shared Key Export

Remote Access Server

VPN Zugang Mitarbeiter UDP:1194

### Client Install Packages

User	Certificate Name	Export
kraut	VPNCert Kraut	<ul style="list-style-type: none"><li>- Standard Configurations:<ul style="list-style-type: none"><li>Archive Config Only</li></ul></li><li>- Inline Configurations:<ul style="list-style-type: none"><li>Android OpenVPN Connect (iOS/Android) Others</li></ul></li><li>- Windows Installers:<ul style="list-style-type: none"><li>2.3-x86 2.3-x64</li></ul></li><li>- Mac OSX:<ul style="list-style-type: none"><li>Viscosity Bundle</li></ul></li></ul>

NOTE: If you expect to see a certain client in the list but it is not there, it is usually due to a CA mismatch between the OpenVPN server instance and the client certificates found in the User Manager.

### Links to OpenVPN clients for various platforms:

[OpenVPN Community Client](#) - Binaries for Windows, Source for other platforms. Packaged above in the Windows Installers  
[OpenVPN For Android](#) - Recommended client for Android  
[FEAT VPN For Android](#) - For older versions of Android  
[OpenVPN Connect: Android \(Google Play\) or iOS \(App Store\)](#) - Recommended client for iOS  
[Viscosity](#) - Recommended client for Mac OSX  
[Tunnelblick](#) - Free client for OSX



# Und verbinden

Unter Interfaces WAN in Testumgebung Haken raus!!!

## Private networks

### ☒ Block private networks

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option unchecked, too.

## OpenVPN Verbindung (pfSense-udp-1194-kraut)

Aktueller Status: Verbinden

```
Thu Oct 30 17:49:37 2014 OpenVPN 2.3.4 i686-w64-mingw32 [SSL (OpenSSL)] [LZO] [PKCS11] [IPv6] built on
Thu Oct 30 17:49:37 2014 library versions: OpenSSL 1.0.1i 6 Aug 2014, LZO 2.05
Thu Oct 30 17:49:54 2014 Control Channel Authentication: using 'pfSense-udp-1194-kraut-tls.key' as a OpenV
Thu Oct 30 17:49:54 2014 UDPv4 link local (bound): [undef]
Thu Oct 30 17:49:54 2014 UDPv4 link remote: [AF_INET]192.168.178.45:1194
Thu Oct 30 17:49:54 2014 WARNING: this configuration may cache passwords in memory -- use the auth-noca
Thu Oct 30 17:49:54 2014 [VPNServer] Peer Connection Initiated with [AF_INET]192.168.178.45:1194
Thu Oct 30 17:49:57 2014 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Thu Oct 30 17:49:57 2014 open_tun, tt->ipv6=0
Thu Oct 30 17:49:57 2014 TAP-WIN32 device [LAN-Verbindung 2] opened: \\.\Global\{F8892F95-5EE0-4839
Thu Oct 30 17:49:57 2014 Notified TAP-Windows driver to set a DHCP IP/netmask of 172.16.1.6/255.255.255
Thu Oct 30 17:49:57 2014 Successful ARP Flush on interface [3] {F8892F95-5EE0-4839-8A58-ECE082812B17
```

Trennen

Neu Verbinden

Minimieren

pfSense-udp-1194-kraut ist nun verbunden.

Zugewiesene IP: 172.16.1.6

DE

<<

1

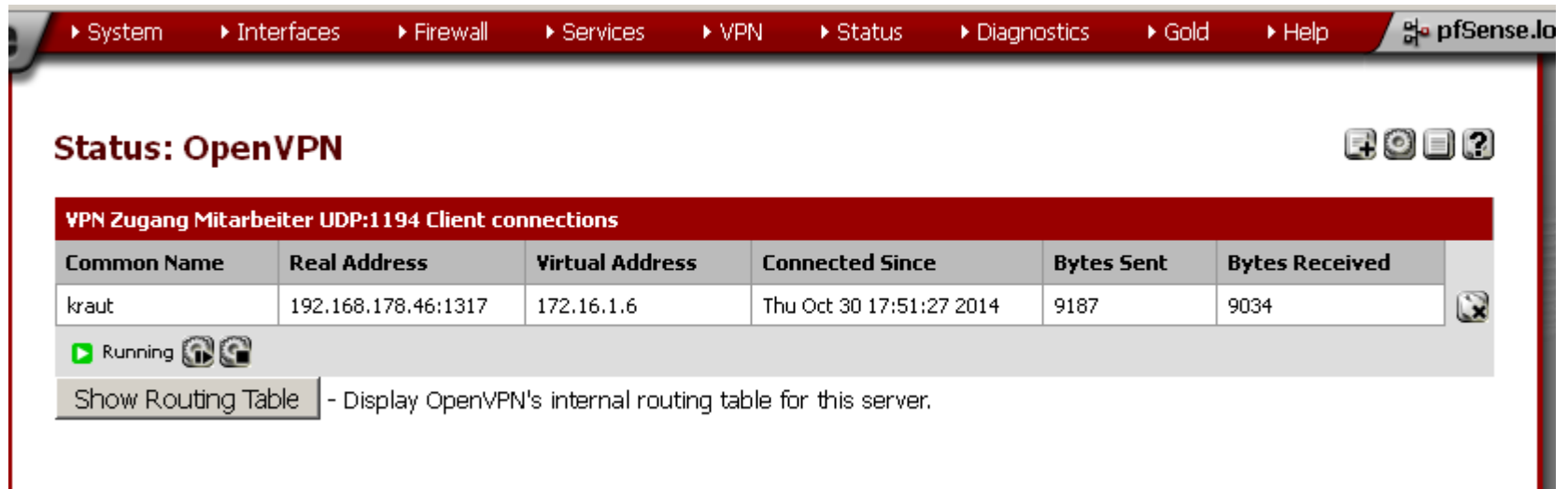
DE

<<

17:49

PN Verbindung ...

# Status OpenVPN



The screenshot shows the pfSense web interface with the 'Status' tab selected. The main heading is 'Status: OpenVPN'. Below it, a table titled 'VPN Zugang Mitarbeiter UDP:1194 Client connections' displays one active client named 'kraut'. The table columns are 'Common Name', 'Real Address', 'Virtual Address', 'Connected Since', 'Bytes Sent', and 'Bytes Received'. Below the table, a status bar indicates 'Running' with a green play button icon. A 'Show Routing Table' button is present, with a tooltip explaining its function: '- Display OpenVPN's internal routing table for this server.'

System Interfaces Firewall Services VPN Status Diagnostics Gold Help pfSense.io

## Status: OpenVPN

VPN Zugang Mitarbeiter UDP:1194 Client connections

Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received
kraut	192.168.178.46:1317	172.16.1.6	Thu Oct 30 17:51:27 2014	9187	9034

Running

Show Routing Table - Display OpenVPN's internal routing table for this server.

# Workshop IV

- ◆ OpenVPN in pfSense aktivieren und einrichten
  - Siehe Vorherige Folien
- ◆ Übertragen des Client-Pakets (Archive) oder eines der Installationspakete auf einen Testrechner oder Smartphone, Tablet
- ◆ VPN-Verbindung zum pfsense aufbauen.
  - Routingtabelle: Zus. Eintrag für „interne“ LAN (vmnet2) kontrollieren.
- ◆ Zugriff auf den „internen“ Web-/FTP-Server od. SMB-Freigabe.
- ◆ Kopplung zweier LANs über einen Net-to-Net-Zugang.

# Mit und ohne redirect

Redirect Gateway

☐ Force all client generated traffic through the tunnel.

IP-Adresse? - Mozilla Firefox

Ansicht Chronik Lesezeichen Extras Hilfe

Adresse? +

www.wieistmeineip.de

WIE IST MEINE IP.DE

Ihre IP-Adresse lautet: **144.41.232.228**

Ihre IPv6-Adresse lautet: NICHT VORHANDEN

System-Informationen: Windows XP Firefox 13.0.1 Deutschland

C:\Dokumente und Einstellungen\cisco>ipconfig

Windows-IP-Konfiguration

Ethernetadapter LAN-Verbindung:

Verbindungsspezifisches DNS-Suffix: fritz.box  
IP-Adresse. . . . . : 192.168.178.47  
Subnetzmaske. . . . . : 255.255.255.0  
Standardgateway. . . . . : 192.168.178.1

Ethernetadapter LAN-Verbindung 2:

Verbindungsspezifisches DNS-Suffix:  
IP-Adresse. . . . . : 172.16.21.6  
Subnetzmaske. . . . . : 255.255.255.252  
Standardgateway. . . . . : 172.16.21.5

C:\Dokumente und Einstellungen\cisco>route print

=====

Schnittstellenliste

0x1 ..... MS TCP Loopback interface  
0x2 ...00 0c 29 87 c2 df ..... Ethernetadapter der AMD-PCNET-Familie - Paketplaner-Miniport  
0x10004 ...00 ff 77 d7 98 26 ..... TAP-Windows Adapter U9 - Paketplaner-Miniport

=====

Aktive Routen:

Netzwerkziel	Netzwerkmaske	Gateway	Schnittstelle	Anzahl
0.0.0.0	0.0.0.0	172.16.21.5	172.16.21.6	1
0.0.0.0	0.0.0.0	192.168.178.1	192.168.178.47	1
10.1.0.0	255.255.0.0	172.16.21.5	172.16.21.6	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
128.0.0.0	128.0.0.0	172.16.21.5	172.16.21.6	1
144.41.232.228	255.255.255.255	192.168.178.1	192.168.178.47	1
172.16.21.1	255.255.255.255	172.16.21.5	172.16.21.6	1
172.16.21.4	255.255.255.252	172.16.21.6	172.16.21.6	30
172.16.21.6	255.255.255.255	127.0.0.1	127.0.0.1	30
172.16.255.255	255.255.255.255	172.16.21.6	172.16.21.6	30
192.168.178.0	255.255.255.0	192.168.178.47	192.168.178.47	10
192.168.178.47	255.255.255.255	127.0.0.1	127.0.0.1	10
192.168.178.255	255.255.255.255	192.168.178.47	192.168.178.47	10
224.0.0.0	240.0.0.0	172.16.21.6	172.16.21.6	30
224.0.0.0	240.0.0.0	192.168.178.47	192.168.178.47	10
255.255.255.255	255.255.255.255	172.16.21.6	172.16.21.6	1
255.255.255.255	255.255.255.255	192.168.178.47	192.168.178.47	1

Standardgateway: 172.16.21.5

Ständige Routen:

Wie ist meine IP-Adresse? - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

Wie ist meine IP-Adresse? +

www.wieistmeineip.de

WIE IST MEINE IP.DE

Ihre IP-Adresse lautet: **79.224.253.76**

Ihre IPv6-Adresse lautet: NICHT VORHANDEN

System-Informationen: Windows XP Firefox 13.0.1 Deutschland

C:\Dokumente und Einstellungen\cisco>ipconfig

Windows-IP-Konfiguration

Ethernetadapter LAN-Verbindung:

Verbindungsspezifisches DNS-Suffix: fritz.box  
IP-Adresse. . . . . : 192.168.178.47  
Subnetzmaske. . . . . : 255.255.255.0  
Standardgateway. . . . . : 192.168.178.1

Ethernetadapter LAN-Verbindung 2:

Verbindungsspezifisches DNS-Suffix:  
IP-Adresse. . . . . : 172.16.21.6  
Subnetzmaske. . . . . : 255.255.255.252  
Standardgateway. . . . . :

C:\Dokumente und Einstellungen\cisco>route print

=====

Schnittstellenliste

0x1 ..... MS TCP Loopback interface  
0x2 ...00 0c 29 87 c2 df ..... Ethernetadapter der AMD-PCNET-Familie - Paketplaner-Miniport  
0x10004 ...00 ff 77 d7 98 26 ..... TAP-Windows Adapter U9 - Paketplaner-Miniport

=====

Aktive Routen:

Netzwerkziel	Netzwerkmaske	Gateway	Schnittstelle	Anzahl
0.0.0.0	0.0.0.0	192.168.178.1	192.168.178.47	10
10.1.0.0	255.255.0.0	172.16.21.5	172.16.21.6	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
172.16.21.1	255.255.255.255	172.16.21.5	172.16.21.6	1
172.16.21.4	255.255.255.252	172.16.21.6	172.16.21.6	30
172.16.21.6	255.255.255.255	127.0.0.1	127.0.0.1	30
172.16.255.255	255.255.255.255	172.16.21.6	172.16.21.6	30
192.168.178.0	255.255.255.0	192.168.178.47	192.168.178.47	10
192.168.178.47	255.255.255.255	127.0.0.1	127.0.0.1	10
192.168.178.255	255.255.255.255	192.168.178.47	192.168.178.47	10
224.0.0.0	240.0.0.0	172.16.21.6	172.16.21.6	30
224.0.0.0	240.0.0.0	192.168.178.47	192.168.178.47	10
255.255.255.255	255.255.255.255	172.16.21.6	172.16.21.6	1
255.255.255.255	255.255.255.255	192.168.178.47	192.168.178.47	1

Standardgateway: 192.168.178.1

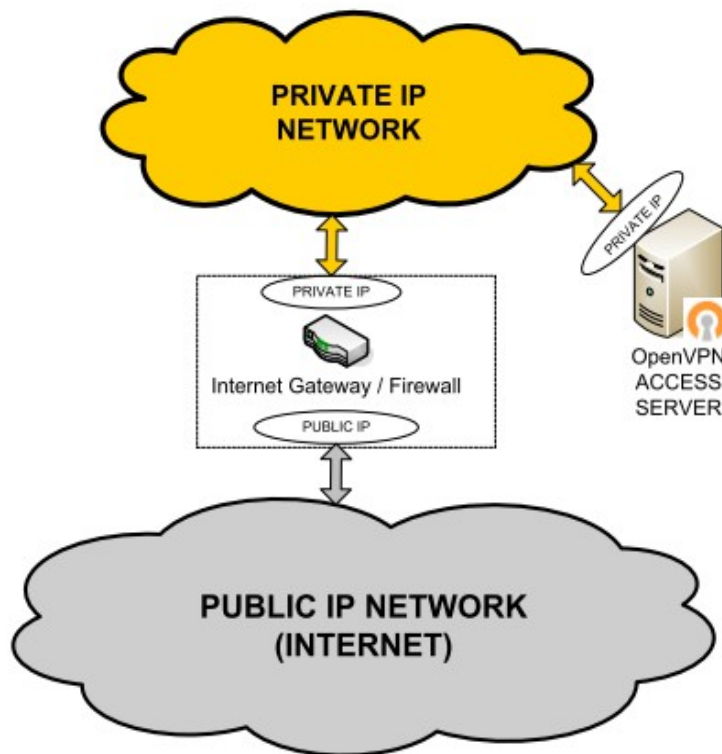
Ständige Routen:

Keine

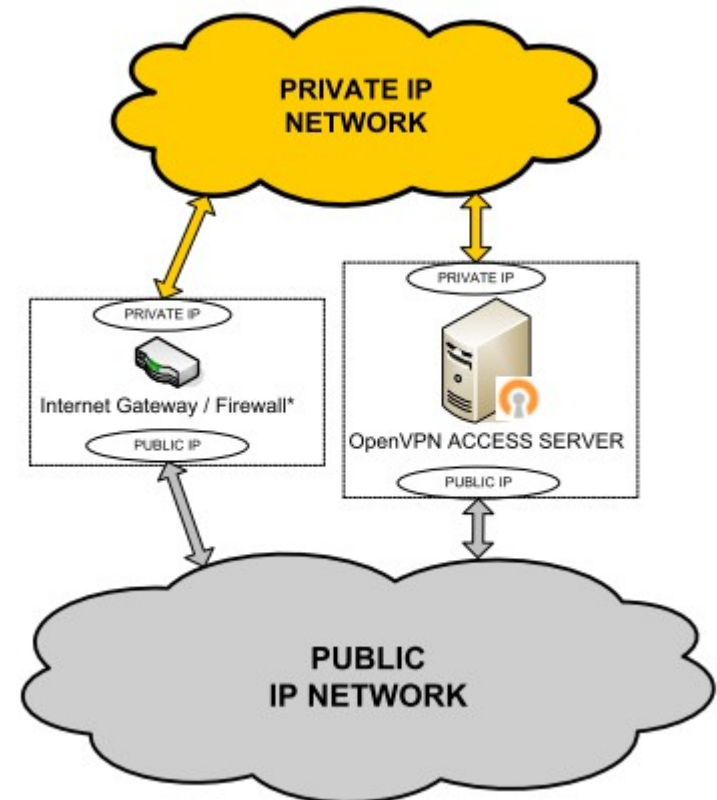
C:\Dokumente und Einstellungen\cisco>

# Alternative OpenVPN Access Server

- ◆ Für 2 Clientverbindungen umsonst
- ◆ Kann schnell als .ova in ESX oder VMware installiert werden
- ◆ Anleitung



oder



Status

- Status Overview
- Current Users
- Log Reports

Configuration

- License
- SSL Settings
- Server Network Settings
- VPN Mode
- VPN Settings
- Advanced VPN
- Web Server
- Client Settings
- Failover

User Management

- User Permissions
- Group Permissions
- Revoke Certificates

Authentication

- General
- PAM
- RADIUS
- LDAP

Tools

- Profiles
- Connectivity Test
- Documentation
- Support

Status Overview

Server Status

The server is currently **ON**

Stop the Server

Active Configuration

Access Server version:	2.0.10
Server Name:	rechner30.gds2.bb.bw.schule.de
Authenticate users with:	local
Accepting VPN client connections on IP address:	eth0: 10.1.1.216
Port for VPN client connections:	tcp/443, udp/1194
OSI Layer:	3 (routing/NAT)
Clients access private subnets using:	NAT
Node:	openvpnas2

Documentation

The Access Server includes a wide range of documentation covering command line tools, scripting, and other advanced topics: [Access Server Documentation](#)

At a glance

Server Status:	on	
License:	2 users	<a href="#">Info</a>
Current Users:	1	<a href="#">List</a>

Öffentliche Adresse  
Schulungsumgebung  
WAN der pFSense

# Wer ist angemeldet?

## Access Server

### Status

[Status Overview](#)[Current Users](#)[Log Reports](#)

### Configuration

[License](#)[SSL Settings](#)[Server Network Settings](#)[VPN Mode](#)[VPN Settings](#)[Advanced VPN](#)[Web Server](#)[Client Settings](#)[Failover](#)

### Current Users

Search By Name or IP Address (Enter joe and all the %joe% names are displayed)

### Current VPN Users

Common Name	Real Address	VPN Address	Bytes Sent Received	Connection Duration	Block
cisco	79.224.249.129:4972	172.27.224.5	6.98KB 6.10KB	0:03:24	<input type="button" value="X"/>
kraut	109.42.3.90:40721	172.27.232.4	4.69KB 3.74KB	0:00:04	<input type="button" value="X"/>