Windows-Installation & Fernwartung

Sicherheitstage WS 2006/2007

Hergen Harnisch

harnisch@rrzn.uni-hannover.de

22.11.2006

Installation

- am Netz
- im geschützten Netz
- mit Update-CD

UltraVNC

Putty-SSH

- Tunnel
- Key

Personal Firewall

- XP/2003: ICF
- ab 2000: Core Force

R|R|Z|N

Problem

- Softwarestand auf Installations-CD ist alt,
  keine aktuellen Patches, daher *exploitable bugs*
- Windows-Update erst möglich, wenn System schon am Netz
- *Infektion während der Installation ist häufig!*

Ausweg

- Absicherung der Netzwerkschnittstelle bzgl. *remote exploits*
- geschütztes Netz für Updates
- Offline-Update

nie: Rechnernutzung (Surfen) vor Windows-Update!

Idee

Windows XP-*SP2* installieren, Netz nur über Filter/ICF

Ablauf

1. Netzwerkkabel abziehen
2. gleich unnötige Netzwerkdienste/-protokolle weglassen
3. zumindest während Installation Netbios deaktivieren
4. TCP/IP-Filter setzen ($\neq$ ICF = Windows-Firewall),
   d.h. *stateless* Paketfilter auf Ports, nicht Quelle/Ziel
5. nach Neustart und ca. 30 s Netzwerkkabel anschließen
6. Windows-Update aufrufen & durchführen (evt. über WSUS)

Ausführliche, schrittweise Anleitung des ZIV der Univ. Münster,
$\longrightarrow$ `http://www.rrzn.uni-hannover.de/its_windows_xp.html`

Institutsnetz mit Institutsfirewall

- sicher vor dem Internet
- Institutsrechner müssen aber verlässlich virenfrei sein,
  das ist nie zu gewährleisten → Restrisiko

Installationsnetz

- während Installation vor den Rechner geschaltete Firewall
- billig umsetzbar mit einfachem Natting-Router
- Netz muss klein bleiben,
  uniweites Installationsnetz wäre nicht praktikabel

R|R|Z|N

Slipstreaming

Begriff für das Integrieren von Service-Packs, Hotfixes, Patches in Installationsmedien (Windows, MS-Office)

Vorgehen

1. Kopieren der Installations-CD auf Festplatte
2. Herunterladen der Fixes
3. Slipstreaming: Fix-Aufruf mit Parameter `/integrate:`*Pfad*
4. CD-Image-Erzeugung, dabei CD-Boot konfigurieren
5. neue Installations-CD brennen und davon installieren

alternativ: Tools verwenden, z.B. nLite

R|R|Z|N

Slipstreaming

Vorteil

- Keine Installation mit alten Dateien, gleich aktueller Stand
- Installationsmedium ohne Zusatzmaßnahmen abgesichert
- gut für Service-Packs
- Tools haben häufig Zusatznutzen

Nachteil

- Integration von Hotfixes kann spätere Updates stören
- für Hotfixes und Patches wegen Anzahl unübersichtlich, manuelles Zusammensuchen der notwendigen Fixes
- ohne Tools aufwändige Handarbeit

R|R|Z|N

Update-CD

- von der GWDG gepflegtes CD-Image für Offline-Updates, basierend auf c't-Projekt Offline-Update
- für Windows-2000 und XP, getrennte CDs für deutsch / englisch
- keine Unterstützung für Windows 2003
- einfach `\ctupdate\update.cmd` von CD starten, das aber nach jedem (erforderlichen) Neustart

⟶ `http://www.rrzn.uni-hannover.de/its_windows_xp.html`
`ftp://ftp.rrzn.uni-hannover.de/pub/uni-intern/Sicherheit/`

- als Windows-Dienst installierbar ⟵ statt Remote-Desktop
- neben Tastatur-/Bildschirmübernahme auch Chat, Filetransfer
- nativer Windows-Client und Java-Client
- Authentifizierung verschlüsselt,
  separates VNC-Passwort oder Windows-Login
- Encryption Plug-Ins (nicht für Java) ⟵ wünschenswert
  - symmetrische Schlüssel (MSRC4)
  - PKI-basiertes, asymmetrisches SSL im Beta-Test
- zusätzliche Add-Ons
  - Proxies: Repeater, Nat-to-Nat ⟵ bei Firewall-Problemen
  - UltraVNC SingleClick: Mini-Server für Hotline
    ⟵ statt Remote-Unterstützung

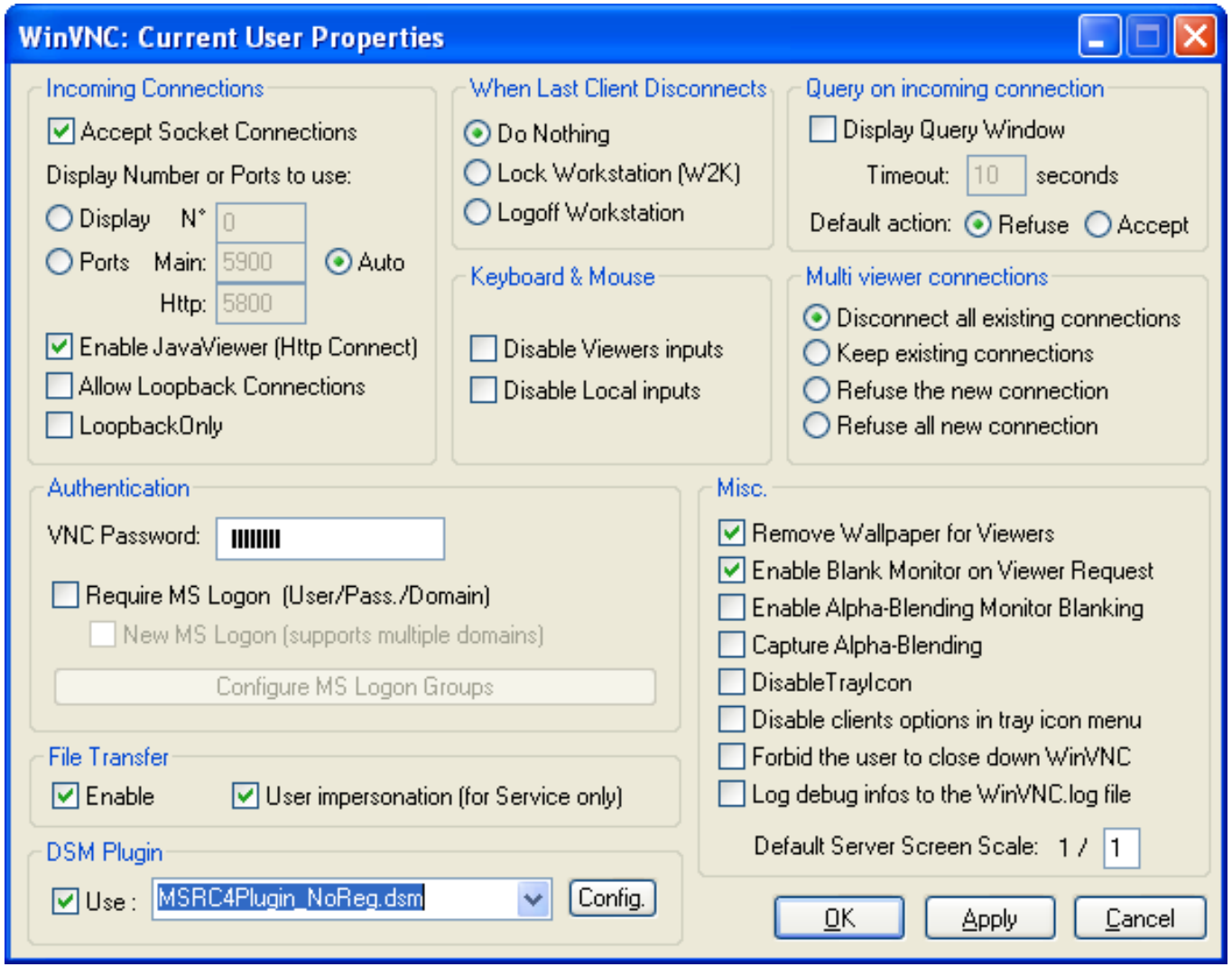
⟶ `http://ultravnc.sourceforge.net/`

Fernwartung

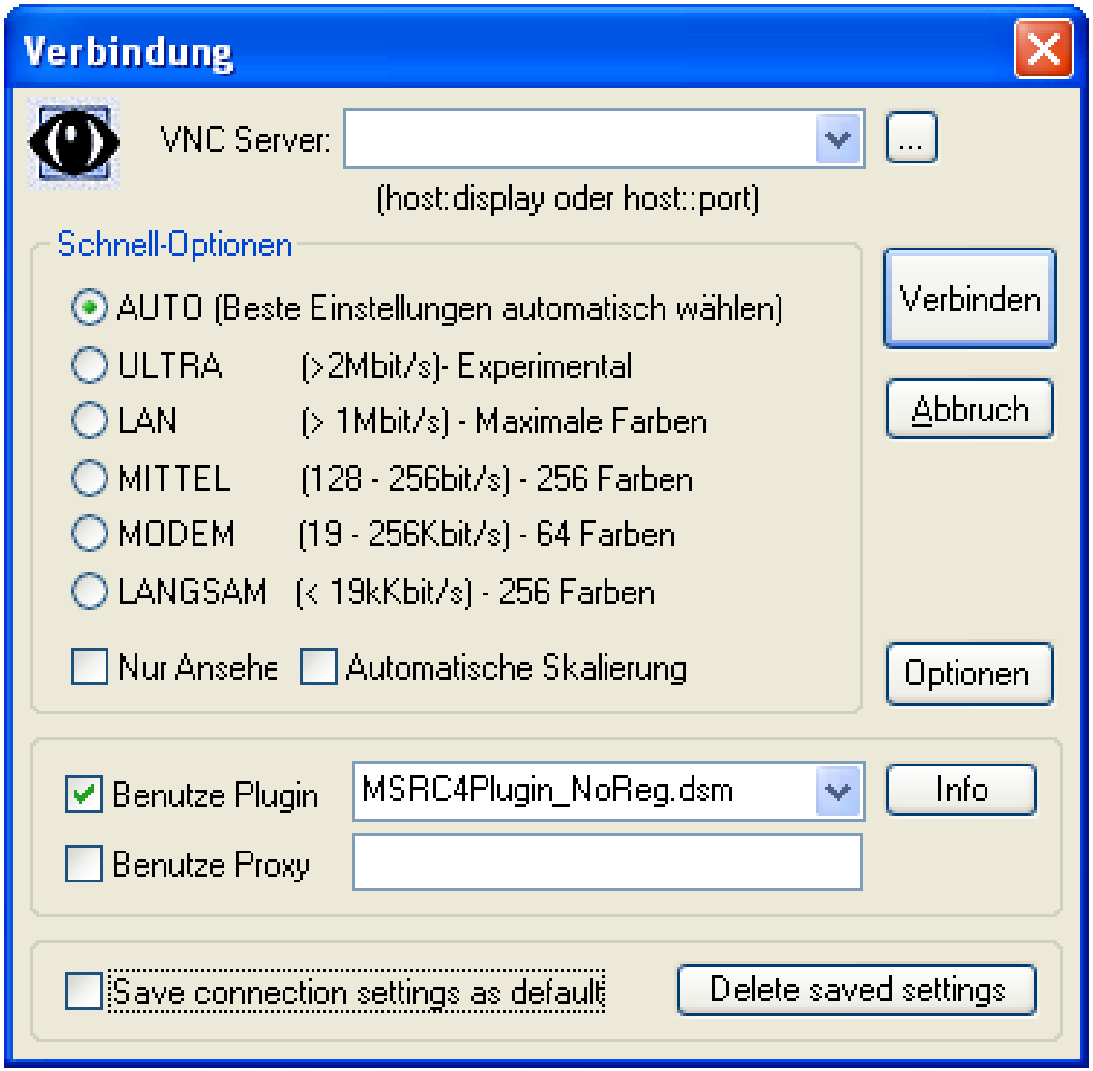
- Installation über Installer
- Installer bietet Auswahl:
  - Komponenten (z.B. DSM-Plugin für Verschlüsselung)
  - Einbindung als Service
- Schutz durch VNC-Passwort und zusätzlich
- Windows-Login, einschränkbar auf Gruppen
- MSRC4-Plugin manuell einbinden
  - `*.dsm` aus Unterverzeichnis `plugin` ins Programmverzeichnis verschieben
  - in Konfiguration des Servers auswählen & konfigurieren

symmetrischer Key separat erstellbar oder per PW-Hash

Server


WinVNC: Current User Properties
Incoming Connections
Accept Socket Connections
Display Number or Ports to use:
Display N° 0
Ports Main: 5900
Auto
Http: 5800
Enable JavaViewer (Http Connect)
Allow Loopback Connections
LoopbackOnly
When Last Client Disconnects
Do Nothing
Lock Workstation (W2K)
Logoff Workstation
Keyboard & Mouse
Disable Viewers inputs
Disable Local inputs
Query on incoming connection
Display Query Window
Timeout: 10 seconds
Default action: Refuse Accept
Multi viewer connections
Disconnect all existing connections
Keep existing connections
Refuse the new connection
Refuse all new connection
Authentication
VNC Password:
Require MS Logon (User/Pass./Domain)
New MS Logon (supports multiple domains)
Configure MS Logon Groups
File Transfer
Enable
User impersonation (for Service only)
DSM Plugin
Use :
MSRC4Plugin_NoReg.dsm
Config.
Misc.
Remove Wallpaper for Viewers
Enable Blank Monitor on Viewer Request
Enable Alpha-Blending Monitor Blanking
Capture Alpha-Blending
DisableTrayIcon
Disable clients options in tray icon menu
Forbid the user to close down WinVNC
Log debug infos to the WinVNC.log file
Default Server Screen Scale: 1 / 1
OK
Apply
Cancel

Client


Verbindung
VNC Server:
...
(host:display oder host::port)
Schnell-Optionen
AUTO (Beste Einstellungen automatisch wählen)
ULTRA (>2Mbit/s)- Experimental
LAN (> 1Mbit/s) - Maximale Farben
MITTEL (128 - 256bit/s) - 256 Farben
MODEM (19 - 256Kbit/s) - 64 Farben
LANGSAM (< 19kKbit/s) - 256 Farben
Nur Ansehe
Automatische Skalierung
Verbinden
Abbruch
Optionen
Benutze Plugin
MSRC4Plugin_NoReg.dsm
Info
Benutze Proxy
Save connection settings as default
Delete saved settings

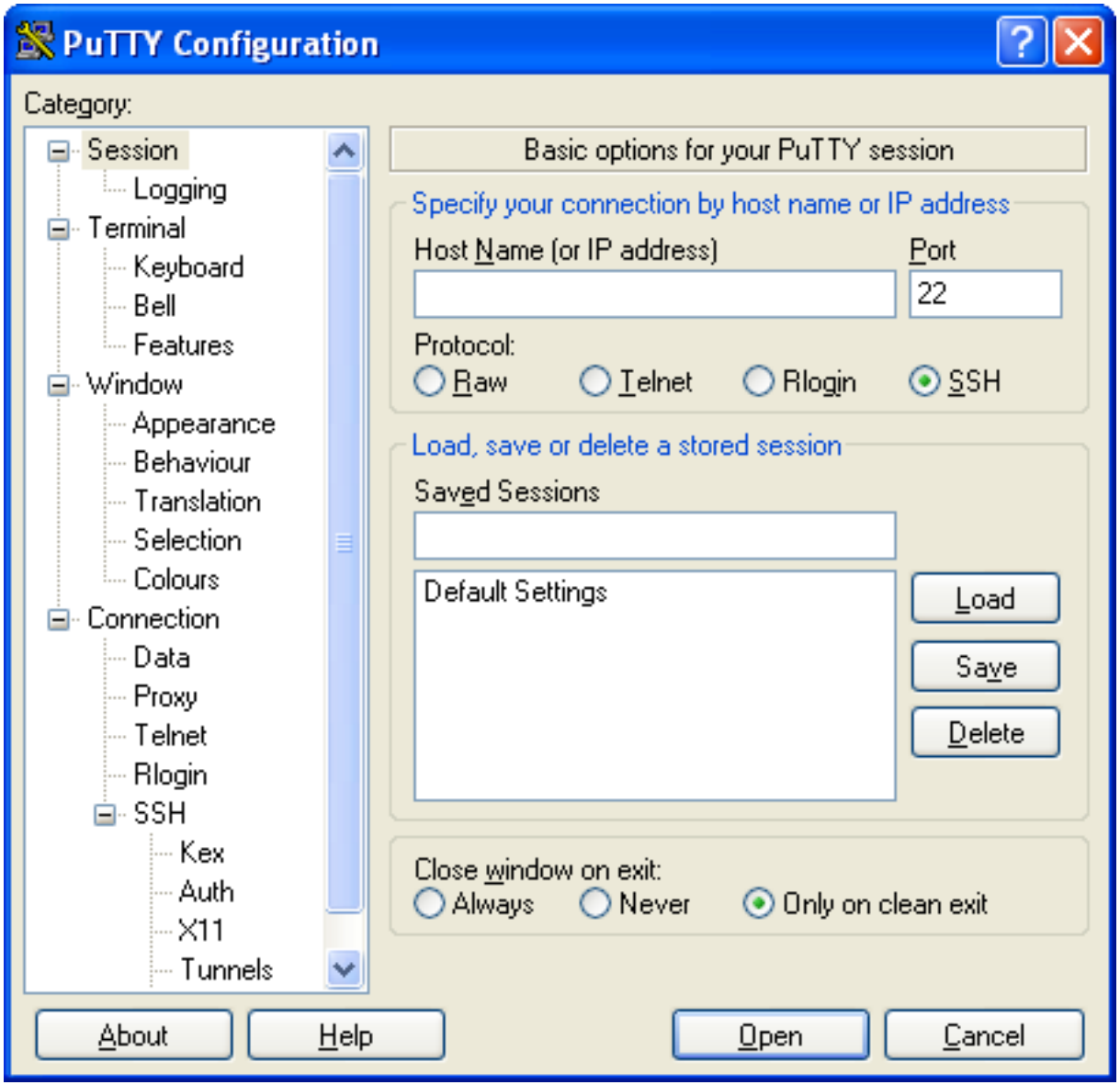
Hotline

- mit UltraVNC-SingleClick
- vorkonfigurierbare `.exe`-Datei
- typische Anwendung:
  1. Kunde hat Problem
  2. Kunde lädt vorbereitete UltraVNC-SC`.exe`-Datei von einer Support-Webseite und startet diese
  3. UltraVNC-SC (d.h. der VNC-Server) verbindet sich aktiv mit VNC-Viewer des Support-Mitarbeiters
     - Firewall auf Kundenseite dabei meist kein Problem
     - Kunde baut bewusst & gezielt Verbindung auf
  4. Kunde kann sehen, was Support tut (konfigurierbar)
  5. Support löst alle Probleme ...

Putty-SSH

- Telnet- und SSH-Client für Windows (und Unix)
- Open-Source (MIT-Lizenz)
- Windows-Installer
- skriptfähig durch `plink.exe`
- sftp-Unterstützung mit `psftp.exe`,
  aber nicht grafisch, ggf. separat mit WinSCP
- Public-/Private-Keys:
  - Keygenerierung mit `puttygen.exe`
  - Keyaustausch mit OpenSSH und ssh.com möglich
  - SSH-Agent: `pageant.exe`

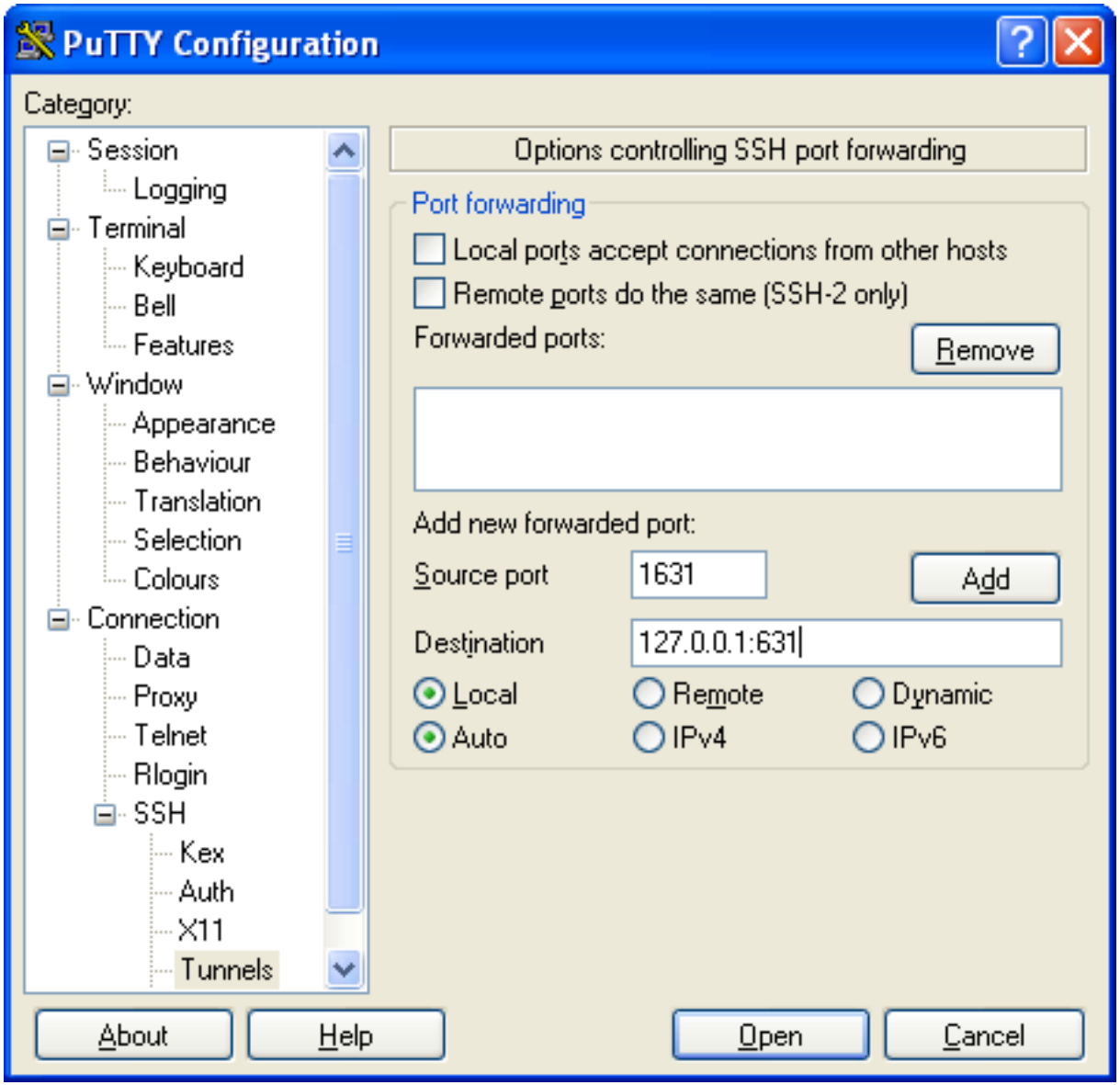
⟶ `http://www.chiark.greenend.org.uk/~sgtatham/putty/`


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Auth
X11
Tunnels
Basic options for your PuTTY session
Specify your connection by host name or IP address
Host Name (or IP address)
Port
22
Protocol:
Raw
Telnet
Rlogin
SSH
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel

Putty-SSH Tunnel

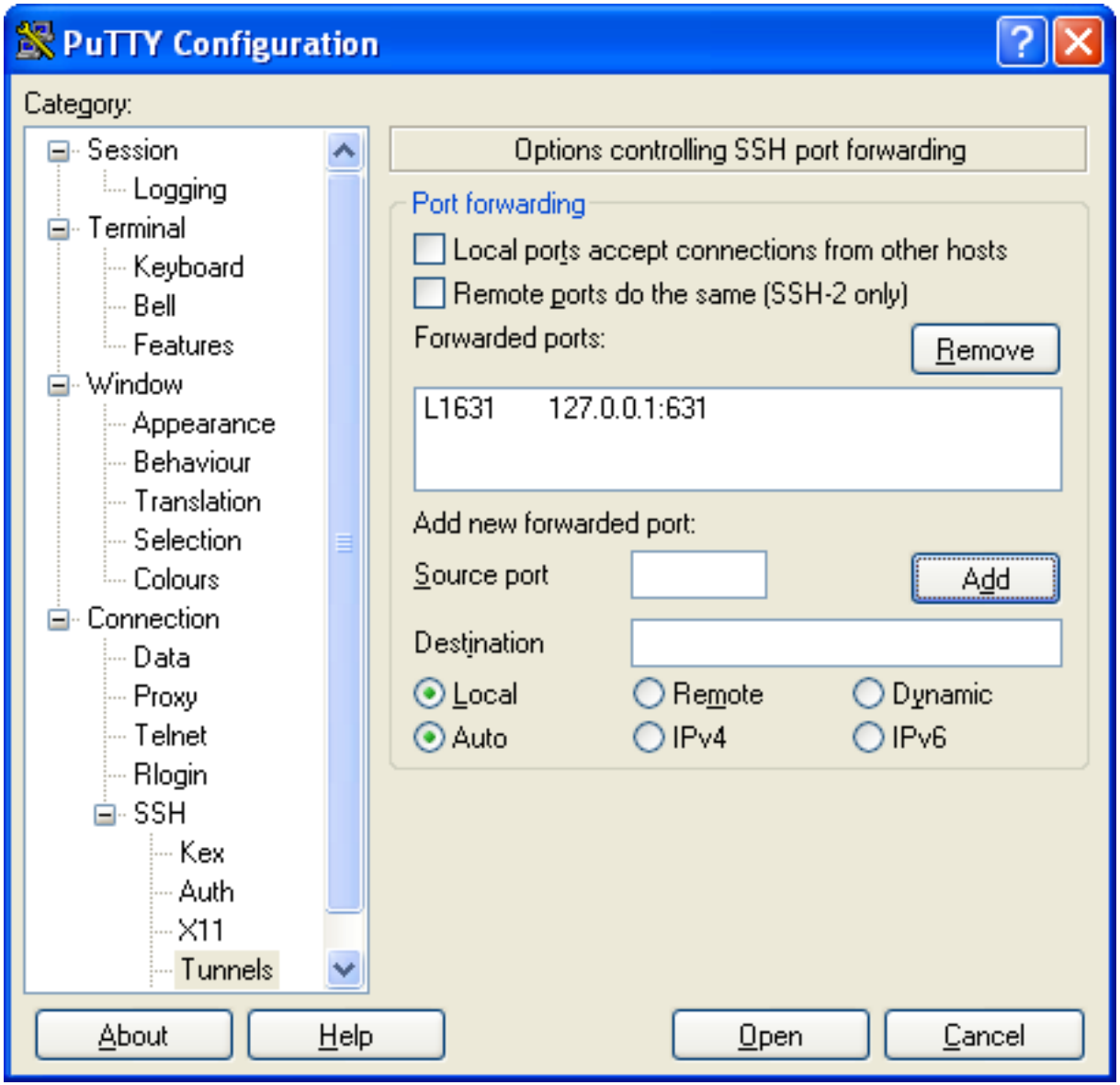
Local-Port-Forwarding

Cups danach auf Windows-Client per URL `127.0.0.1:1631/`



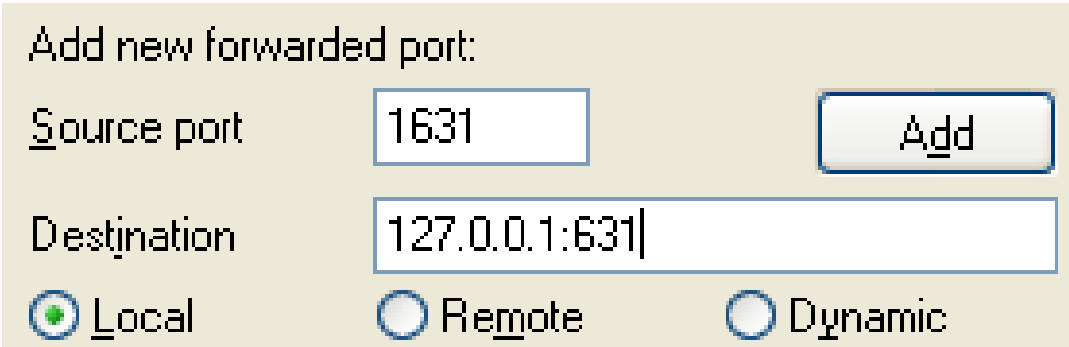
Local-Port-Forwarding

Cups danach auf Windows-Client per URL `127.0.0.1:1631/`



bei OpenSSH:

`-L1631:127.0.0.1:631`



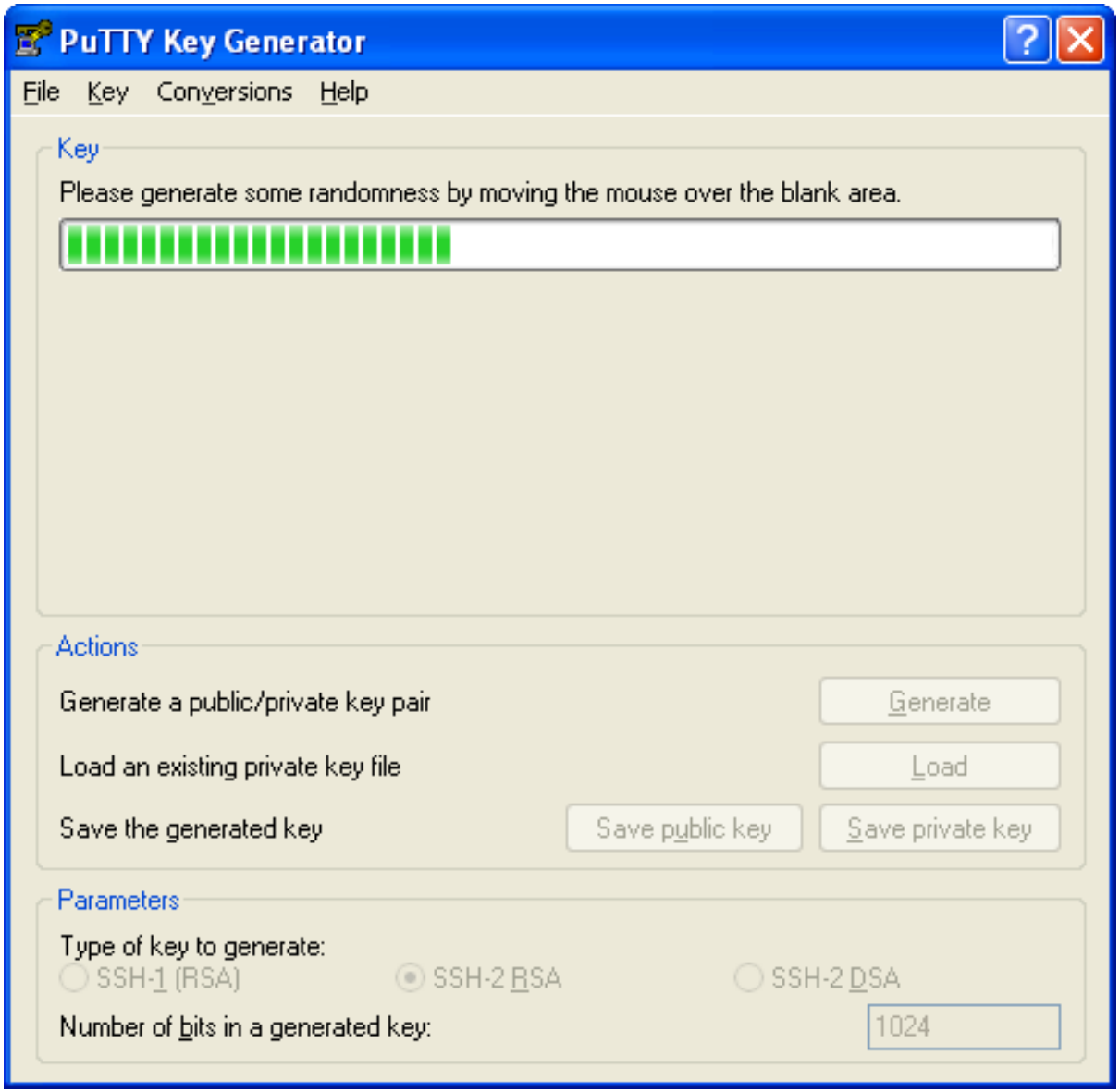
- `Source port`: Port, zu dem ein Programm verbindet, Putty lauscht an diesem Port als Daemon; bei `Local` auf Windows-Client, bei `Remote` auf SSH-Server
- `Destination`: auf Source-Port reinkommende Verbindung wird an Destination weiterverbunden, wo eigentlicher Daemon lauscht; Namensauflösung & Weiterverbindung bei `Local` von SSH-Server aus, bei `Remote` von Client aus
- `Local` = (Server-) Dienst zum Client bringen, `Remote` = (Client-) Dienst zum Server bringen

Putty-SSH Key

Schlüssel-

- Erzeugung
- Import

mit `puttygen.exe`



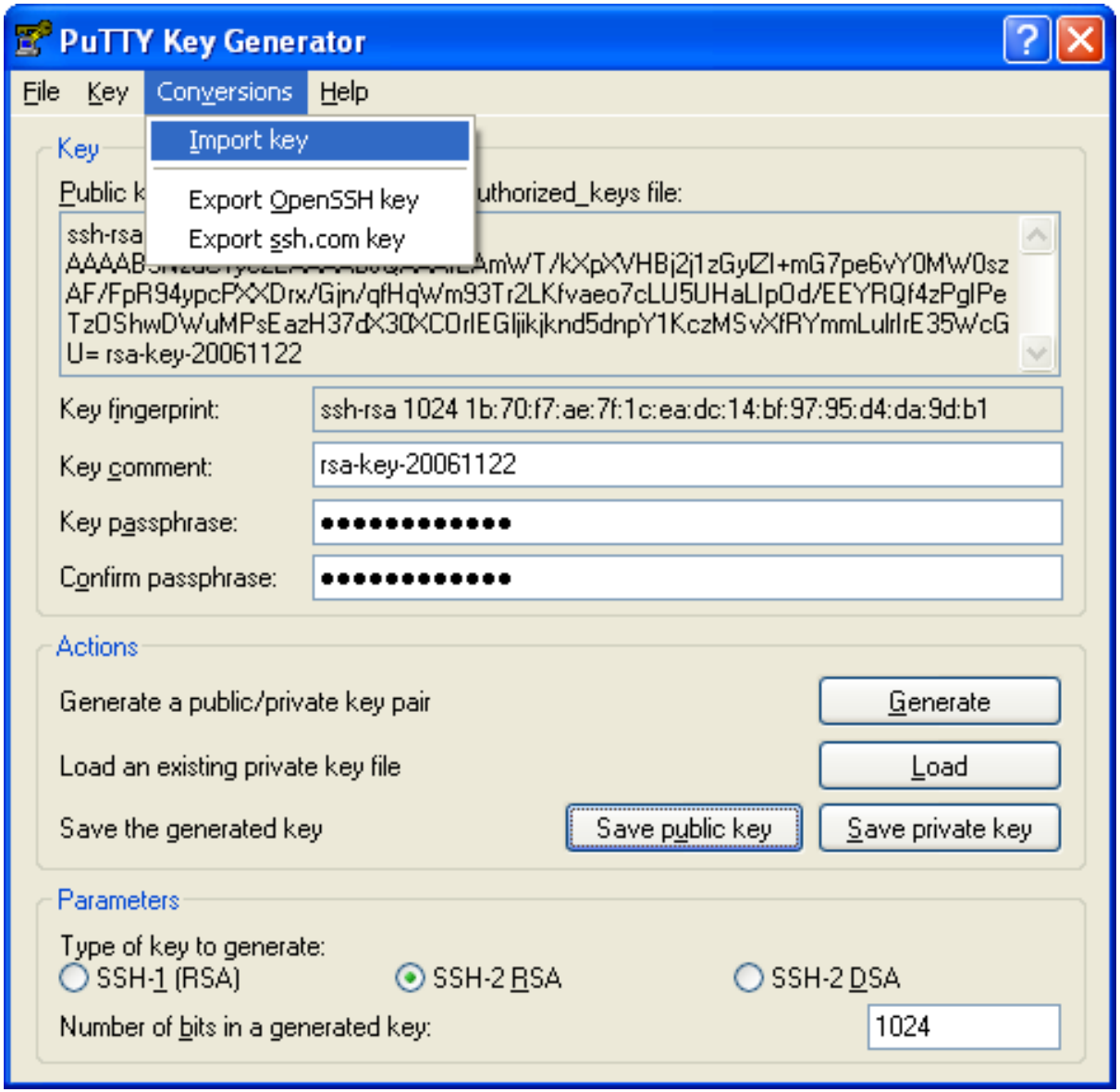
R|R|Z|N

Public-Key

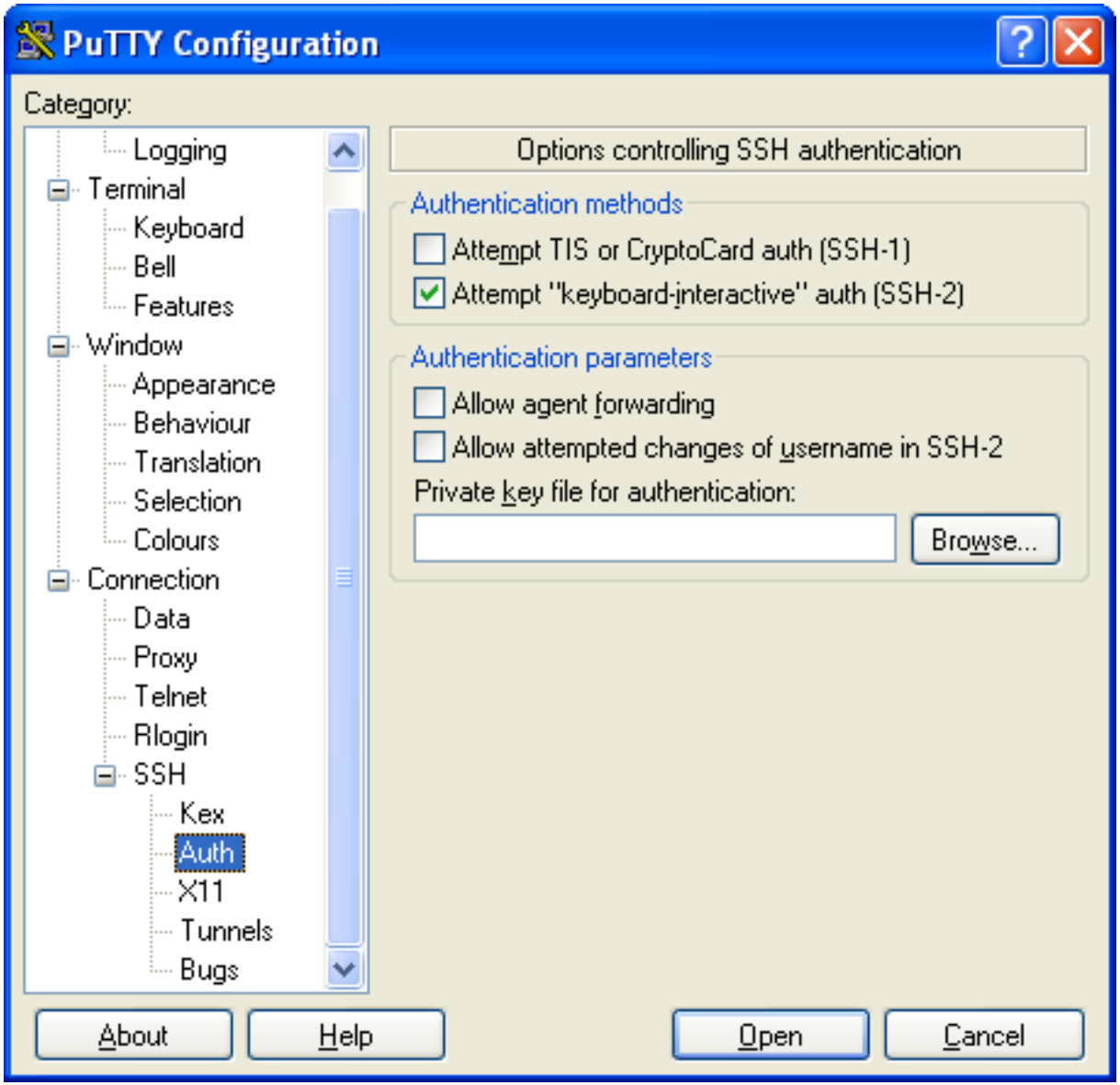
exportieren und auf Server als *authorized* einspielen

Private-Key

Passphrase setzen!

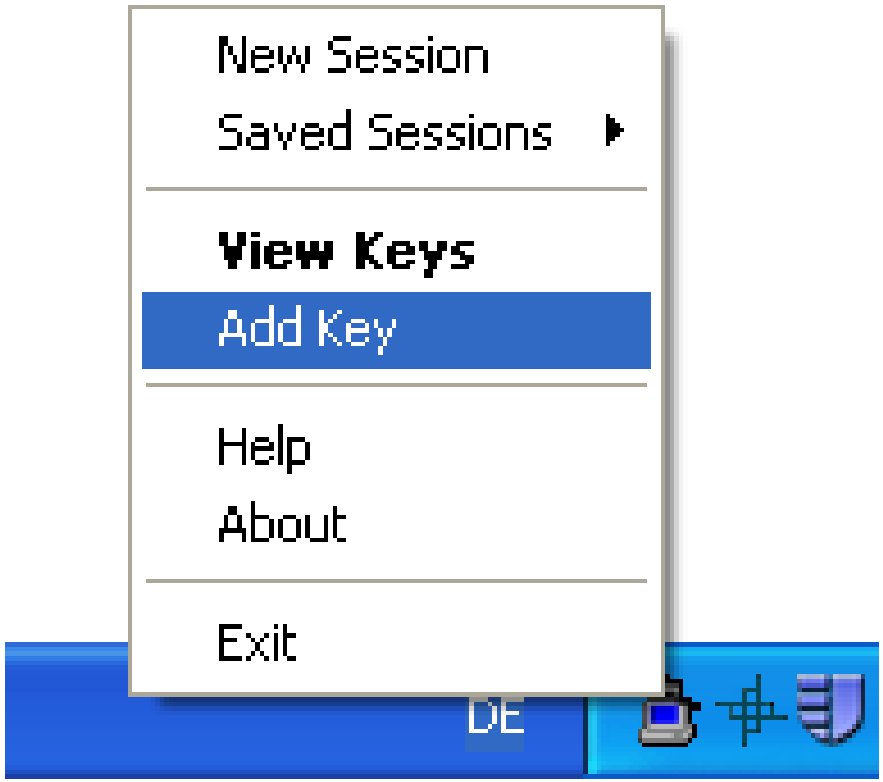


Private-Key zur Authentifizierung in `putty.exe` nutzen



`pageant.exe`

- ein SSH-Agent
- Key einmal laden, d.h. einmal mit Passphrase freischalten
- danach ohne Passphrase in `putty.exe`, `pscp.exe`, `psftp.exe` nutzen



R|R|Z|N

Windows-Firewall

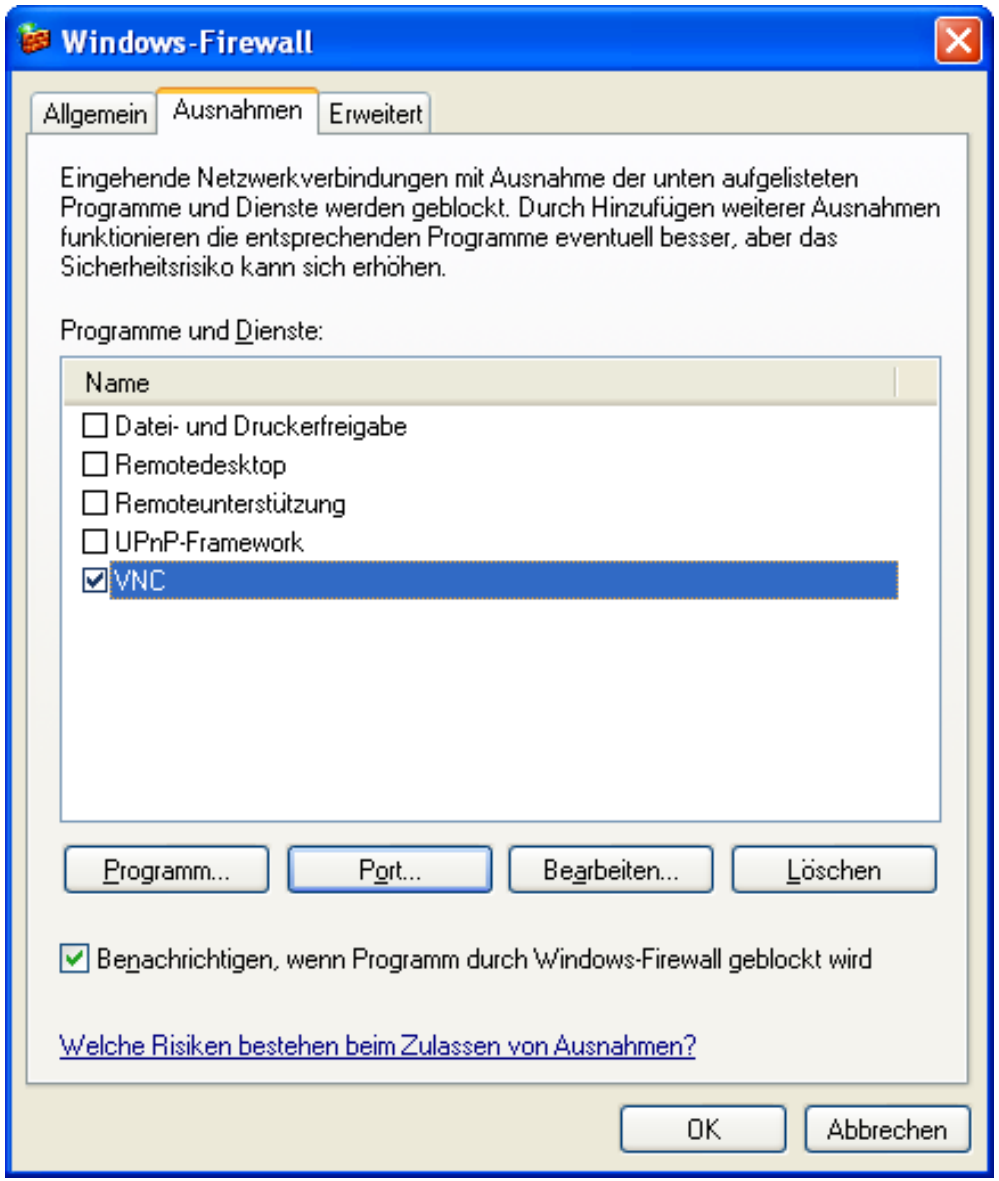
auch bezeichnet als ICF (Internet Connection Firewall)

- im Lieferumfang von Windows XP & 2003,
  bei XP standardmäßig aktiviert, bei 2003 zu tun
- einige Freischaltungen automatisch (z.B. Remote-Desktop)
- Ports auf Subnetze (IP-Adr./Netzmaske) einschränkbar
- steuerbar über Gruppenrichtlinien
- nur Filterung eingehender Verbindungen
  - das ist das Wichtigste
  - PFW-Nachfragen werden meist durch Nutzer bestätigt,
    eine Ablehnung ist ggf. schwer zu entfernen
  - lokale Prozesse können PFW umgehen

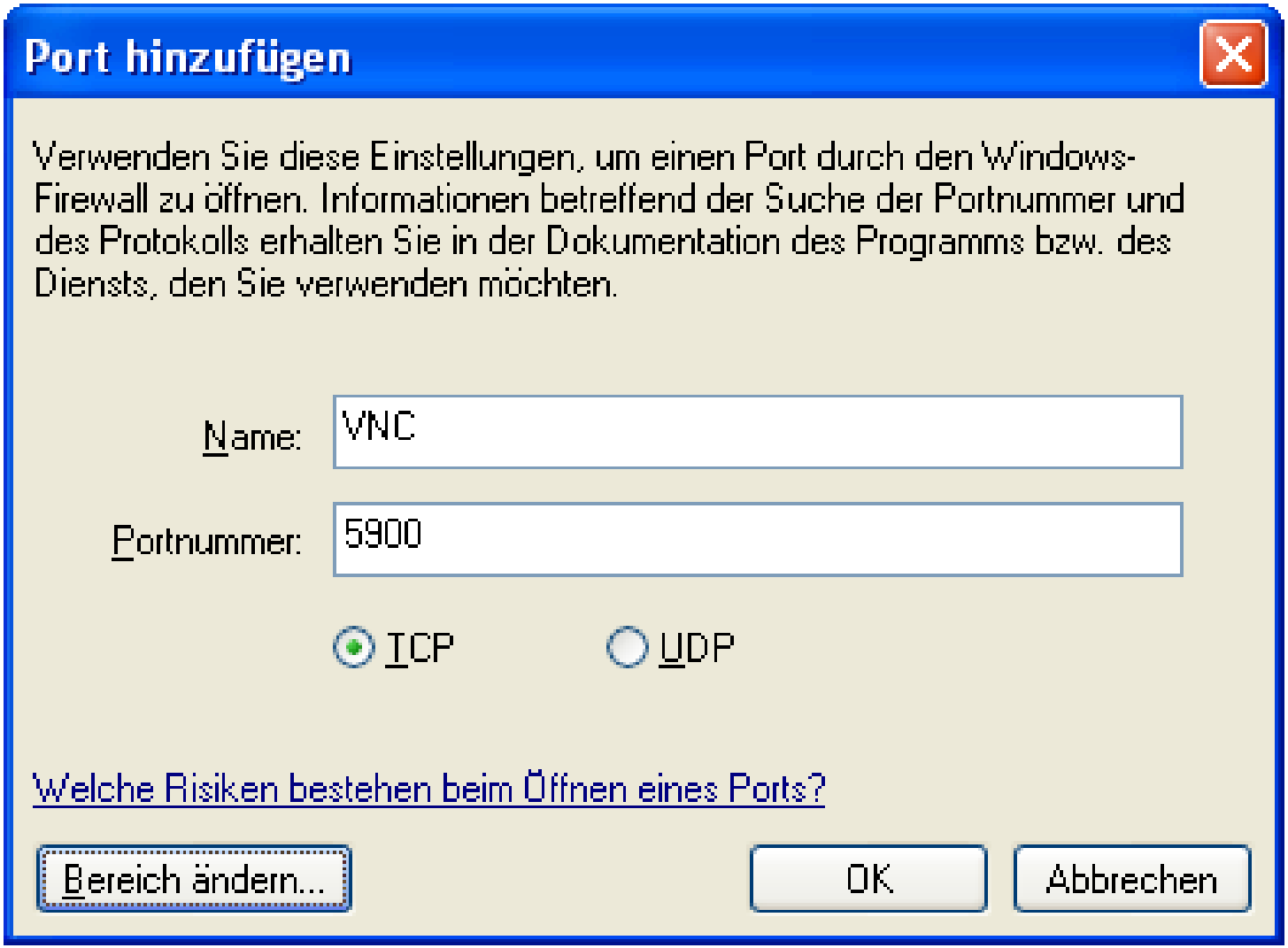
R|R|Z|N

Konfiguration

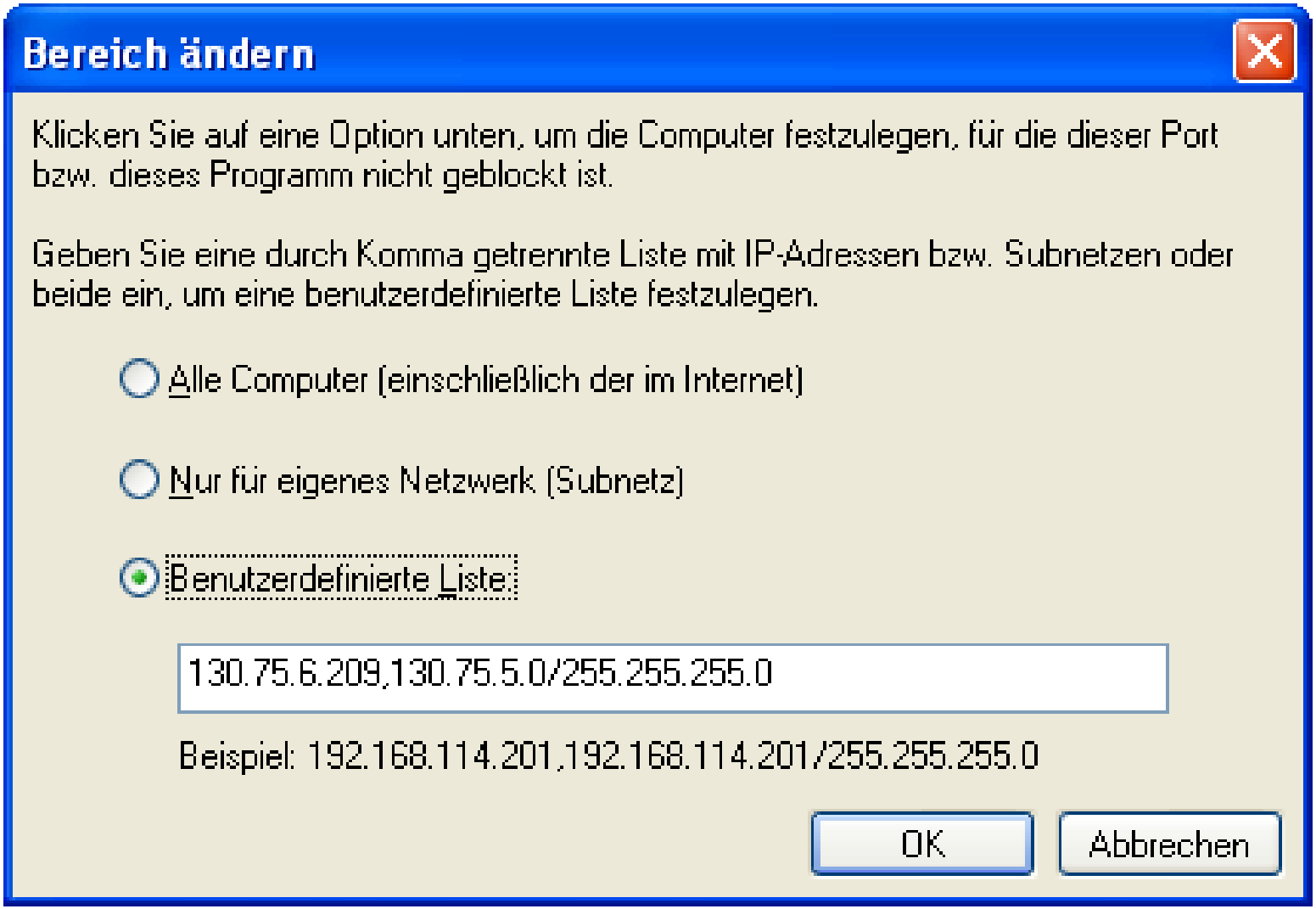
Aufruf z.B. über
Systemsteuerung /
Windows-Firewall



Konfiguration: Port hinzufügen



Konfiguration: IP-Adressen zulassen



Personal Firewall ab 2000: Core Force

R|R|Z|N

- auch für kommerzielle Nutzung freie Personal-Firewall für Windows 2000, XP
- basiert auf OpenBSD-PF
- Zugriff aufs Netz je nach Programm, Auswahl von vorgefertigten *security levels* und *policies* (z.B. für Programme) aus „*community*“
- erlaubt neben üblichem Lernmodus explizite Freigaben
- mehr als PFW: auch Datei- und Registryzugriffe
- Konfiguration über GUI, abgespeichert in *security profiles* (XML), damit gut zu verteilen; Konfiguration komplex, eher für zentrale Adminstration gedacht, dafür aber mächtig
- evt. Ersatz für fehlende ICF in Windows 2000 (nicht NT4, 98)

erste Tests vielversprechend, bisher *keine* Empfehlung des RRZN!

⟶ `http://force.coresecurity.com/`