Anleitung

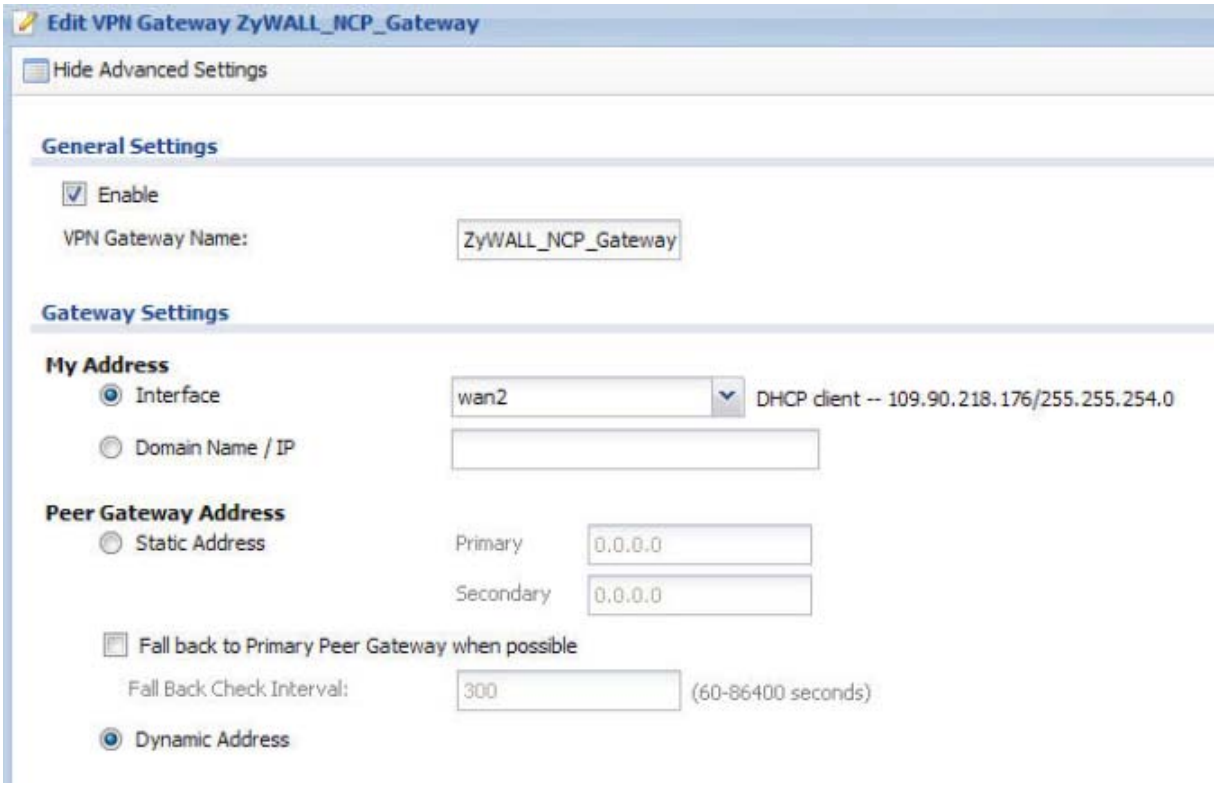
IPSec VPN zwischen ZyWALL USG und dem NCP Client

Autor: Marc Stefanski (ZyDE)

Datum: 14.01.2011

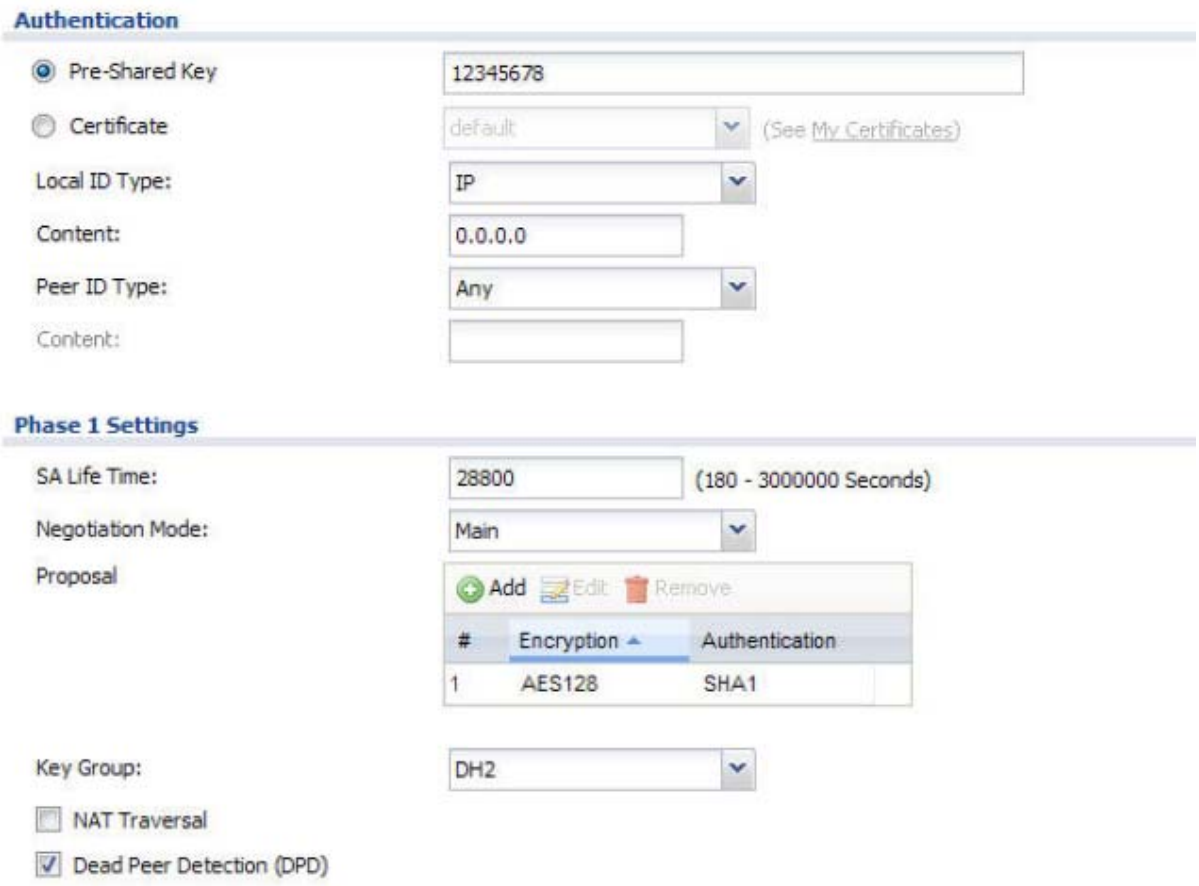
1. Einstellungen in der ZyWALL USG-200

Phase 1 Einstellungen



Bitte wählen Sie im Auswahlfeld „My Address – Interface“, Ihr WAN Interface aus, worüber dieser VPN Tunnel aufgebaut wird. Wichtig hierbei, sollte sich Ihre WAN IP Adresse ändern, sollten Sie im NCP Client und in der USG Firewall mit einem „dyndns account“ arbeiten.

Im Bereich „Peer Gateway Address“ wählen Sie bitte den Punkt „Dynamic Address“ aus, da hier ein dynamischer Tunnel erstellt wird und nicht immer die gleiche WAN IP Adresse als Gegenstelle vorhanden ist. „Static Address“ benötigen wir nur im Bereich „Side to Side VPN“.



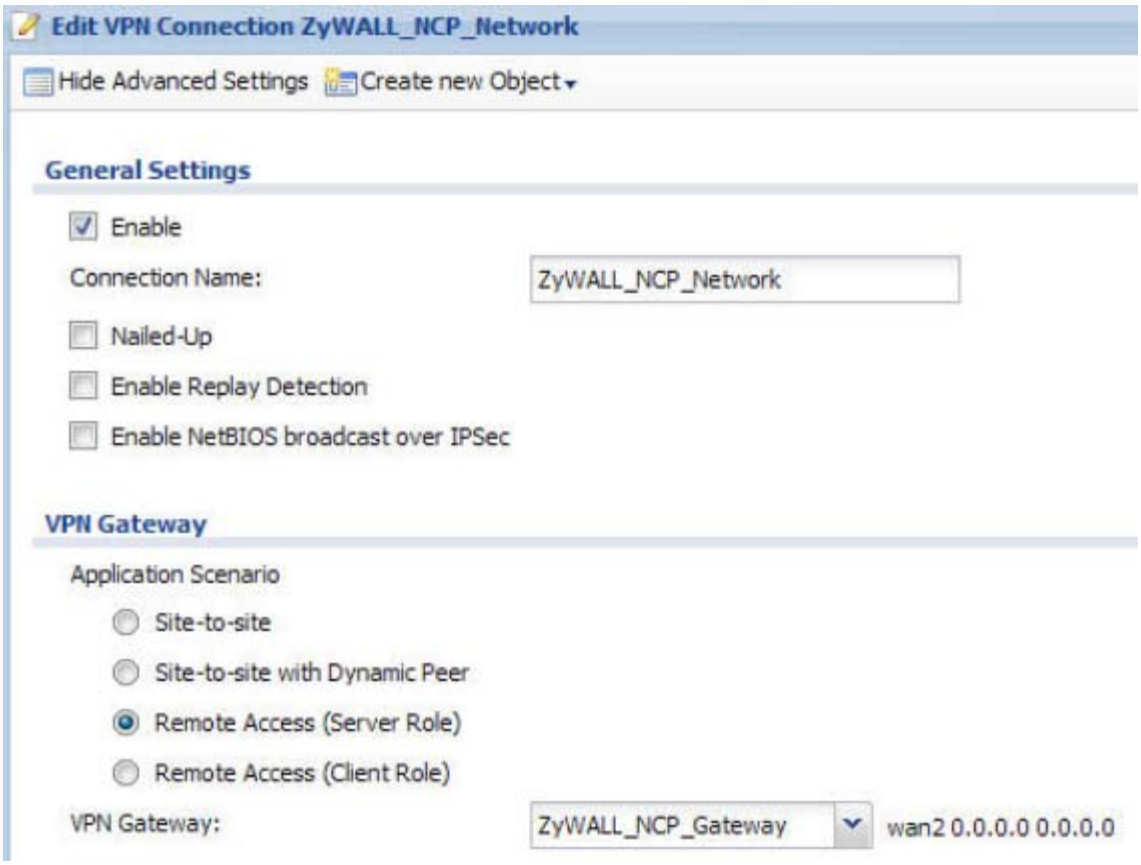
Um die Phase1 in der ZyWALL USG erfolgreich abzuschließen, benötigen wir nun als nächstes einen min. 8 stelligen PSK, den wir hinterher auch genauso im NCP Client eintragen müssen. !!Wichtig!! Sonderzeichen werden von der ZyWALL USG auch unterstützt. Bitte beachten Sie die Hinweise dazu in der WEB-Hilfe.

„Local & Peer ID“ lassen wir auf IP stehen und verwenden den Inhalt 0.0.0.0

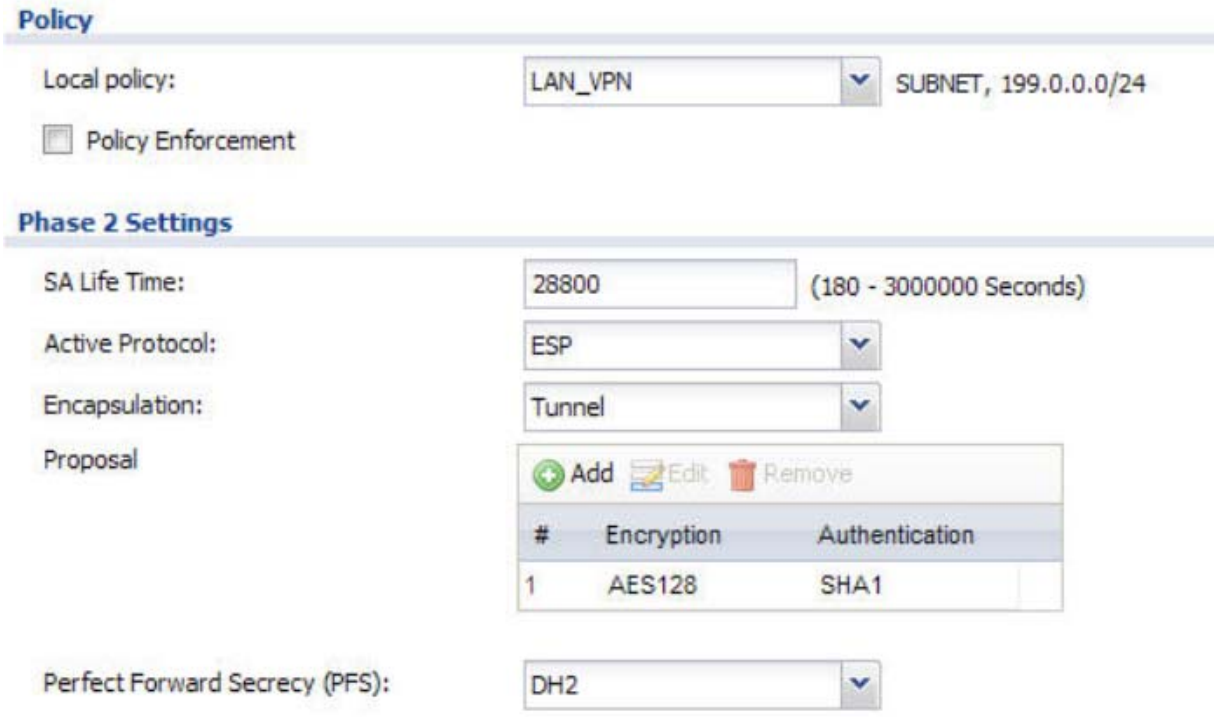
Die „SA Life Time“ setzen wir auf 28800 Sekunden. Bitte beachten Sie dass, sollten Sie einen anderen Wert verwenden, dass beide Seiten des VPN Tunnels, die gleichen „SA Life Time“ Einstellungen besitzen.

In den Phase1 Einstellungen verwenden wir den Main Mode und eine Verschlüsselung mit AES 128bit. Die „Authentication“ arbeitet sowohl in Phase1 als auch später in Phase2 mit SHA-1 und wir arbeiten mit DH2.

Phase 2 Einstellungen



Starten wir nun mit der Phase2 in der ZyWALL USG. Wichtig hierbei, Sie müssen der Phase2 eine Phase1 zu ordnen, deswegen sollte man immer erst die Phase1 anlegen und dann erst mit der Phase2 fortfahren.



Unter dem Punkt „Policy“ wählen wir das lokale Zielnetzwerk aus, auf dass später die NCP Clients zugreifen können.

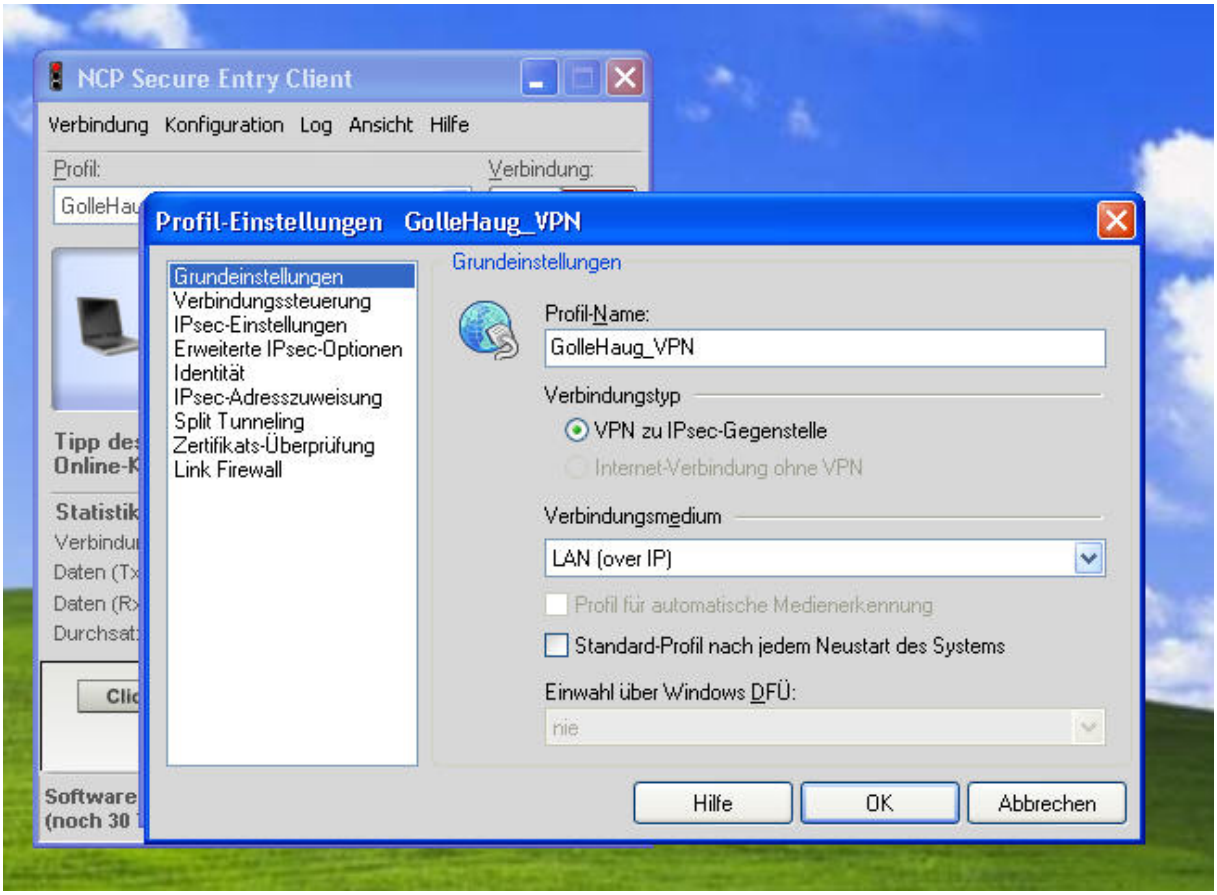
In den Phase2 Einstellungen legen wir wieder die „SA Life Time“ auf 28800sek. an und arbeiten mit ESP; Tunnel-Mode; AES128bit; SHA1 und DH2.

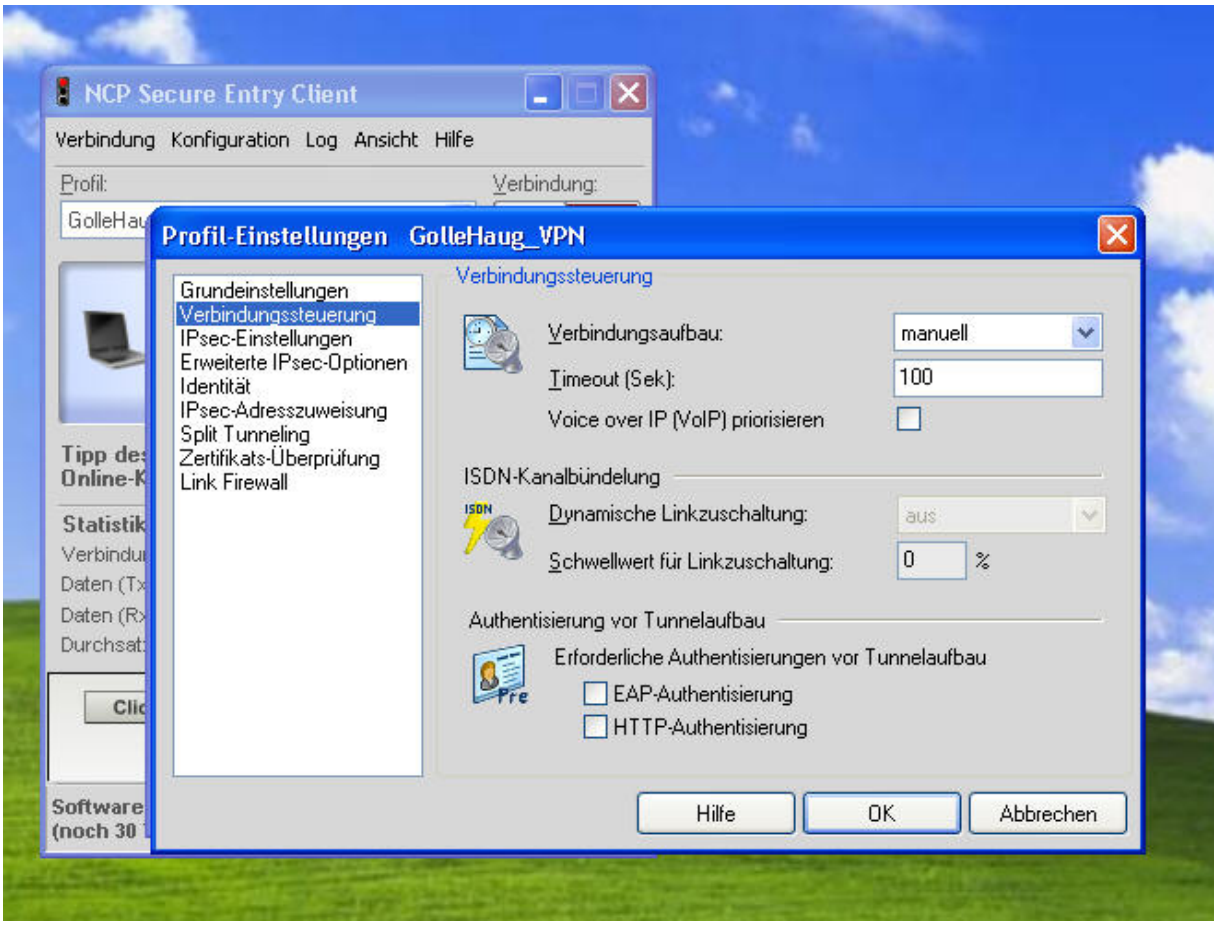
2. Einstellungen am NCP Client

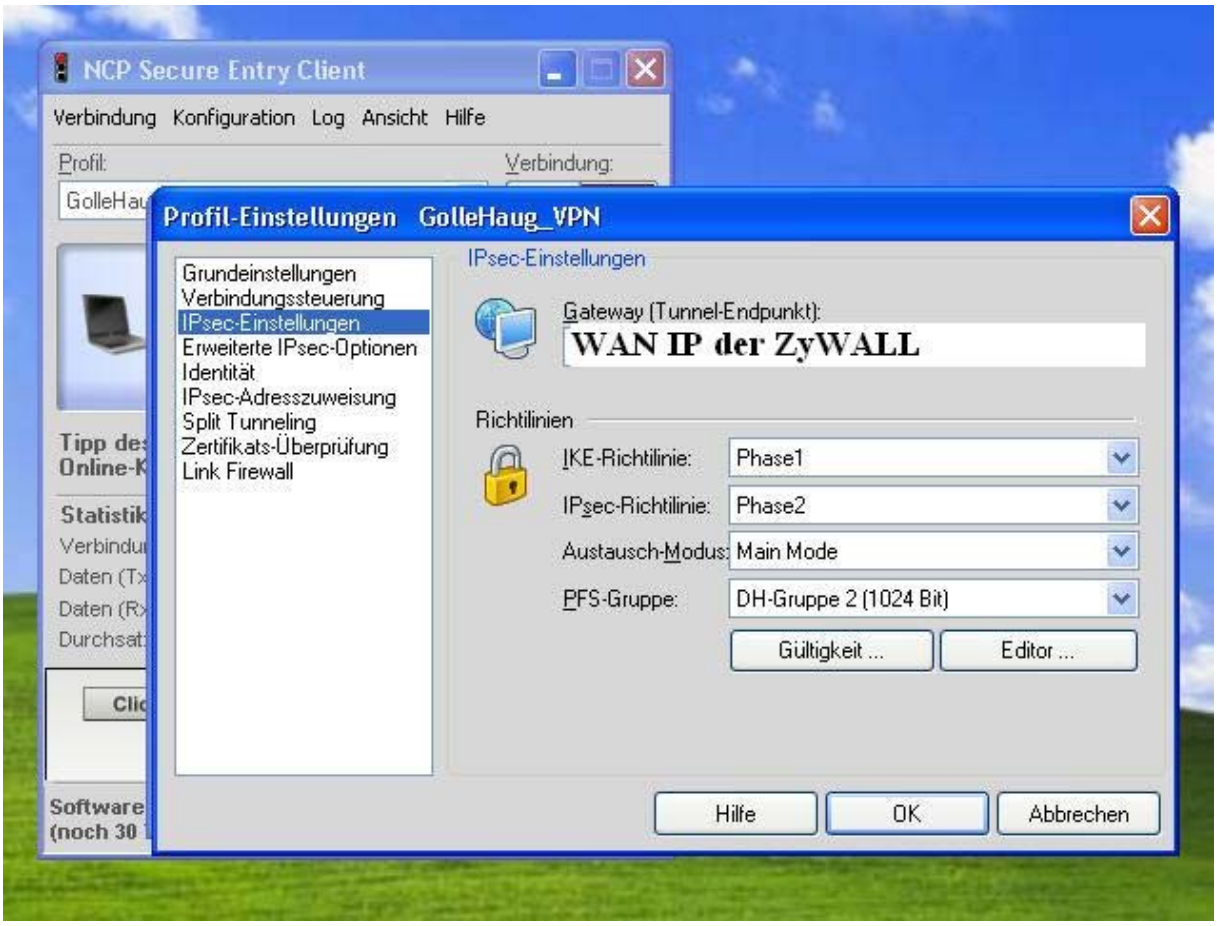
Auf den nun nachfolgenden Seiten, sehen Sie die Einstellungen, die am NCP Client notwendig sind, damit man erfolgreich einen IPSec Tunnel zwischen der ZyWALL USG und dem NCP Client aufbauen kann.

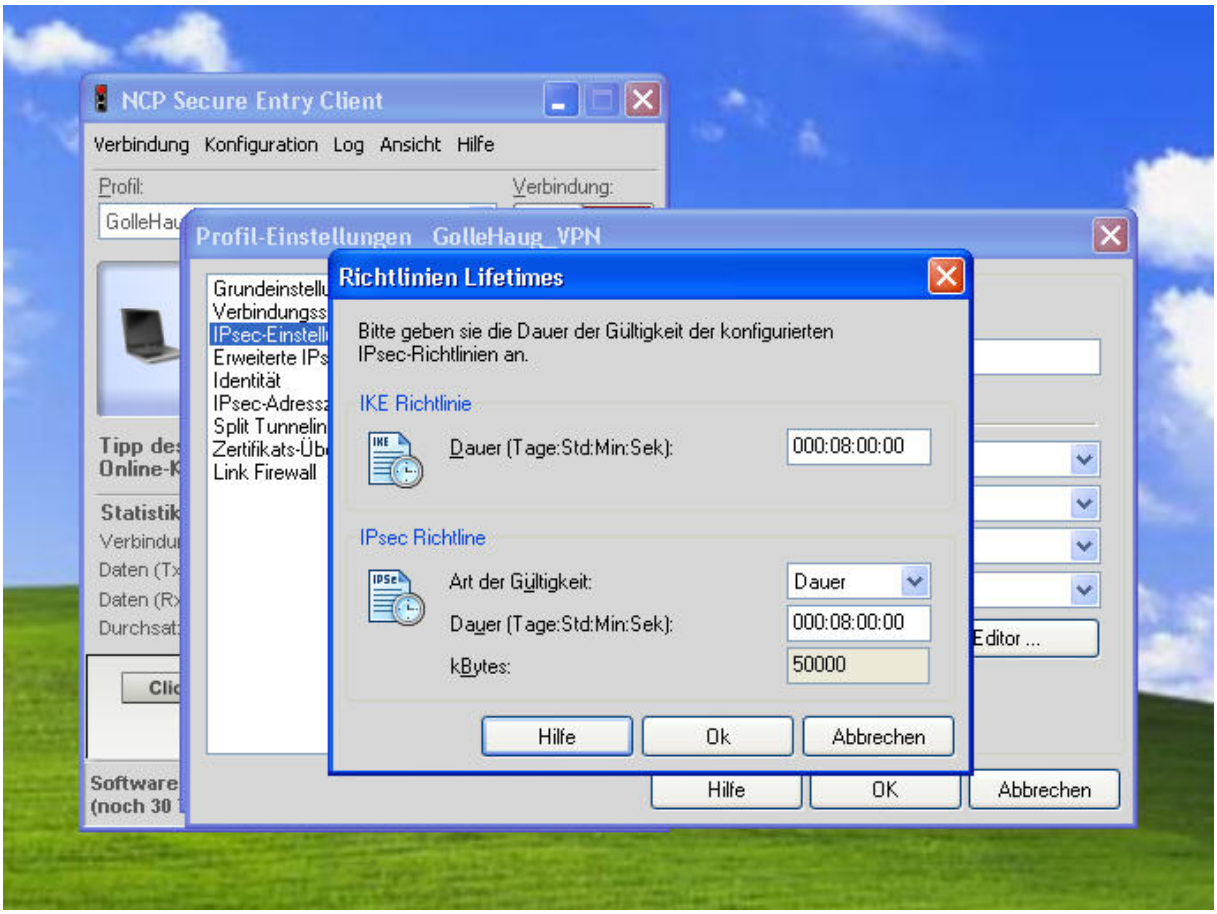
!!Wichtig!!

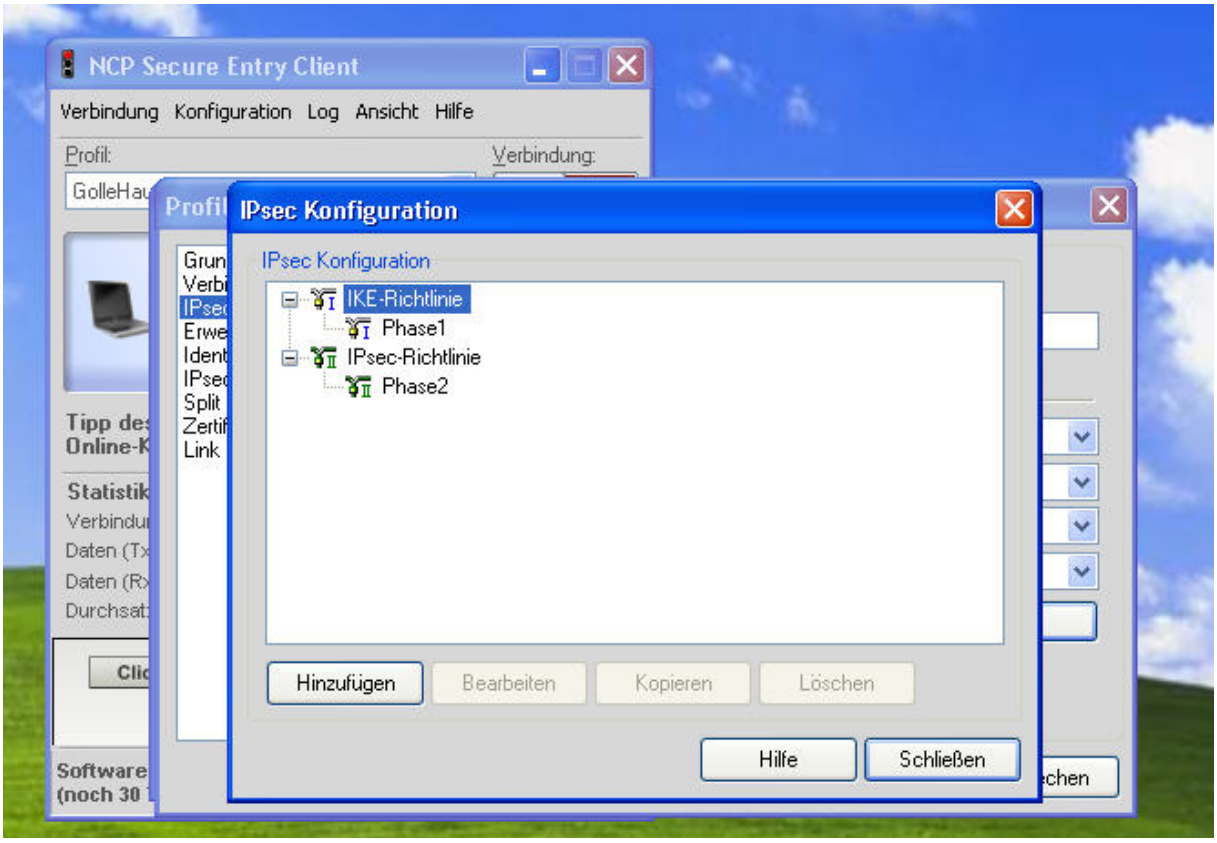
Auf dem Screenshot Nummer 10 wird mit einer virtuellen IP Adresse gearbeitet, damit der Client nicht die gleiche IP Adresse verwendet, wie das Zielnetzwerk.

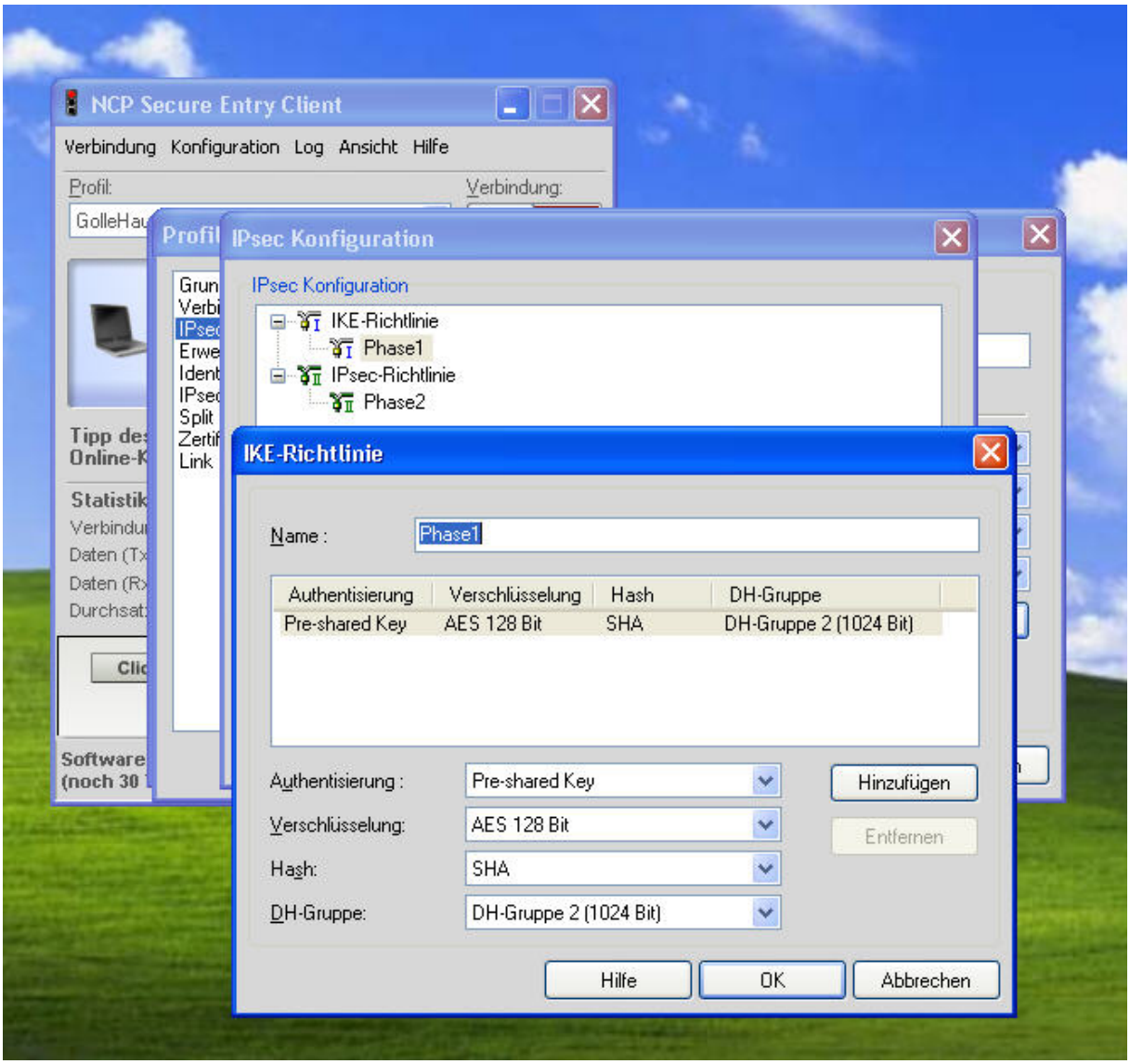


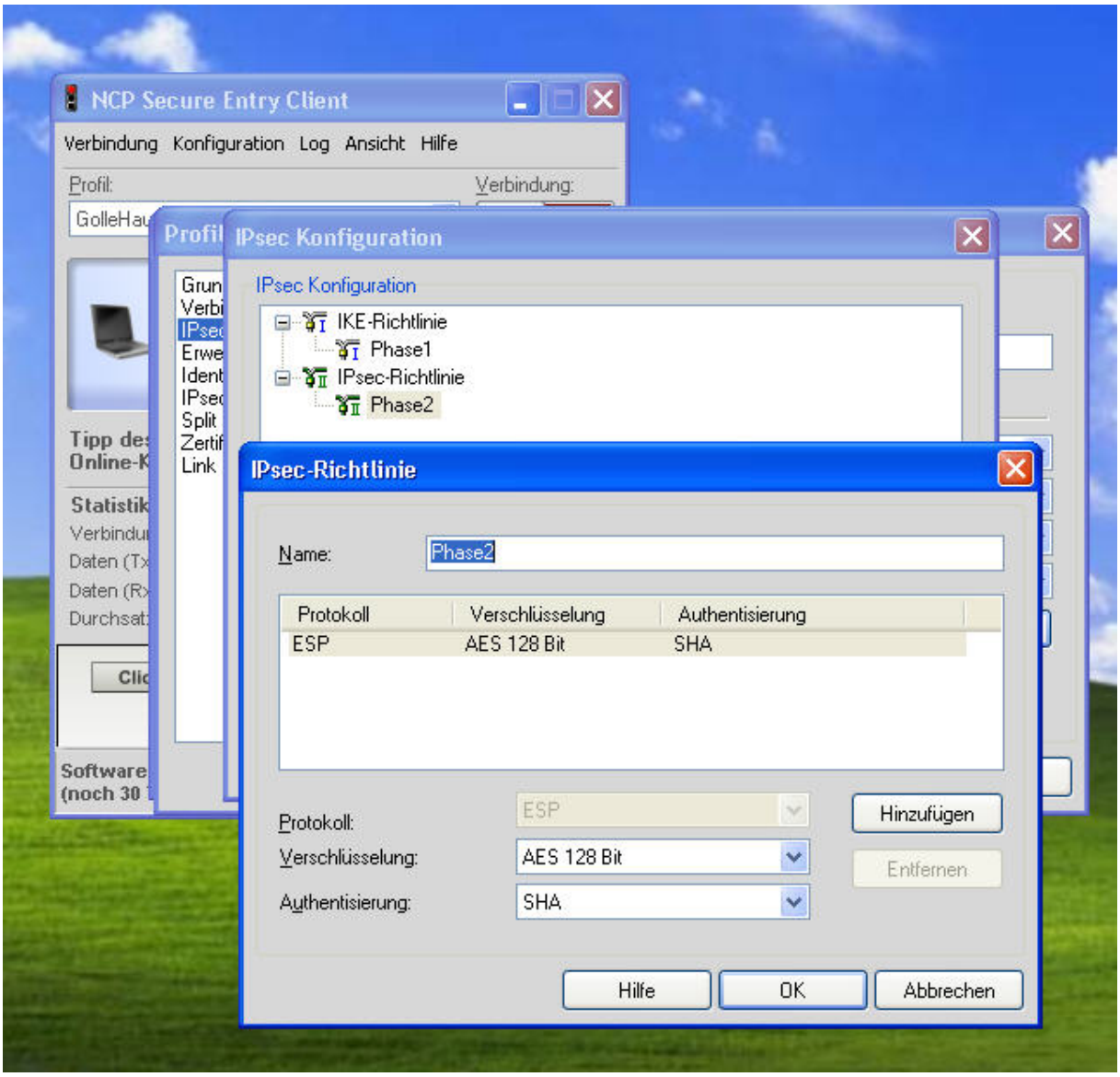

NCP Secure Entry Client
Verbindung Konfiguration Log Ansicht Hilfe
Profil:
Verbindung:
Profil-Einstellungen GolleHaug_VPN
Grundeinstellungen
Verbindungssteuerung
IPsec-Einstellungen
Erweiterte IPsec-Optionen
Identität
IPsec-Adresszuweisung
Split Tunneling
Zertifikats-Überprüfung
Link Firewall
Verbindungssteuerung
Verbindungsaufbau:
manuell
Timeout (Sek):
100
Voice over IP (VoIP) priorisieren
ISDN-Kanalbündelung
Dynamische Linkzuschaltung:
aus
Schwellwert für Linkzuschaltung:
0
%
Authentisierung vor Tunnelaufbau
Erforderliche Authentisierungen vor Tunnelaufbau
EAP-Authentisierung
HTTP-Authentisierung
Hilfe
OK
Abbrechen

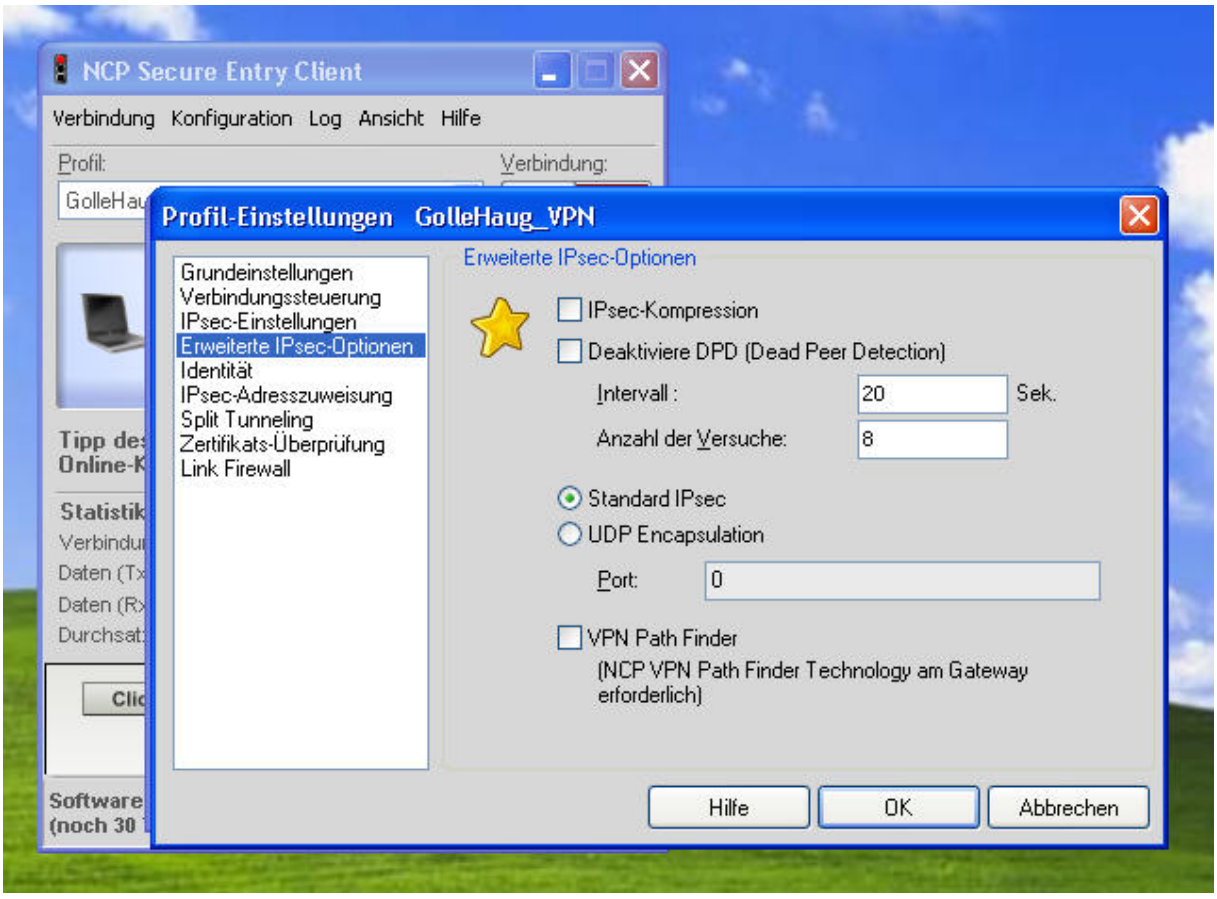

NCP Secure Entry Client
Verbindung Konfiguration Log Ansicht Hilfe
Profil:
Verbindung:
Profil-Einstellungen GolleHaug_VPN
Grundeinstellungen
Verbindungssteuerung
IPsec-Einstellungen
Erweiterte IPsec-Optionen
Identität
IPsec-Adresszuweisung
Split Tunneling
Zertifikats-Überprüfung
Link Firewall
IPsec-Einstellungen
Gateway (Tunnel-Endpunkt):
WAN IP der ZyWALL
Richtilinien
IKE-Richtilinie:
Phase1
IPsec-Richtilinie:
Phase2
Austausch-Modus:
Main Mode
PFS-Gruppe:
DH-Gruppe 2 (1024 Bit)
Gültigkeit ...
Editor ...
Hilfe
OK
Abbrechen

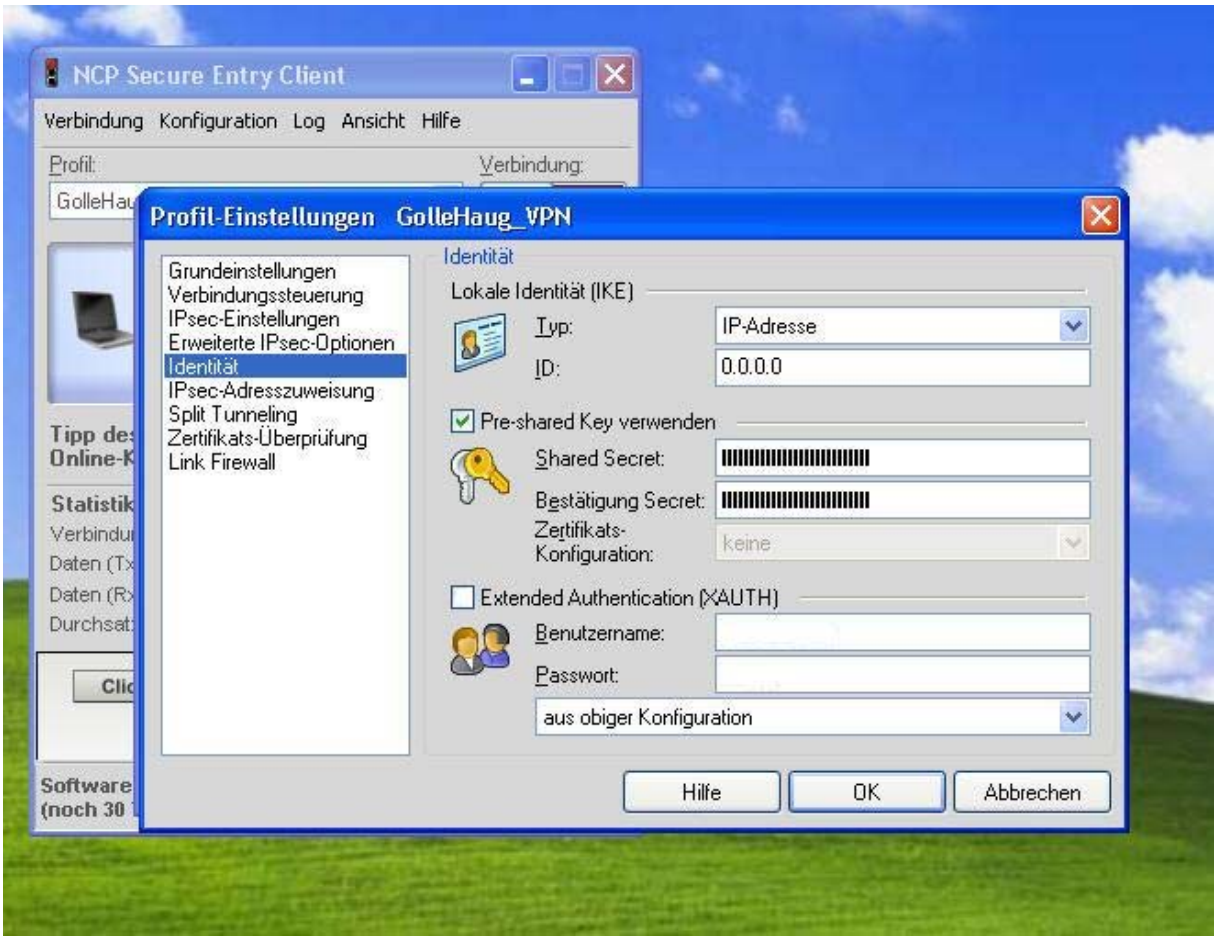

NCP Secure Entry Client
Verbindung Konfiguration Log Ansicht Hilfe
Profil:
Verbindung:
Profil-Einstellungen GolleHaug_VPN
Grundeinstellu
Verbindungss
IPsec-Einstell
Erweiterte IPs
Identität
IPsec-Adress
Split Tunnelin
Zertifikats-Üb
Link Firewall
Richtlinien Lifetimes
Bitte geben sie die Dauer der Gültigkeit der konfigurierten IPsec-Richtlinien an.
IKE Richtlinie
Dauer (Tage:Std:Min:Sek):
000:08:00:00
IPsec Richtline
Art der Gültigkeit:
Dauer
Dauer (Tage:Std:Min:Sek):
000:08:00:00
kBytes:
50000
Hilfe
Ok
Abbrechen
Editor ...
Hilfe
OK
Abbrechen

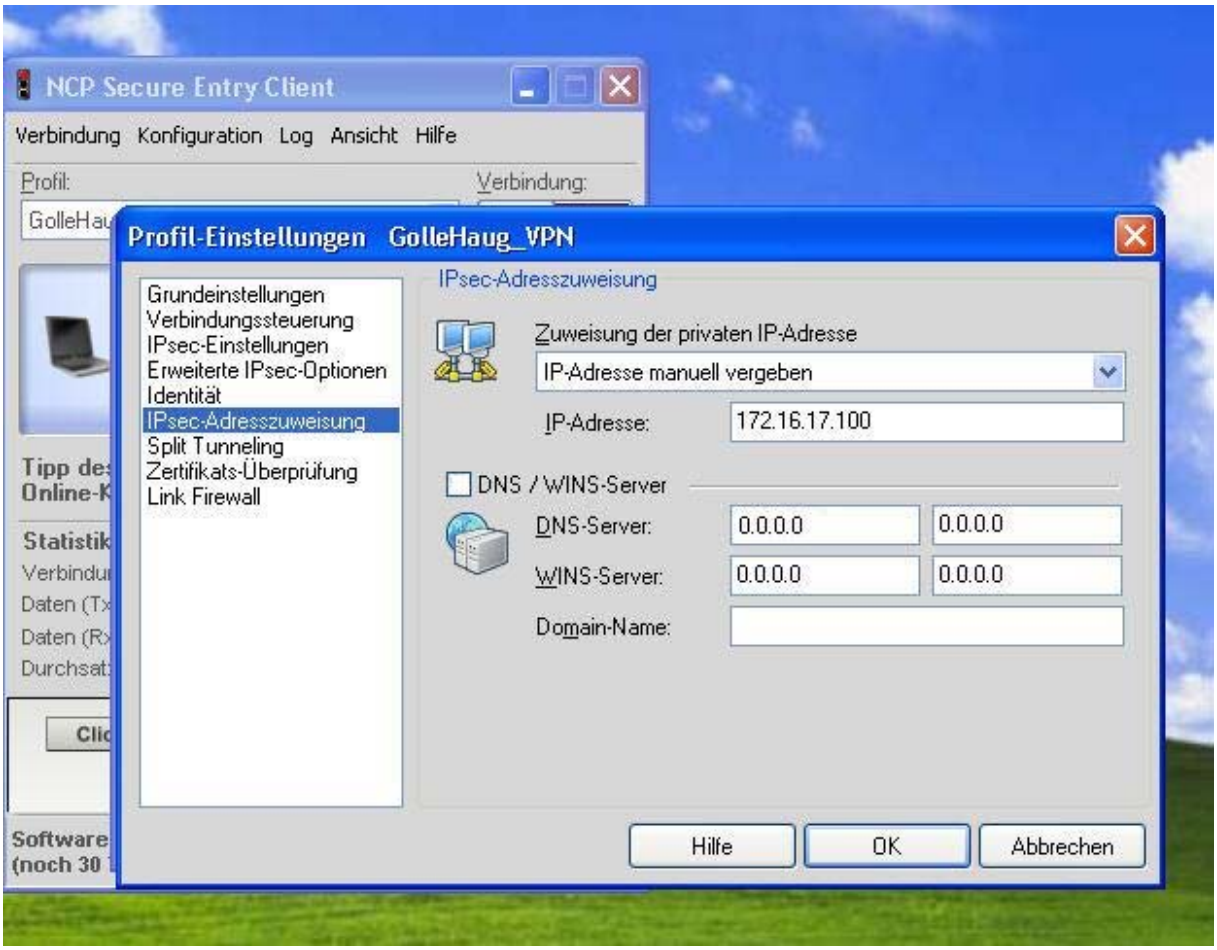

NCP Secure Entry Client
Verbindung Konfiguration Log Ansicht Hilfe
Profil:
Verbindung:
IPsec Konfiguration
IPsec Konfiguration
IKE-Richtlinie
Phase1
IPsec-Richtlinie
Phase2
Hinzufügen
Bearbeiten
Kopieren
Löschen
Hilfe
Schließen

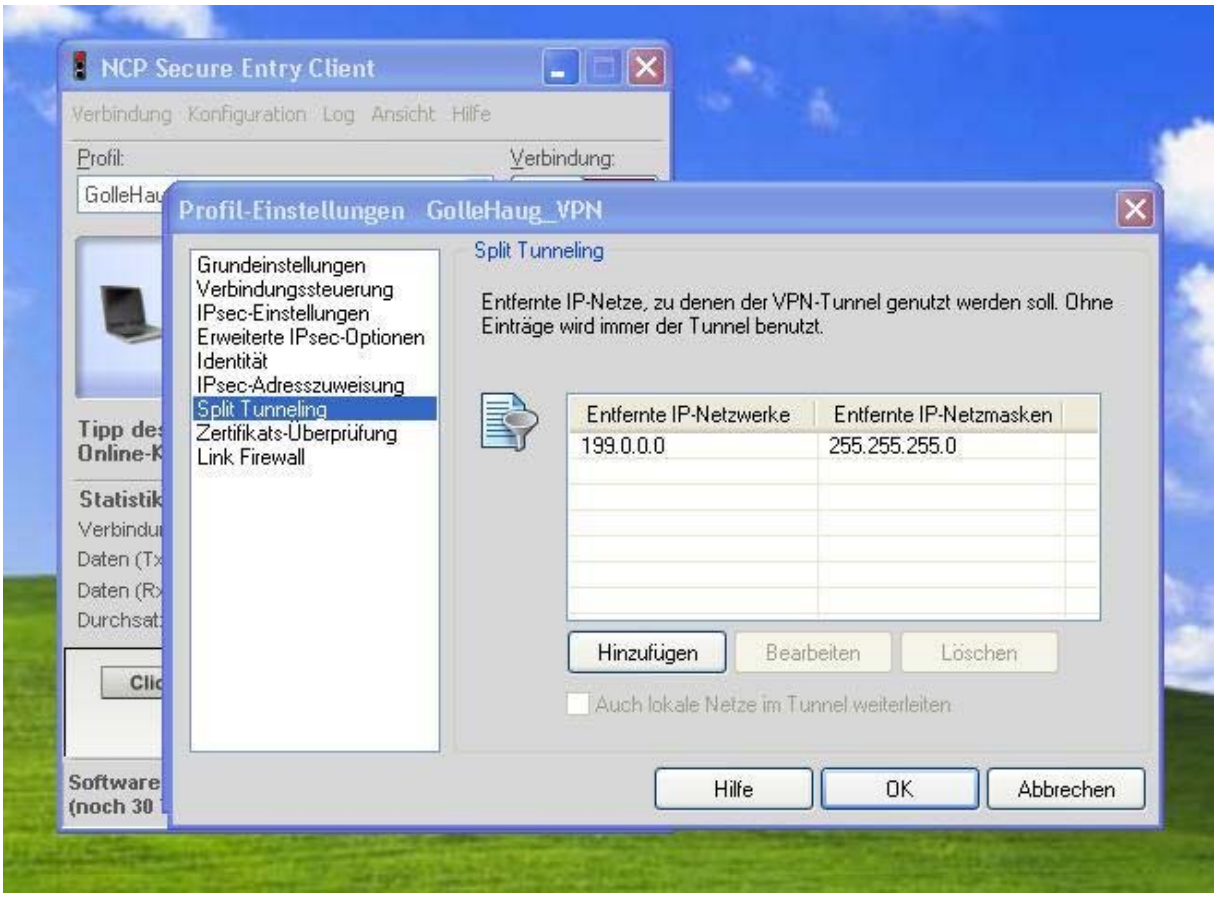

NCP Secure Entry Client
Verbindung Konfiguration Log Ansicht Hilfe
Profil:
Verbindung:
IPsec Konfiguration
IPsec Konfiguration
IKE-Richtlinie
Phase1
IPsec-Richtlinie
Phase2
IKE-Richtlinie
Name :
Phase1
Authentisierung
Verschlüsselung
Hash
DH-Gruppe
Pre-shared Key
AES 128 Bit
SHA
DH-Gruppe 2 (1024 Bit)
Authentisierung :
Pre-shared Key
Verschlüsselung:
AES 128 Bit
Hash:
SHA
DH-Gruppe:
DH-Gruppe 2 (1024 Bit)
Hinzufügen
Entfernen
Hilfe
OK
Abbrechen

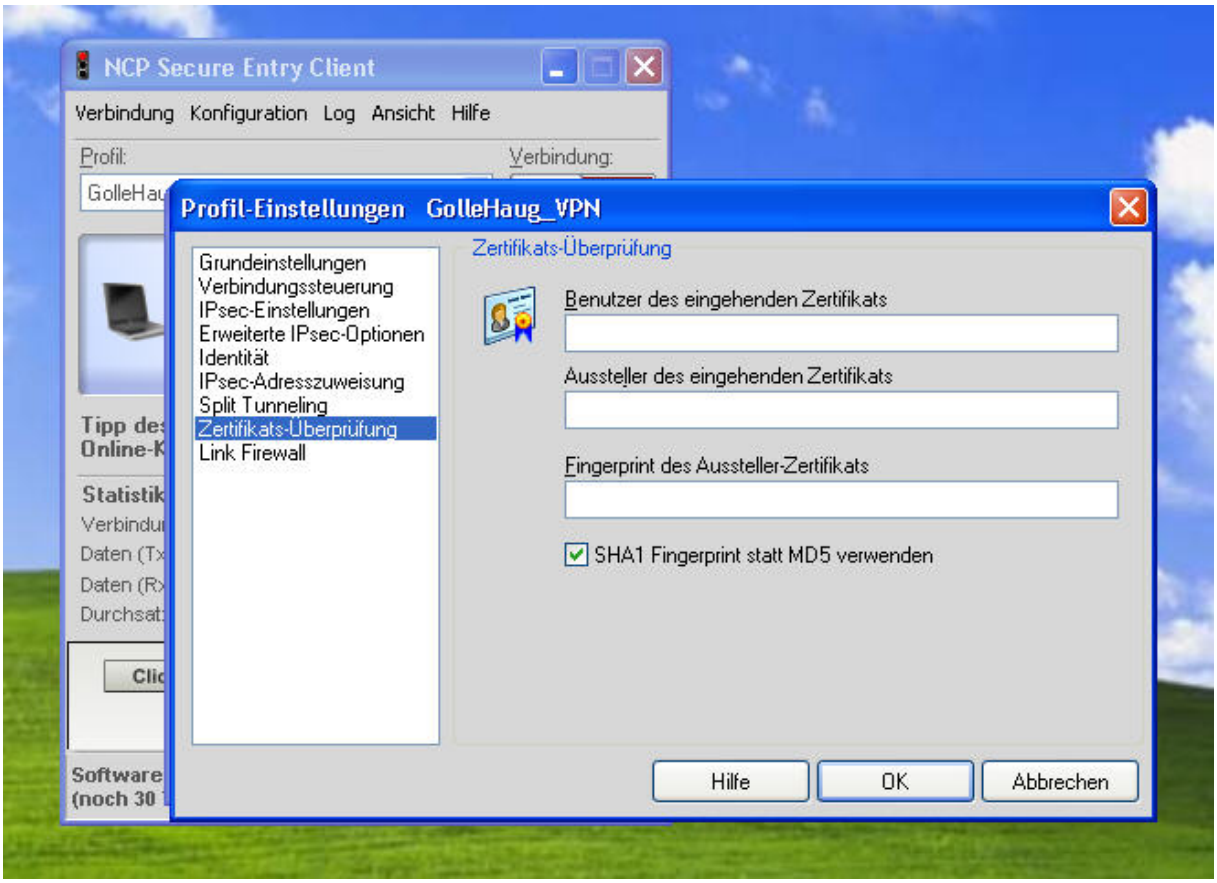

NCP Secure Entry Client
Verbindung Konfiguration Log Ansicht Hilfe
Profil:
Verbindung:
IPsec Konfiguration
IPsec Konfiguration
IKE-Richtlinie
Phase1
IPsec-Richtlinie
Phase2
IPsec-Richtlinie
Name:
Phase2
Protokoll
Verschlüsselung
Authentisierung
ESP
AES 128 Bit
SHA
Protokoll:
ESP
Verschlüsselung:
AES 128 Bit
Authentisierung:
SHA
Hinzufügen
Entfernen
Hilfe
OK
Abbrechen

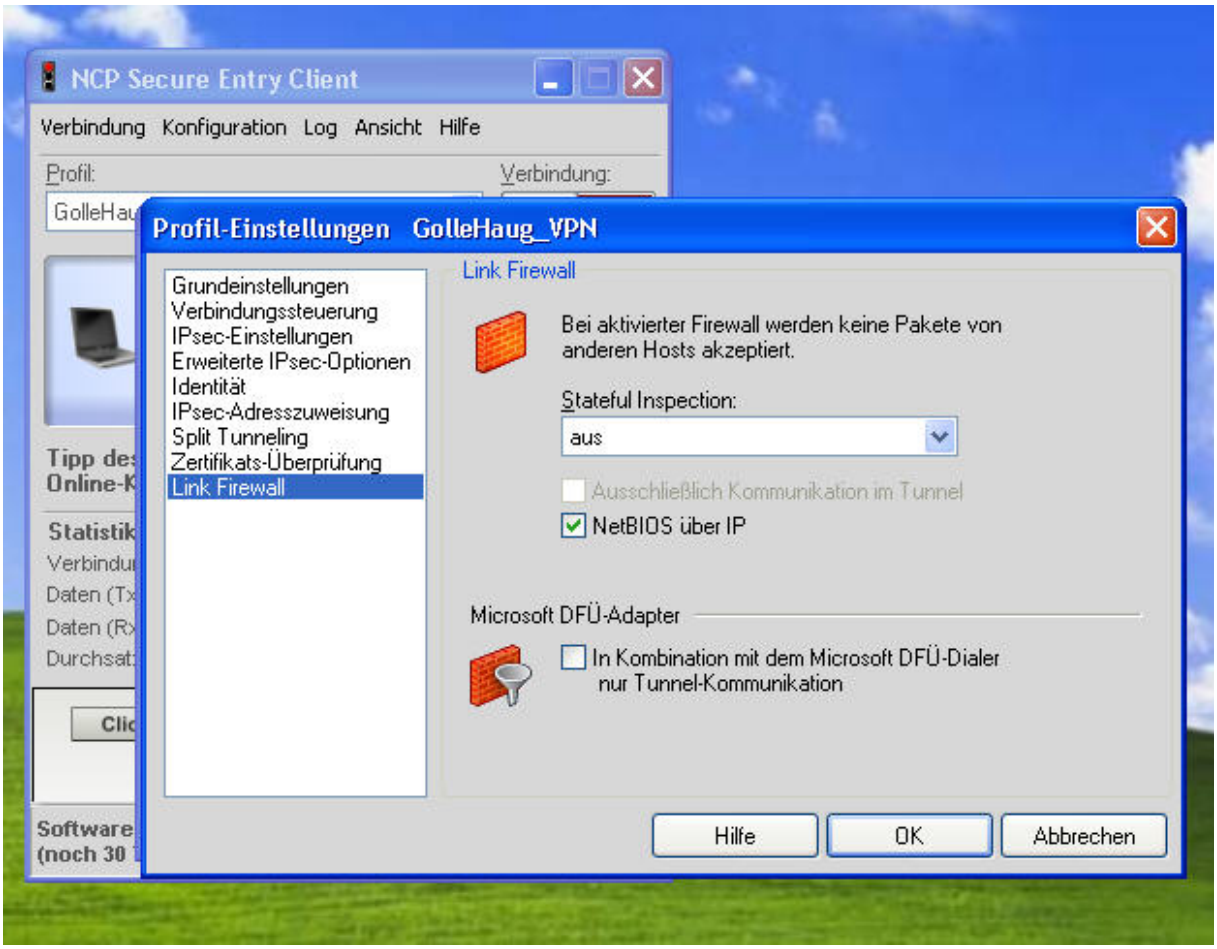

NCP Secure Entry Client
Verbindung Konfiguration Log Ansicht Hilfe
Profil:
Verbindung:
Profil-Einstellungen GolleHaug_VPN
Grundeinstellungen
Verbindungssteuerung
IPsec-Einstellungen
Erweiterte IPsec-Optionen
Identität
IPsec-Adresszuweisung
Split Tunneling
Zertifikats-Überprüfung
Link Firewall
Erweiterte IPsec-Optionen
IPsec-Kompression
Deaktiviere DPD (Dead Peer Detection)
Intervall : 20 Sek.
Anzahl der Versuche: 8
Standard IPsec
UDP Encapsulation
Port: 0
VPN Path Finder
(NCP VPN Path Finder Technology am Gateway erforderlich)
Hilfe
OK
Abbrechen


NCP Secure Entry Client
Verbindung Konfiguration Log Ansicht Hilfe
Profil:
Verbindung:
Profil-Einstellungen GolleHaug_VPN
Grundeinstellungen
Verbindungssteuerung
IPsec-Einstellungen
Erweiterte IPsec-Optionen
Identität
IPsec-Adresszuweisung
Split Tunneling
Zertifikats-Überprüfung
Link Firewall
Identität
Lokale Identität (IKE)
Typ: IP-Adresse
ID: 0.0.0.0
Pre-shared Key verwenden
Shared Secret:
Bestätigung Secret:
Zertifikats-Konfiguration: keine
Extended Authentication (XAUTH)
Benutzername:
Passwort:
aus obiger Konfiguration
Hilfe
OK
Abbrechen


NCP Secure Entry Client
Verbindung Konfiguration Log Ansicht Hilfe
Profil:
Verbindung:
Profil-Einstellungen GolleHaug_VPN
Grundeinstellungen
Verbindungssteuerung
IPsec-Einstellungen
Erweiterte IPsec-Optionen
Identität
IPsec-Adresszuweisung
Split Tunneling
Zertifikats-Überprüfung
Link Firewall
IPsec-Adresszuweisung
Zuweisung der privaten IP-Adresse
IP-Adresse manuell vergeben
IP-Adresse:
172.16.17.100
DNS / WINS-Server
DNS-Server:
0.0.0.0
0.0.0.0
WINS-Server:
0.0.0.0
0.0.0.0
Domain-Name:
Hilfe
OK
Abbrechen


NCP Secure Entry Client
Verbindung Konfiguration Log Ansicht Hilfe
Profil:
Verbindung:
Profil-Einstellungen GolleHaug_VPN
Grundeinstellungen
Verbindungssteuerung
IPsec-Einstellungen
Erweiterte IPsec-Optionen
Identität
IPsec-Adresszuweisung
Split Tunneling
Zertifikats-Überprüfung
Link Firewall
Split Tunneling
Entfernte IP-Netze, zu denen der VPN-Tunnel genutzt werden soll. Ohne Einträge wird immer der Tunnel benutzt.
Entfernte IP-Netzwerke
Entfernte IP-Netzmasken
199.0.0.0
255.255.255.0
Hinzufügen
Bearbeiten
Löschen
Auch lokale Netze im Tunnel weiterleiten
Hilfe
OK
Abbrechen


NCP Secure Entry Client
Verbindung Konfiguration Log Ansicht Hilfe
Profil:
Verbindung:
Profil-Einstellungen GolleHaug_VPN
Grundeinstellungen
Verbindungssteuerung
IPsec-Einstellungen
Erweiterte IPsec-Optionen
Identität
IPsec-Adresszuweisung
Split Tunneling
Zertifikats-Überprüfung
Link Firewall
Zertifikats-Überprüfung
Benutzer des eingehenden Zertifikats
Aussteller des eingehenden Zertifikats
Fingerprint des Aussteller-Zertifikats
SHA1 Fingerprint statt MD5 verwenden
Hilfe
OK
Abbrechen


NCP Secure Entry Client
Verbindung Konfiguration Log Ansicht Hilfe
Profil:
Verbindung:
Profil-Einstellungen GolleHaug_VPN
Grundeinstellungen
Verbindungssteuerung
IPsec-Einstellungen
Erweiterte IPsec-Optionen
Identität
IPsec-Adresszuweisung
Split Tunneling
Zertifikats-Überprüfung
Link Firewall
Link Firewall
Bei aktivierter Firewall werden keine Pakete von anderen Hosts akzeptiert.
Stateful Inspection:
aus
Ausschließlich Kommunikation im Tunnel
NetBIOS über IP
Microsoft DFÜ-Adapter
In Kombination mit dem Microsoft DFÜ-Dialer nur Tunnel-Kommunikation
Hilfe
OK
Abbrechen