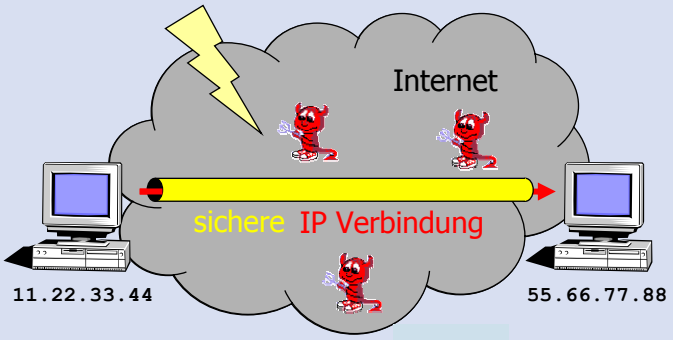
IT-SECURITY - Forum #2

Virtuelle Private Netzwerke in der Anwendung

Dr. Andreas Steffen
Professor für Sicherheit und Kommunikation
Zürcher Hochschule Winterthur
andreas.steffen@zhwin.ch

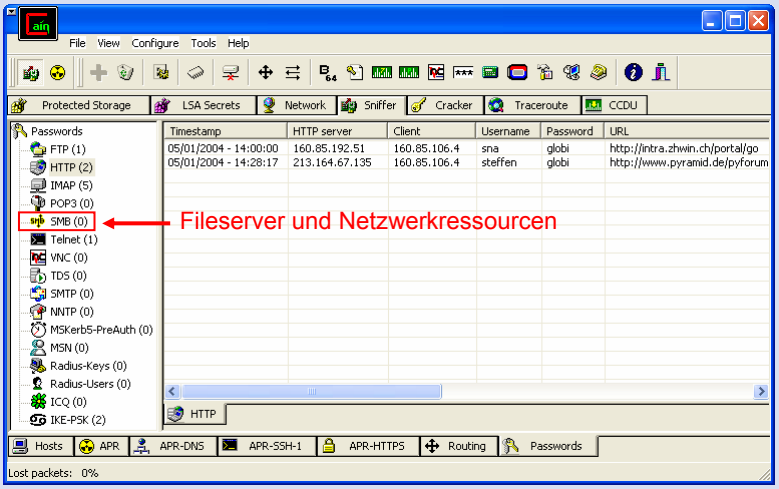
IT-SECURITY - Forum #2

Internet - günstig aber unsicher!



- IP Pakete sollten **verschlüsselt** sein, damit sie unterwegs nicht gelesen werden können!
- IP Pakete sollten **authentisiert** sein, damit sie unterwegs nicht verändert werden können!
- Die Identität von Sender und Empfänger sollte **fälschungssicher** feststehen!

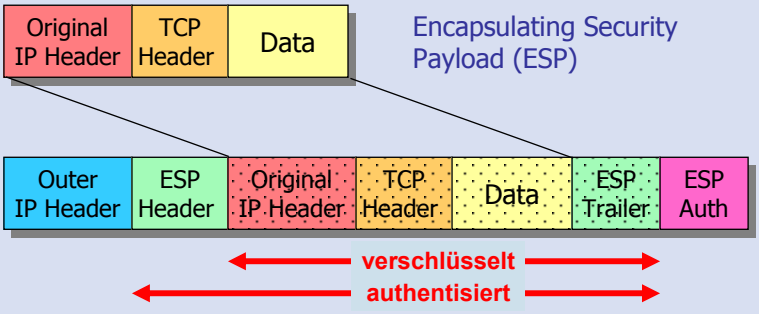
Kinderleichtes Abhören!



- OpenSource Passwort-Sniffer und Cracker **Cain** erhältlich von http://www.oxid.it

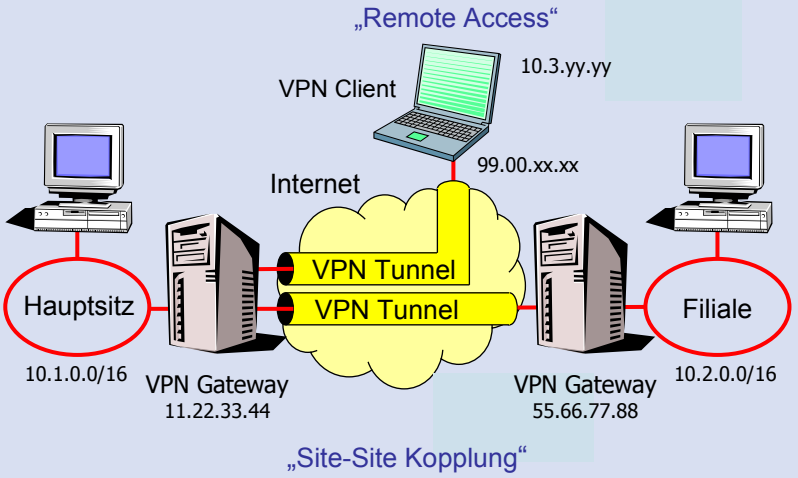
IT-SECURITY - Forum #2

IP Security (IPsec) - Tunnel Modus

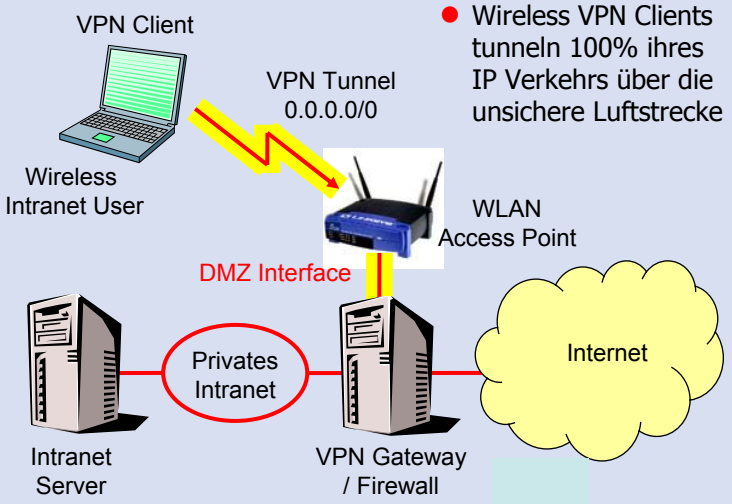


- Eigenes IP Protokoll für ESP: **50**
- ESP Authentisierung ist optional, wird aber meist genutzt
- Der Original IP Header wird mitverschlüsselt und ist deshalb geschützt.

Virtuelle Private Netzwerke

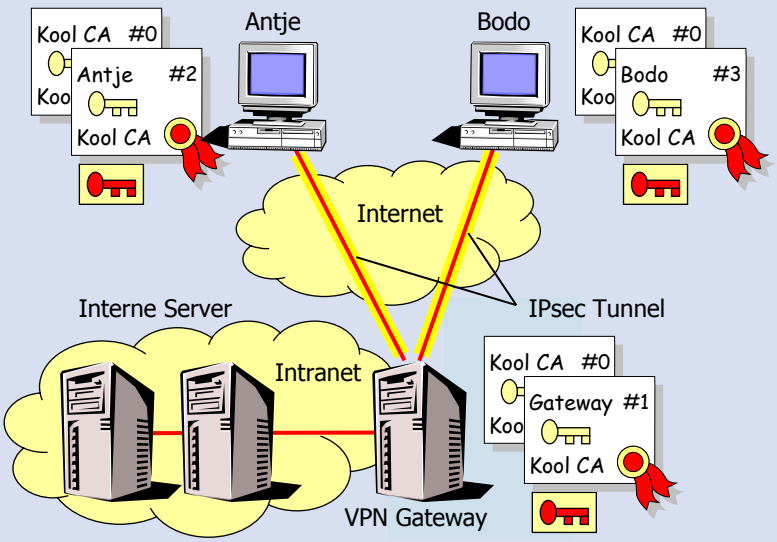


Intranet VPN

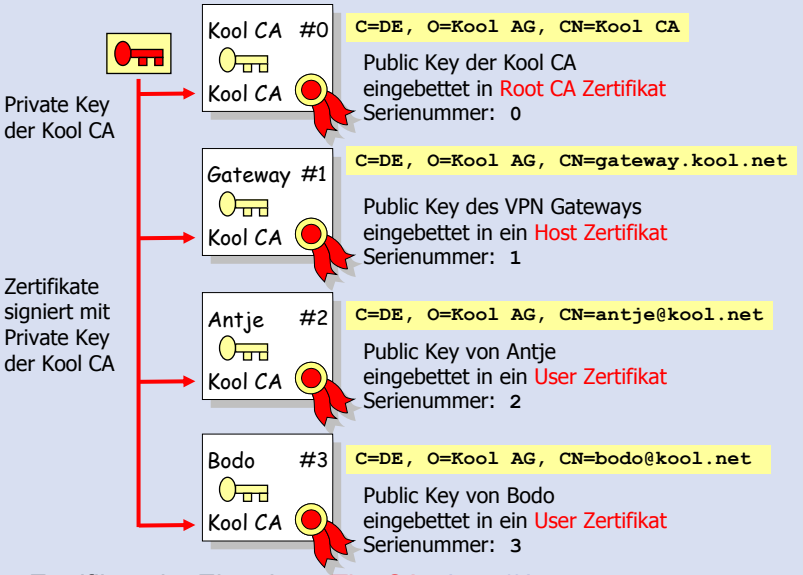


- Wireless VPN Clients tunneln 100% ihres IP Verkehrs über die unsichere Luftstrecke

Authentisierung mit Zertifikaten



Einfache Public Key Infrastruktur

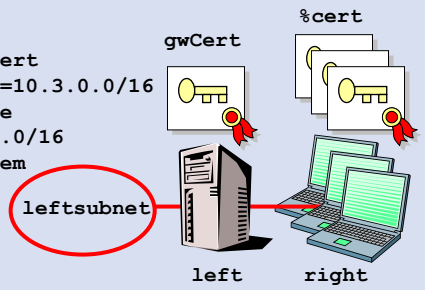


- Zertifikate im Eigenbau: TinyCA - http://tinyca.sm-zone.net

Linux FreeS/WAN VPN Gateway

- OpenSource IPsec Stack für Linux
- Authentisierung durch Zertifikate entwickelt an der **ZHW !**
- Unbegrenzte Anzahl von VPN Tunnel
- Linux FreeS/WAN auch als VPN Client geeignet
- Erhältlich als SuSE/RedHat/Debian/Mandrake RPM
- Kommerzielle CD-Firewall Version: www.astaro.de
- Einfache Konfiguration:

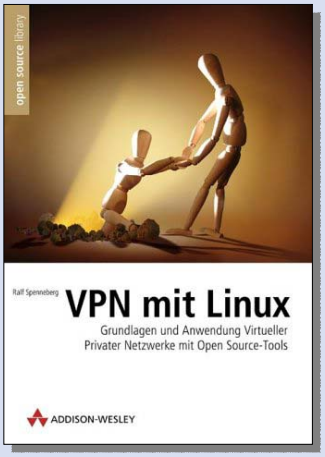
```
conn remote-access
     right=%any
     rightrsasigkey=%cert
     rightsubnetwithin=10.3.0.0/16
     left=%defaultroute
     leftsubnet=10.1.0.0/16
     leftcert=gwCert.pem
     auto=add
```



IT-SECURITY - Forum #2

Literatur

- **Ralf Spenneberg,**
  "VPN mit Linux"
  Grundlagen und Anwendung Virtueller Privater Netzwerke mit Open Source-Tools,
  418 Seiten, November 2003,
  Addison-Wesley, München
  ISBN 3-8273-2114-X
- **FreeS/WAN Howto**
  http://www.spenneberg.de/linux-magazin/024-028_freeswan.pdf
- **Andreas Steffen,**
  "Virtual Private Networks – Coping with Complexity"
  http://security.zhwin.ch/DFN_VPN.pdf



IT-SECURITY - Forum #2

Windows 2000/XP VPN Client

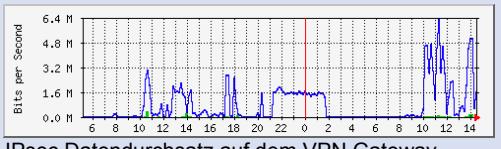
- Windows 2000/XP hat einen eingebauten IPsec Stack
- Konfiguration über die Management Konsole (mmc) ist extrem mühsam und fehleranfällig.
- Open Source IPsec Tool von http://vpn.ebootis.de lädt Konfiguration direkt in die Windows Registry:

```
conn wlan-client
     left=%any                    # insert client IP
     right=10.1.0.1               # gateway IP
     rightsubnet=*                # tunnel all traffic
     rightca="C=CH,O=ZHW,CN=ZHW CA"
     network=lan
     auto=start
```

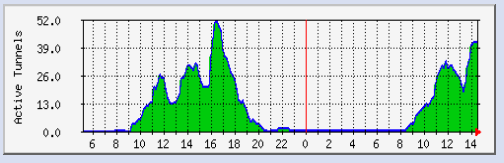
- Kommerzielle Windows VPN Clients
  - SafeNet/SoftRemote: www.safenet-inc.com
  - SSH Sentinel: www.ssh.com
    (Produktlinie am 14.10.2003 durch SafeNet übernommen)

Beispiel – Universität Freiburg i. Br.

Campus



IPsec Datendurchsatz auf dem VPN Gateway



Anzahl aktiver VPN Tunnel

- 44 WLAN Access Points, 1 Linux VPN Gateway
- 202 aktive and 88 gesperrte X.509 Zertifikate
- Linux FreeS/WAN Clients / SSH Sentinel Windows Clients
- Weitere Information: http://mopoinfo.vpn.uni-freiburg.de

IT-SECURITY - Forum #2

Zusammenfassung

- Virtuelle Private Netzwerke basierend auf IPsec sind eine **reife** Technologie geworden.
- Interoperabilitätstest am IPsec 2001 Global Summit in Paris haben gezeigt, dass fast alle IPsec Produkte [nach einem Fine-Tuning] zusammenarbeiten können:

Linux FreeS/WAN, OpenBSD, NetScreen, Nortel Contivity, Cisco IOS/PIX/VPN3000, Checkpoint, 6WIND (IPv6), etc.

- Es existieren kostengünstige OpenSource Lösungen für das Aufsetzen von VPN Gateways, sowie das Betreiben einer einfachen In-House PKI.

Weitere Informationen unter: http://security.zhwin.ch