

Schutz und Absicherung von Internetverbindungen

Maßnahmen zur Abwendung verschiedener Gefahren:
von lokalen Angreifern bis zu Backbone-Providern

Informationsveranstaltung
Informationssicherheit
19. November 2009, Steyr

Priv.-Doz. Dr. Rene Mayrhofer
eSYS Informationssysteme GmbH / Gibraltar

<http://www.esys.at>
rene.mayrhofer@gibraltar.at

Gefahren für Internetverbindungen

- Abhören („Eavesdropping“)
- Aufzeichnen und erneut einspeisen („Replay“)
- Manipulieren, Absender fälschen („Forgery“)
- „Man-in-the-middle“
- Unterbrechen („Denial of Service“)
- Angriff auf die Privatsphäre („Privacy Attack“)
- ...

Einfach durchzuführende Angriffe: Jeder

- Verschiedene DNS-Attacken zum Umleiten von Verbindungen in der Praxis erfolgreich („DNS Poisoning“)
- Abhören von Verbindungen über WLAN (typischerweise sehr einfach)
- Umleiten von Verbindungen durch ADSL-Router (UPnP und Browser-basierte Exploits)
- IP-Spoofing zum Einschleusen gefälschter Pakete
- Rücksetzen / Abbrechen von TCP-Verbindungen aus der Ferne (DoS)
- Überlasten von Internetverbindungen (DDoS)
- ...

Einfach durchzuführende Angriffe: Provider

- Mitlesen aller Pakete, Reassemblieren, Aufzeichnen von Passwörtern, Inhalten, etc.
- Blockieren bestimmter Verbindungen
- Traffic-Shaping je nach vom Provider gewünschten/ungewünschten Diensten
- Protokollieren von Meta-Daten über Verbindungen (Quelle, Ziel, Datum/Zeit, Dauer der Verbindung, übertragene Datenmenge, Häufigkeit von Verbindungen zum selben Ziel, Ermittlung der Client-Betriebssysteme, Anzahl Hosts im Unternehmensnetzwerk – auch hinter NAT, etc.) und Speicherung auf unbestimmte Zeit
- volle Man-in-the-Middle Attacken

VPNs zum Schutz gegen viele Angriffe

VPNs auf verschiedenen Ebenen

- ISO/OSI Layer 3 (IP): **IPsec**
- ISO/OSI Layer 2-4 (TCP/UDP mit IP- oder Ethernet-Tunneling):
OpenVPN
- ISO/OSI Layer 5-7: **TLS/SSL**

Ziel ist immer gleich: Herstellung eines **sicheren Kanals** zwischen zwei Entitäten (Hosts oder Applikationen)

Sicherer Kanal

- Kommunikationskanal zwischen zwei Personen/Objekten (Prinzipale/Principals, Entitäten)
- Beide sind **wechselseitig authentifiziert**
⇒ stellt sicher, dass keine Man-in-the-Middle oder Tunneling / Relaying Angriffe möglich sind
⇒ in der Praxis leider oft nur kryptographisch sichere Authentifizierung **einer** Seite, daher noch Möglichkeiten für Angriffe
- Kanal ist **verschlüsselt** und dessen **Integrität** gegen Abhören / Änderung / Erzeugung **geschützt**

Hauptproblem: initialer Schlüsselaustausch

Wenn Schlüsselaustausch nicht sicher ist, sind alle nachfolgenden kryptographischen Maßnahmen sinnlos!

- Meist schwächstes Glied im Protokoll
⇒ z.B. Grund für völlige Unsicherheit von PPTP in Microsoft Windows Server
- Möglichkeiten
 - „in-band“: Diffie-Hellman (Schlüsselvereinbarung über unsichere Kanäle) + Authentifizierung der Schlüssel
 - „out-of-band“: über anderen Kanal (TAN-Brief, USB-Stick, etc. oder neue Protokolle basierend auf Sensoren in Mobilgeräten)

Verdachtsunabhängige Vorratsdaten

Verbindungs- / Verkehrsdaten: Meta-Daten

- wer, wann, wo, wie, nicht was
- Zeitpunkt, Dauer, Telefonnummern, Ort des Verbindungsauf- und -abbaus, Emailadressen, Webadressen, etc.
- automatische Aufzeichnung auf Vorrat, Speicherung 6-24 Monate

Verdachtsunabhängige Vorratsdaten

Pro und Contra aus technischer Sicht

- Aufklärung im Nachhinein erleichtert weil Daten „einfach“ verfügbar
- keine Verhinderung von Strafdaten „live“ möglich – zu viele Daten!
- **Meta-Daten verraten oft schon viel über Inhalt**

Pro und Contra aus rechtlicher Sicht

- Argumentation mit schweren Straftaten und Terrorismus
EU Richtlinie: Straftaten mit >3 Jahre, Entwurf Österreich: 1 Jahr
- in Deutschland scharfe Kritik und heftige Kontroversen auch in Presse
in Österreich noch wenig öffentlicher Diskurs, aber erste Kritik
Verfassungsbeschwerde von AK Vorrat mit 30.000 Unterstützern
- direkter Konflikt mit europäischem Datenschutzgesetz
- **Wer trägt die hohe Kosten?**

Sicherheitspolizeigesetz als Umgehung

Sicherheitspolizeigesetz in Österreich

- Polizei- (und Militär-)Ermächtigungsgesetz
- am 6.12.2007 um 23:50 im Nationalrat beschlossen, ohne Behandlung im zuständigen Ausschuss, letzte Version nicht dem Datenschutzrat vorgelegt
- Zugriff auf Mobilfunk-Standortdaten und IP-Adressen bei „Gefahr um Verzug“ **ohne Richtervorbehalt und Verständigungsverpflichtung (!)**
- Begründung durch Suche von Vermissten oder Entführten
seit Inkrafttreten am 1. Jänner 2008: **„Auffällig ist, dass die Suizidgefährdung zu steigen scheint, seitdem der Paragraph in Kraft getreten ist“** (Chef der Rechtsabteilung von T-Mobile, Klaus Steinmaurer)

1. Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses; 2. Internet-Protokoll-Adresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung sowie 3. Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war. Das gelte, "wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen".

IPsec Übersicht

- IETF Standard, ursprünglich 1998 entwickelt
- aktuelle RFCs 4301–4303, 2407–2409, 4306 + viele mehr
- kontinuierlich weiterentwickelt
- (meist) zwischen verschiedenen Implementierungen interoperabel
- ursprünglich für IPv6 entwickelt, dann für IPv4 angepasst
- zwingend für IPv6 Implementierungen, optional für IPv4 (aber heute für viele Betriebssysteme verfügbar)

⇒ **derzeit einer der sichersten Standards!**

IPsec Modi

Transport Modus

- Ende-zu-Ende Sicherheit zwischen zwei Hosts
- ist (mit kleinen Einschränkungen) eine Untermenge des Tunnel Modus und könnte daher weggelassen werden

Tunnel Modus

- Netzwerk-zu-Netzwerk, Host-zu-Netzwerk oder Host-zu-Host (siehe VPN)
- Unterschied zum Transport Modus nur durch "Next Header" Feld
 - entweder ganzes IP Paket als Payload
 - oder Protokoll der nächsthöheren Schicht

IPsec Protokolle

ESP: Encapsulating Security Payload

- (IP Protokoll Nummer 50): (optionale) Authentifizierung + Verschlüsselung des Payload

AH: Authentication Header

- (IP Protokoll Nummer 51): Nur Authentifizierung, aber des Payload + IP Header
- Alle IP Header Felder außer TOS, Flags, Fragment Offset, TTL und Header Checksum authentifiziert

IPsec Protokolle

Für beide Protokolle verwendet

- **IKE** für Schlüsselverwaltung, basiert auf
- **ISAKMP**

Typische Kombinationen:

- Transport Modus mit ESP (+Authentifizierung) für verschlüsselte oder mit AH für authentifizierte Pakete
- **Tunnel Modus mit ESP**

IPsec Implementierungen

IPsec kann an verschiedenen Stellen implementiert werden:

- Gateways: für VPNs zwischen Netzwerken oder sichere „Einwahl“ von „Road Warriors“ aus dem Internet ins eigene Netzwerk
- Hosts: für Ende-zu-Ende Sicherheit

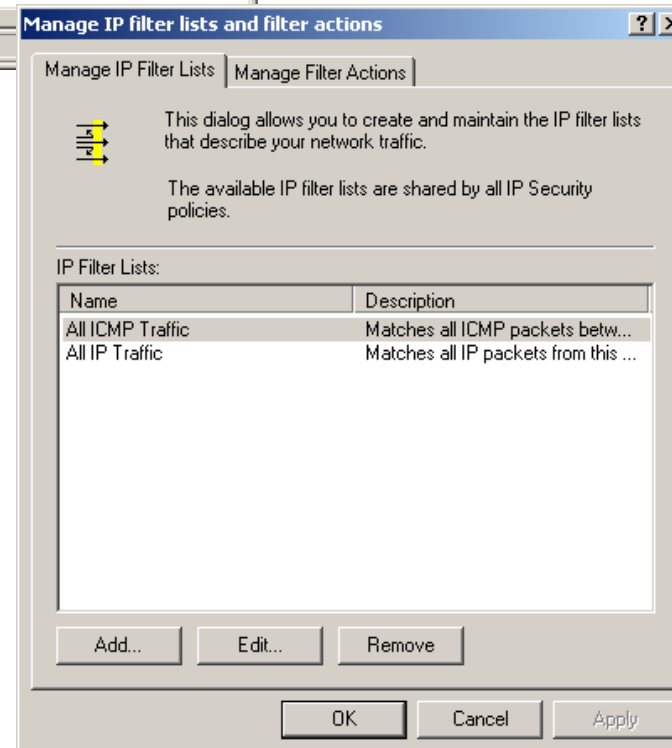
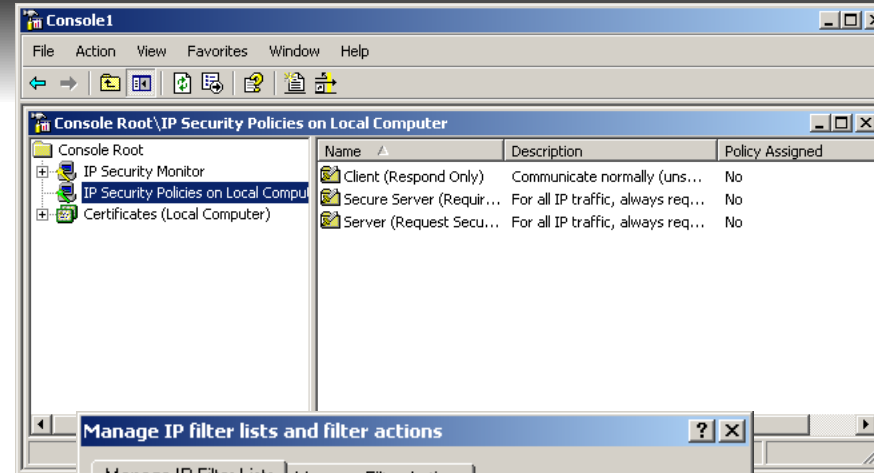
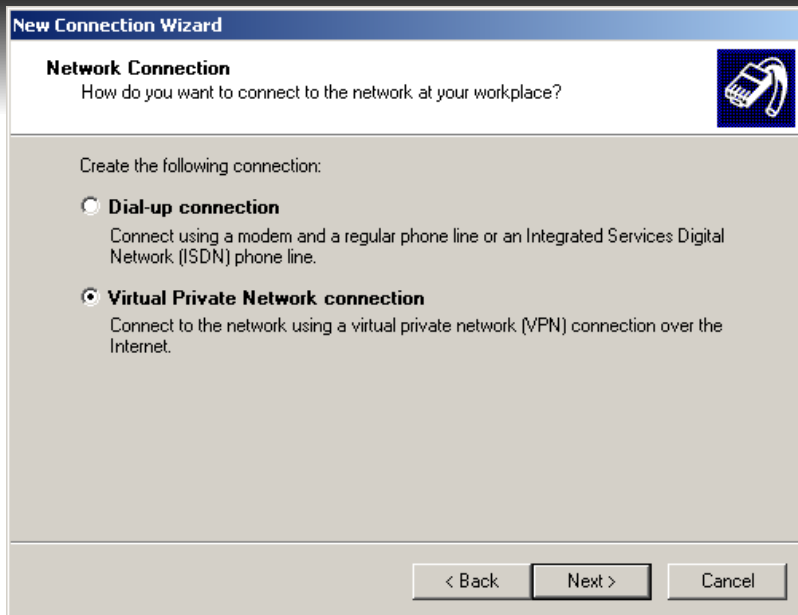
Authentifizierung erfolgt immer gegenseitig

- Pre-Shared Keys (PSK): ähnlich Passwörter
- RSA public/private key Signaturen, typisch mit X.509 Zertifikaten und PKI
- Erweiterungen für Benutzerauthentifizierung (XAUTH)

IPsec in der Praxis

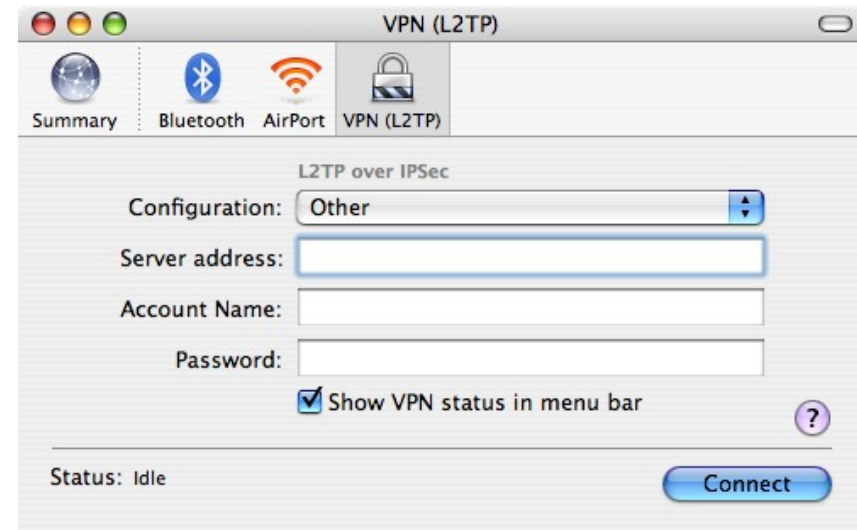
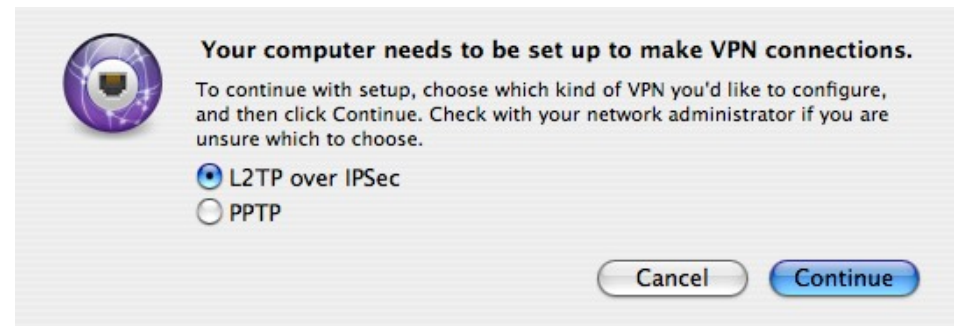
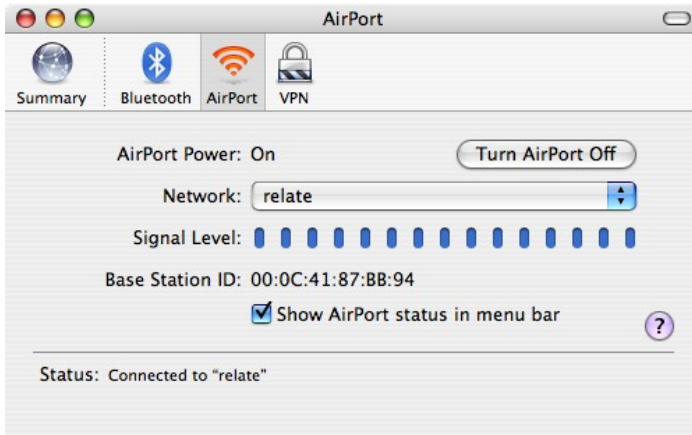
- Integriert seit Windows 2000 (Windows XP SP2 für NAT-Traversal), seit Windows 7 „einfach“ einzurichten (Wizard-Unterstützung nur für IPsec ohne Zwang zu L2TP)
- Linux: FreeS/WAN, Openswan, strongSwan (mit IKEv2), ...
- Mac OS/X: racoon + eigenes GUI
- OpenBSD: isakmpd
- FreeBSD/NetBSD (KAME): racoon
- Div. Mobilbetriebssysteme (Windows Mobile, Erweiterungen für Symbian, etc.)

IPsec in der Praxis: Windows



**Einfacher in
Verbindung
mit L2TP!**

IPsec in der Praxis: Mac OS/X



IPsec in der Praxis: Gibraltar Firewall Linux

Gibraltar-WebInterface --- Host: gibraltar3-esys-master - Shiretoko

File Edit View History Bookmarks Tools Help

80.120.3.125 https://80.120.3.125:8443/vpn/tunnel.jsp

Stumble! I like it! All Share Info Channels: Favorites Friends Tools

ar GibADMIN 2.99 beta097 Upload license Support Update Help Quick-Save Logout English Go

IPSec Settings

General settings Tunnel

Tunnel:	Description	Local IP address	Local subnet	Remote IP or FQDN address	Remote subnet	State	
	Bestattung_Eckl	80.120.3.125	10.50.48.0/20	88.116.68.214	192.168.11.0/24	(started)	
	BlueSky	80.120.3.125	10.50.50.52/32	80.120.3.65	10.10.1.0/24	(started)	
	Chris	80.120.3.125	10.50.48.0/20	Any	192.168.13.0/24	(started)	
	Copyright	80.120.3.125	10.50.48.0/20	85.124.41.98	192.168.0.0/24	(started)	
	CopyrightDMZ	80.120.3.125	10.50.48.0/20	85.124.41.98	10.0.5.0/24	(started)	
	Ebnerbau	80.120.3.125	10.50.48.0/20	80.120.44.114	192.168.33.0/24	(started)	
	elters	80.120.3.125	10.50.56.0/24	91.112.226.242	10.128.26.0/24	(standby)	
	envitec	80.120.3.125	10.50.57.15/32	80.120.3.65	192.168.37.0/24	(started)	
	esys_Rangger	80.120.3.125	10.50.50.0/24	Any	172.21.200.0/24	(deactivated)	
	eSYSKdf	80.120.3.125	10.50.48.0/20	91.112.37.195	10.100.100.0/24	(started)	
	Einedie...	80.120.3.125	10.50.48.0/20	92.82.120.116	192.168.50.0/24	(started)	

Done rmayr Now: Mostly Cloudy, 15° C Tue: 19° C Wed: 23° C

IPsec in der Praxis: Gibraltar Firewall Linux

The screenshot shows the Gibraltar WebInterface configuration page for an IPsec tunnel. The browser window title is "Gibraltar-WebInterface --- Host: gibraltar3-esys-master - Shiretoko". The address bar shows the URL "https://80.120.3.125:8443/vpn/detail.jsp". The left sidebar contains a navigation menu with categories like Home, System, Monitoring, Services, Definitions, Network, Firewall, NAT, User, Mail, VPN, Proxy Server, IDS, Traffic shaping, Captive Portal, and Configuration management. The main content area is titled "IPsec Settings" and has three tabs: "Default", "Advanced", and "Watchdog". The "Default" tab is active, showing the following configuration fields:

- Description: Rene_Linz1
- State after start: (standby)
- Local IP address: 80.120.3.125 - wan:0
- Local subnet: 10.50.50.0/24
- Local certificate: esys_gibraltar.pem
- Remote IP or FQDN address: (empty) Host Any remote IP
- Remote subnet: 10.0.0.0/25 Special handling for road warriors behind NAT gateways: rightsubnetwithin
- Authorization: Password X.509 certificate gibraltar-rene.pem
- Signed by Certified Authority:
- Use with L2TP:
- Local ID (left ID): (empty)
- Remote ID (right ID): (empty)
- Next router IP (The system will detect one if empty): 80.120.3.65

At the bottom of the configuration area are "Save" and "Cancel" buttons. The system tray at the bottom of the window shows the date "2009-11-19", the user "rmayr", and weather information: "Now: Mostly Cloudy, 15° C", "Tue: 19° C", "Wed: 23° C".

IPsec in der Praxis: Gibraltar Firewall Linux

Gibraltar-WebInterface --- Host: gibraltar3-esys-master - Shiretoko

File Edit View History Bookmarks Tools Help

80.120.3.125 https://80.120.3.125:8443/vpn/advancedDetail.jsp

System
Monitoring
Services
Definitions
Network
Firewall
NAT
User
Mail
VPN
• OpenVPN
• **IPSec**
• PPTP
• L2TP
• Certificates
• SSL
• SSL-VPN
Proxy Server
IDS
Traffic shaping
Captive Portal
Configuration management

Default **Advanced** Watchdog

Type: Tunnel Transport

IP compression:

PFS:

Number of trials: (0 for unlimited trials)

Keylife (IKE - Phase 1): s

Keylife (Phase 2): s

Phase 1: **IKE algorithms**

- aes128
- aes192
- aes256
- 3des
- blowfish
- twofish
- serpent
- cast

Hash algorithms

- sha1 (160 bits)

Done rmayr Now: Mostly Cloudy, 15° C Tue: 19° C Wed: 23° C

TLS Übersicht

Transport Layer Security, hervorgegangen aus SSL

- Handshake protocol
- Record protocol
- Change cipher spec protocol
- Alert protocol

Detailspezifikationen

- [1] Rescorla, E., et al.. HTTP Over TLS. RFC 2818. 2000.
- [2] Dierks, T. and C. Allen. The TLS Protocol. RFC 2246.1999.

Basis für HTTPS, IMAPS, POP3S, FTPS, SMTP-TLS, etc.

OpenVPN Übersicht

- Kein RFC-Standard, sondern Pseudo-Standard durch Open Source Implementierung
- Aber: verfügbar für so gut wie alle Betriebssysteme
- Im Vergleich zu IPsec deutlich einfacher (eine freie Referenzimplementierung, kein Design eines Konsortiums)
- Gilt derzeit in Crypto-Community als sicher

OpenVPN Details

- Für Verbindung nur TCP oder UDP Port 1194 benötigt, Möglichkeit zum Tunneling über HTTPS- oder Socks-Proxies ⇒ **NAT-friendly**
 - Schlüsselaustausch an TLS angelehnt
 - Sicherer Kanal an ESP angelehnt
- Authentifizierung
 - PSK oder X.509 Zertifikate für Server **und** Client
 - **Zusätzliche** Möglichkeit für Benutzername/Passwort

OpenVPN in der Praxis: Gibraltar Server

OpenVPN in der Praxis: Gibraltar Server

The screenshot shows a web browser window titled "Gibraltar-WebInterface --- Host: gibraltar3-esys-master - Shiretoko". The address bar shows the URL "https://80.120.3.125:8443/vpn/extended.jsp". The browser's address bar also contains "80.120.3.125" and "https://80.120.3.125:8443/vpn/extended.jsp". The browser's address bar also contains "80.120.3.125" and "https://80.120.3.125:8443/vpn/extended.jsp". The browser's address bar also contains "80.120.3.125" and "https://80.120.3.125:8443/vpn/extended.jsp".

The main content area is titled "OpenVPN" and has three tabs: "General settings", "Extended Settings" (selected), and "Status".

Under "Extended Settings", the following options are visible:

- Enable:
- Compression:
- Keep alive (Ping):
- Keep alive (Timeout):
- assigned client IP range:
- internal DNS Server 1:
- internal DNS Server 2:
- internal WINS Server:
- Allow Fragmentation:
- MTU Size:
- MSS Fix:
- Float:

At the bottom of the settings area, there are two buttons: "Save" and "Download client config".

OpenVPN in der Praxis: Gibraltar Server

Gibraltar GibADMIN 2.99beta097

Upload license | Support | Update | Help | Quick-Save | Logout | English

OpenVPN

General settings | Extended Settings | **Status**

Currently connected users:

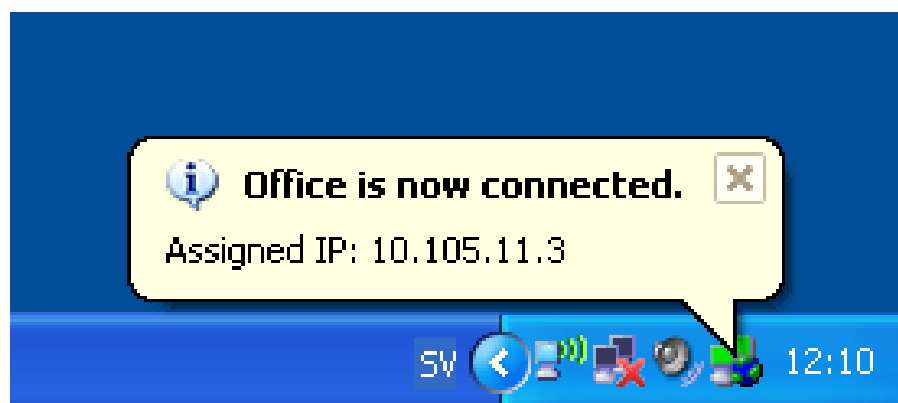
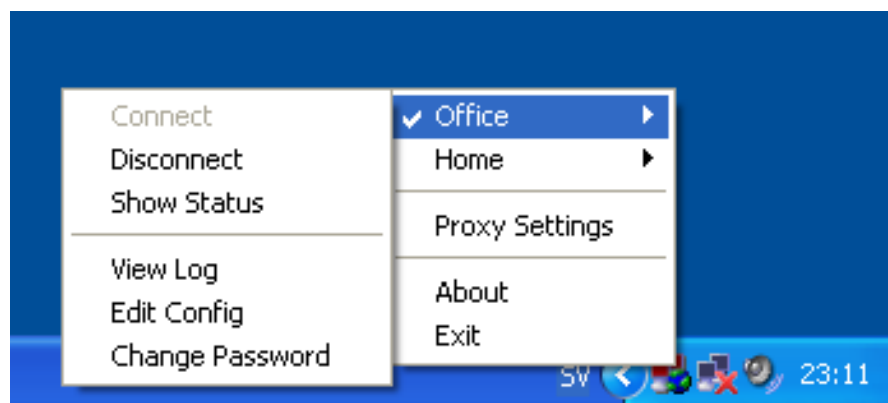
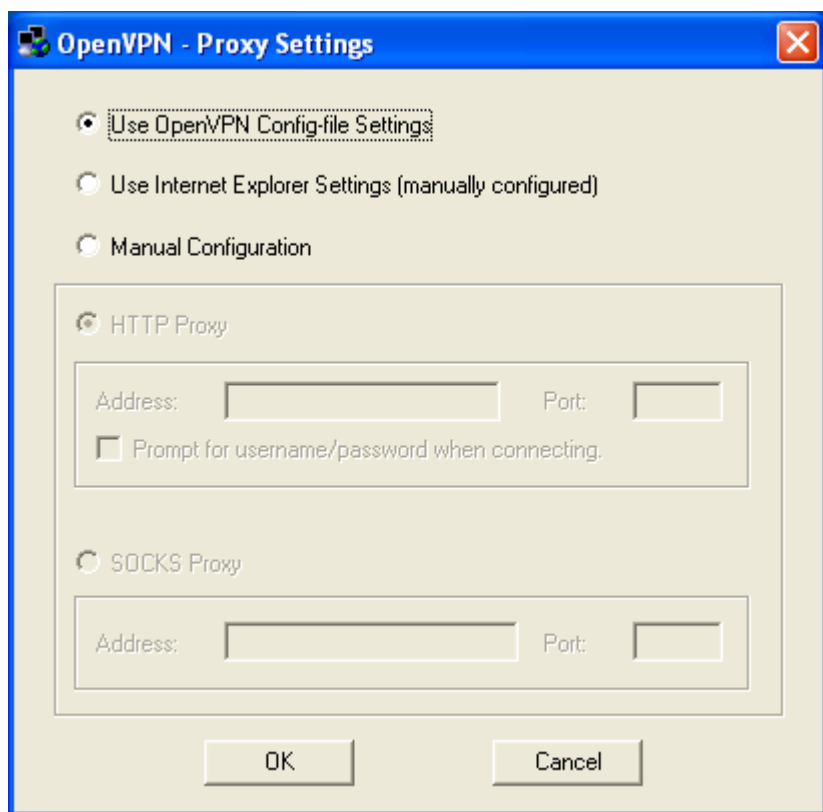
	Common Name	Real Address	Bytes received	Bytes sent	Connected since
	Networking	212.227.252.203:36211	514880	538548	Mon Oct 5 06:42:31 2009
	pgastinger	91.128.117.57:48454	777810	2704697	Mon Oct 5 20:22:00 2009

Assigned, static addresses:

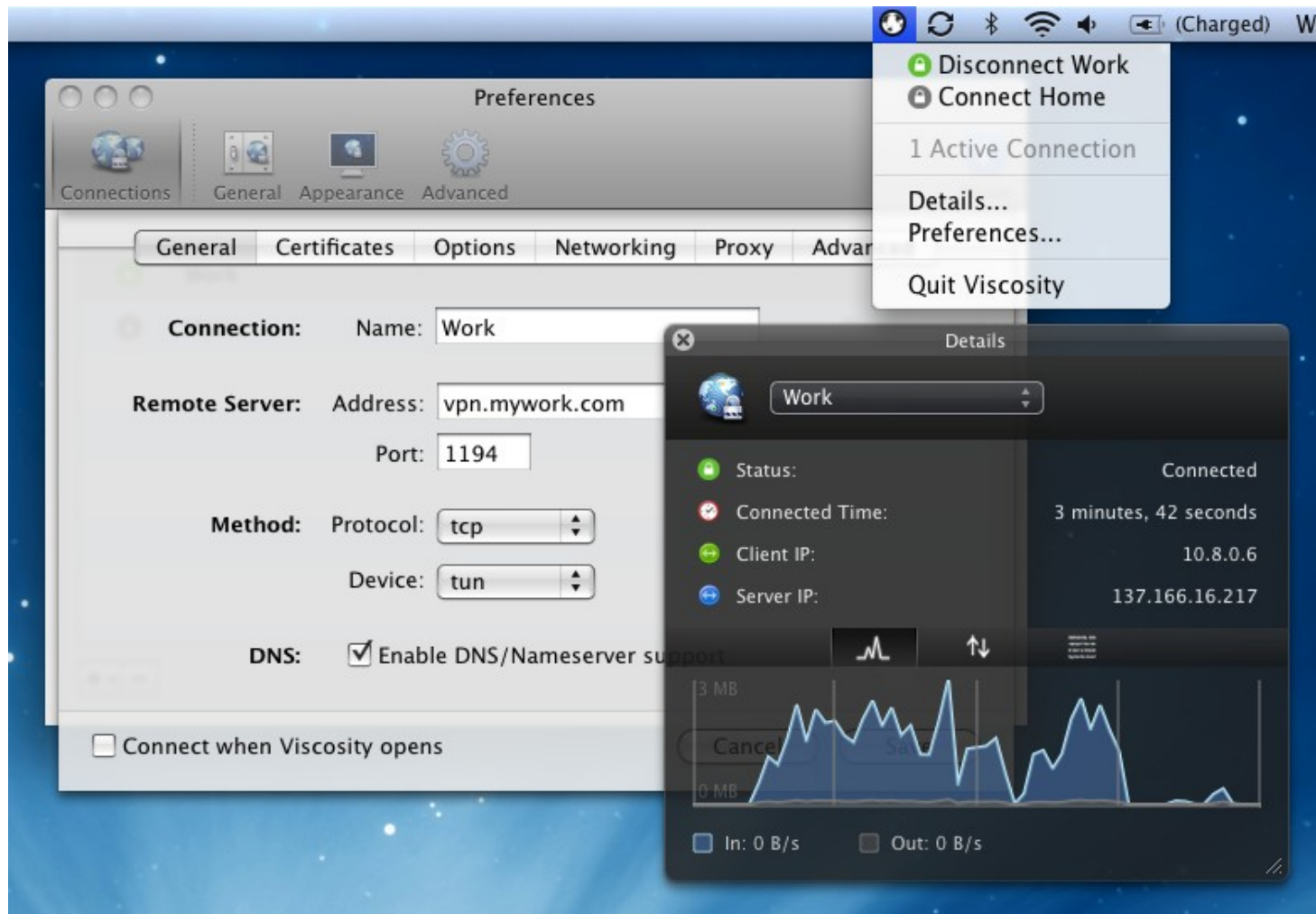
	Common Name	Virtual address
	ckatterl	10.8.0.10
	lrangger	10.8.0.18
	Networking	10.8.0.6
	pgastinger	10.8.0.14
	rleitner	10.8.0.26
	rmayrhofer	10.8.0.22

Done | rmayr | de-DE | Now: Mostly Cloudy, 15° C | Tue: 19° C | Wed: 23° C

OpenVPN in der Praxis: Windows Client



OpenVPN in der Praxis: Mac OS/X Client



Sicherheit gegen Verbindungsanalyse

Auch sichere Kanäle haben eine Quelle und ein Ziel und sind meist als solche identifizierbar

- Wer mir wem, wann, wie oft, wie lange, etc. kommuniziert ist auch mit sicheren Kanälen sichtbar (außer wenn **alle Verbindungen in einem VPN** stattfinden, z.B. bei Roadwarriorn)
- Zusätzlicher Schutz gegen Analyse der Verkehrsdaten daher je nach entsprechender Gefährdung nötig
 - **Tor**: Socks-Proxy für TCP- und UDP-Verbindungen durch „Onion-Routing“ Mix-Netzwerk
 - **JonDonym** (früher JAP): HTTPS-Proxy durch statische Mix-Kaskaden, kommerzielle Kaskaden für höheren Durchsatz
 - **Freenet**: Speichernetz für Inhaltsdaten mit anonymem Zugriff

Tor in Gibraltar Firewall

Gibraltar 2.99beta097, 2009 by eSYS Informationssysteme GmbH

JonDonym in Gibraltar Firewall

The screenshot shows a web browser window titled "Gibraltar-WebInterface --- Host: gibraltar3-esys-master - Shiretoko". The address bar shows the URL "https://80.120.3.125:8443/proxy/jondonym.jsp". The browser's tab bar contains several open tabs, including "An Introduction To J...", "Displaying Richface...", "Using a Linux L2TP/I...", "HOWTO: Linux VPN...", "eGroupWare: Gibra...", and "Gibraltar-WebInterfa...".

The main content area of the browser displays the "Gibraltar GibADMIN 2.99beta097" interface. At the top, there is a navigation bar with links for "Upload license", "Support", "Update", "Help", "Quick-Save", "Logout", and a language dropdown set to "English".

On the left side, there is a sidebar menu with the following items: Home, System, Monitoring, Services, Definitions, Network, Firewall, NAT, User, Mail, VPN, **Proxy Server** (with sub-items: HTTP proxy, POP3 proxy, FTP proxy), **Anonymization**, IDS, Traffic shaping, Captive Portal, and Configuration management.

The main content area is titled "HTTP proxy" and contains three tabs: "JonDonym HTTP Anonymizer" (selected), "Tor Anonymizer", and "Freenet".

Under the "JonDonym HTTP Anonymizer" tab, the following configuration options are visible:

- Anonymization service status:** connected (indicated by a red dot)
- Auto-start at bootup:**
- Automatically switch cascades on disconnect:**
- Remaining transfer volume on commercial cascades:** 0 Quota should be recharged as soon as possible!
- Save:** A button to save the current configuration.
- Connected to cascade:** SecureInternet2-GPF, false, 397/400; 2 -- [Mix1 ch\(Contact ch\)](#), [Mix2 de\(Contact de\)](#) Mix1 ch(Contact ch), [Mix2 de\(Contact de\)](#)> [Switch to different cas](#)
- Enter new coupon code for commercial cascades:** A text input field followed by a **Validate** button.

Gibraltar 2.99beta097, 2009 by eSYS Informationssysteme GmbH

Freenet in Gibraltar Firewall

Gibraltar-WebInterface --- Host: gibraltar3-esys-master - Shiretoko

File Edit View History Bookmarks Tools Help

80.120.3.125 https://80.120.3.125:8443/proxy/freenet.jsp

gpg universal server

An Introduction To J... Displaying Richface... Using a Linux L2TP/... HOWTO: Linux VPN... eGroupWare: Gibral... Gibraltar-WebInterfa...

Home
System
Monitoring
Services
Definitions
Network
Firewall
NAT
User
Mail
VPN
Proxy Server
• HTTP proxy
• POP3 proxy
• FTP proxy
• **Anonymization**
IDS
Traffic shaping
Captive Portal
Configuration management

Anonymization

JonDonym HTTP Anonymizer Tor Anonymizer **Freenet**

This function is still experimental!

Server Port: 14327

Client Port: 8481

Access allowed from: IP/network address

Add entry

Do announce:

Store size (in MB; min. 256): 256

Bandwidth limit incoming: 0

Bandwidth limit outgoing: 12288

Maximum number of connections: 200

Mainport: 8888

Access web frontend from: IP/network address

Add entry

Save

Done rmayr Now: Mostly Cloudy, 15° C Tue: 19° C Wed: 23° C

Points to take away

- Internet-Verbindungen sind vielen Gefahren ausgesetzt
- **VPNs schützen** gegen viele davon (Abhören, Modifizieren, Replay, unauthorisierter Verbindungsaufbau, etc.)
- IPsec derzeit sicherster Standard mit vielen Implementierungen, aber komplex
- TLS auf Anwendungsebene weit verbreitet, aber problematisch wegen meist einseitiger Authentifizierung
- OpenVPN ähnlich sicher wie IPsec, deutlich einfacher und mit Unterstützung für Ethernet-Tunneling
- Empfehlung: **IPsec für Site-to-Site, OpenVPN für Roadwarrior, TLS für Anwendungen** (am besten für alle, auch durch andere VPNs)
- **VPNs alleine sind nicht ausreichend** um Privatsphäre zu schützen!

Referenzen

Vorratsdatenspeicherung

- <http://futurezone.orf.at/it/stories/232326/>
- <http://futurezone.orf.at/it/stories/267080/>
- <http://futurezone.orf.at/it/stories/263387/>
- <http://futurezone.orf.at/it/stories/265465/>
- <http://futurezone.orf.at/it/stories/264650/>
- <http://futurezone.orf.at/it/stories/259971/>
- <http://oe1.orf.at/highlights/108201.html>
- <http://oe1.orf.at/inforadio/83381.html?filter=3>

Sicherheitspolizeigesetz

- <http://futurezone.orf.at/it/stories/249406/>
- <http://futurezone.orf.at/it/stories/263387/>
- <http://futurezone.orf.at/it/stories/241208/>
- <http://futurezone.orf.at/it/stories/242015/>
- <http://futurezone.orf.at/it/stories/243929/>
- <http://futurezone.orf.at/it/stories/243503/>
- <http://www.ueberwachungsstaat.at/>

Danke für Ihre Aufmerksamkeit!

Folien: <http://www.mayrhofer.eu.org/presentations>

eSYS Informationssysteme GmbH
Steinhüblstraße 1
4800 Attnang-Puchheim
Tel: +43 720 702 845
Fax: +43 7674 21 495
office@esys.at

OpenPGP Schlüssel: 0xC3C24BDE
7FE4 0DB5 61EC C645 B2F1 C847 ABB4 8F0D C3C2 4BDE