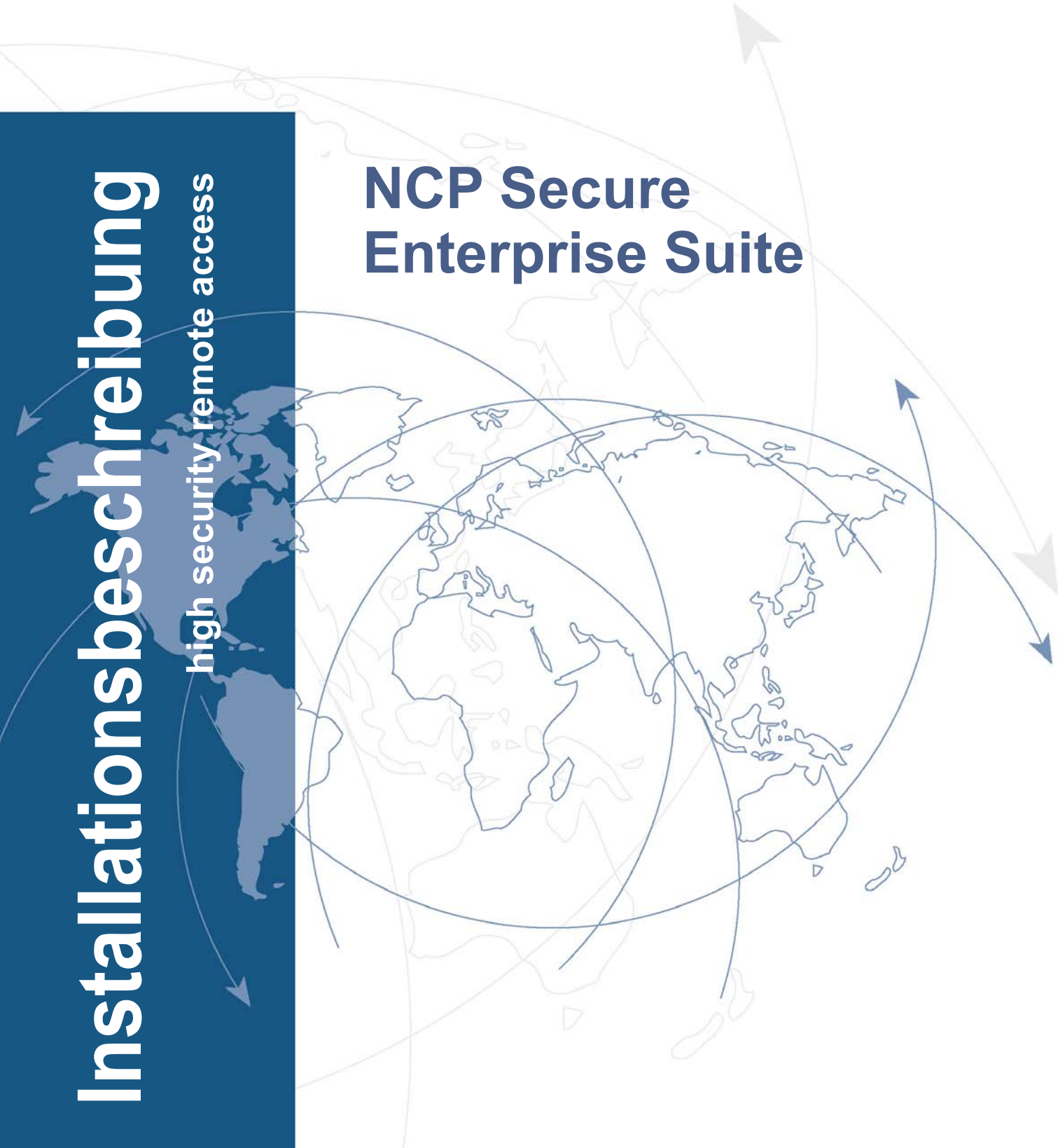
NCP
SECURE COMMUNICATIONS

Installationsbeschreibung

high security remote access

NCP Secure Enterprise Suite



Copyright

Network
Communications
Products engineering GmbH

Dombühler Str.2
D-90449 Nürnberg
Tel.: 0911 / 99 68-0
Fax: 0911 / 99 68-299
internet http:// www.ncp-e.com
E-mail: info@ncp-e.com

Installation der Secure Enterprise Suite

In diesem Dokument finden Sie neben der Installationsbeschreibung eine kurze Produktbeschreibung. Zudem sind spezielle Installationsmöglichkeiten und die Lizenzierung beschrieben.

Inhaltsübersicht

Weiterführende Beschreibungen zur Erstellung von Profilen und zur IPsec-Konfiguration finden Sie in den Beschreibungen **Secure Client Monitor** und **Secure Client Parameter**.

Eine Übersicht bietet die **Suite-Navigation**. In dieser PDF-Datei sind alle aktuell verfügbaren Dokumente zu Ihrem Client verzeichnet.

Vom Navigator aus können Sie alle relevanten Dokumente direkt anspringen und – falls sie noch nicht in Ihrem Navigatorverzeichnis gespeichert sind – von der NCP Homepage herunterladen.

Produktbeschreibung

Die NCP Secure Enterprise Suite lässt sich durch Auswahl bei der Installation für einen Testzeitraum wahlweise als NCP Dynamic Personal Firewall oder NCP Secure Enterprise Client installieren. In beiden Fällen wird immer die komplette Software auf dem Rechner installiert, wobei die Produktvariante der Dynamic Personal Firewall keine VPN-Funltionalität zur Verfügung stellt.

Die jeweils installierte Produktvariante kann nach Ablauf der Testphase erworben und lizenziert werden. Die jeweilige Funktionalität wird durch den erworbenen Lizenzschlüssel spezifiziert.

Secure Enterprise Client

Der NCP Secure Enterprise Client verfügt über den kompletten Leistungsumfang. Die entsprechenden Funktionalitäten werden unter **Optionen** im Ansichtmenü des Monitors angezeigt und können hier nach Bedarf ein- oder ausgeblendet werden:
– Dialer für Internet-Einwahl (zusätzl. externer Dialer)
– WLAN (auch Hotspot-Anmeldung)
– EAP (erweiterte Authentisierung in LAN / WLAN)
– Dynamic Personal Firewall
– VPN (Security-Modi IPsec und L2sec, PKI-Unterstützung, automatische Medienerkennung, LAN over IP)

Der NCP Secure Enterprise Client ist eine Komponente der ganzheitlichen NCP Secure Enterprise Solution. Die Kommunikationssoftware dient dem universellen Teleworking in beliebigen Remote Access VPN-Umgebungen. Auf Basis des IPsec-Standards können hochsichere Datenverbindungen sowohl zu NCP Secure Enterprise Servern als auch zu VPN Gateways aller namhaften Anbieter hergestellt werden. Der Datentransfer erfolgt unabhängig vom Mediatyp (any network) über Festnetze, öffentliche Funknetze, LANs (z. B. im Filialnetz), das Internet sowie Nahbereichs-Funknetze wie Wireless LANs am Firmengelände und an Hotspots. Mittels beliebiger Endgeräte (any device) können Teleworker von jedem Standort (any location) auf zentrale Datenbestände und Anwendungen (any application) zugreifen.

Universelle Einsatzmöglichkeiten fordern umfangreiche Sicherheitsmechanismen zur Abwehr von Attacken in jeder Remote Access-Umgebung. Auch an Hotspots während des An- und Abmeldevorganges. Die wichtigsten, integrierten Security-Bausteine sind neben dem VPN-Tunneling: Datenverschlüsselung, eine **Dynamic Personal Firewall**, die Unterstützung von OTP-Token (One Time Passwort) und Zertifikaten in einer PKI (Public Key Infrastructure).

Alle Konfigurationen können zentral vom Administrator so eingegeben werden, dass sie durch den Anwender nicht veränderbar sind. Mechanismen des zentralen Managements (**Secure Enterprise Management**) ermoglichen eine automatische Übernahme aller Konfigurationsparameter in den Client. Der NCP Dialer bietet zudem Schutz vor kostenintensiven Fremd-Dialern.

Stationäre und mobile PC-Arbeitsplätze werden über öffentliche Netze (via Internet) hinweg als vollwertige Teilnehmer in das Firmennetz integriert. Teleworker arbeiten in gewohnter Weise wie an einem Büroarbeitsplatz. Ihnen stehen alle LAN-Applikationen und -Ressourcen 1:1 am remote PC zur Verfügung.

Die Software arbeitet nach dem Prinzip der LAN-Emulation, d. h. sie erscheint dem PC-Betriebssystem gegenüber als LAN-Adapter (virtueller Netzwerkadapter). Deshalb ist es u.a. möglich, dem remote Client vom zentralen Secure Enterprise Gateway eine private IP-Adresse zuzuweisen. Diese kann je nach Anforderung fest oder variabel (dynamisch) aus einem Adresspool zugeordnet werden. Bei Bedarf kann eine einmal zugewiesene IP-Adresse trotz physikalischem Verbindungsabbau (z. B. bei Short-Hold-Mode) beibehalten werden, d. h. die logische Verbindung zwischen remote Client und zentraler LAN-Ressource bleibt erhalten. Auch die Einwahl in verschiedene Standort-Netze bereitet trotz wechselnder IP-Adressen keine Probleme. Der remote User ist immer mit demselben Namen im Unternehmensnetz identifizierbar, wo immer er sich auch befindet. Weiter ist die Einbindung in eine DDNS-Struktur (Dynamic Domain Name Service-Protokoll) möglich. Optional kann der Verbindungsaufbau und die Überwachung mit dem zentralen Server für den Anwender unbemerkt automatisiert im Hintergrund seiner Tätigkeiten erfolgen.

Die NCP Secure Client Software unterstützt die routbaren Protokolle TCP/IP und IPX/SPX. Die Client Software (für ISDN) wurde für den Einsatz mit dem D-Kanal-Protokoll DSS1 getestet. Darüber hinaus unterstützt sie jedoch auch andere D-Kanal-Protokolle, wie VN3/4, NT1, CT1, 5ESS, Austel, usw.

Die aktuelle Version und künftige Versionen des Secure Clients werden von der Qualitätssicherung nur noch für die Windows-Betriebssysteme Windows XP, Windows Vista und Windows 7 getestet. Für ältere Windows-Betriebssysteme kann somit keine Gewähr mehr für die volle Funktionsfähigkeit der Client Software übernommen werden.

Die NCP Secure Communications Lösung garantiert durch die standardmäßig integrierte Personal Firewall, dass ein Telearbeitsplatz aus dem Internet und von anderen LAN-Teilnehmern (z. B. an Hotspots) nicht attackiert werden kann!

Dynamic Personal Firewall

Anwender die die Vorteile einer zentral administrierbaren Firewall inkl. friendly Net Detection nutzen möchten, jedoch keine VPN Funktionalität benötigen, können die Produktvariante der Dynamic Personal Firewall ohne VPN Client nutzen.

Mittels der Personal Firewall können Regelwerke und Applikationen definiert werde für: Ports, IP-Adressen und Segmente. Ein weiteres Sicherheitskriterium ist **Friendly Net Detection**, d. h. die automatische Erkennung von sicheren und unsicheren Netzen. In Abhängigkeit davon werden die entsprechenden Firewall-Regeln aktiviert bzw. deaktiviert.

Die lizenzierte Dynamic Personal Firewall erscheint zunächst nur im Tray Icon. Der Monitor muss über das Menü der Firewall im Tray Icon eigens eingeblendet werden. Anschließend können die Features der Firewall auch über das Ansichtmenü angezeigt und hier nach Bedarf ein- oder ausgeblendet werden:
– Dialer für Internet-Einwahl (zusätzl. ext. Dialer)
– WLAN (auch Hotspot-Anmeldung)
– EAP (erweiterte Authentisierung in LAN / WLAN)
– Personal Firewall

Die NCP Dynamic Personal Firewall besitzt bis auf die VPN-Funktionalität alle Funktionalitäten der Software und ist wie der Secure Enterprise Client ebenso mit dem Secure Enterprise Management zentral via Update über LAN administrierbar.

Ein späteres Upgrade auf den Secure Enterprise Client ist mit dem entsprechenden Lizenzschlüssel jederzeit möglich.

Secure Enterprise Management

Das Secure Enterprise Management (SEM) bietet einen lückenlosen Funktionsumfang. Maximale Transparenz für die Netzwerkadministration und Minimierung der TCOs (Total Costs of Ownership) sind garantiert.

Secure Enterprise Solution

Weitere Informationen erhalten Sie auf der NCP Website: http://www.ncp-e.com

Hinweise zur Installation

Die Installation der Software für Windows-Systeme erfolgt komfortabel über Setup. Der Installationsablauf ist für alle Windows-Betriebssysteme identisch. Im folgenden ist die Installation für Windows Vista beschrieben.

Bevor Sie die Software installieren, müssen die Installationsvoraussetzungen, wie im folgenden Kapitel beschrieben, erfüllt sein.

Beachten Sie außerdem, das der Client ab Version 8.31 bei einer Neu-Installation in das Programm-Verzeichnis des Betriebssystems
Programme\NCP\SecureClient
installiert wird.

Alter Pfad: %Windows%\ncple

Neuer Pfad: %Programme%\NCP\SecureClient

Bei einem Update wird weiterhin der Pfad genutzt, der bei der letzten Installation eingetragen war.

Registry-Reparatur (RegRep)

Bei jeder Neuinstallation des Clients, d. h. auch wenn eine ältere Version deinstalliert wurde, überprüft das Setup-Programm die Registry-Einträge. Werden problematische Einträge gefunden, so werden bereinigt. Das Setup-Programm generiert dazu eine Meldung, wonach der PC neu gestartet werden sollte.

Installationsvoraussetzungen

Betriebssystem

Die Software kann auf Computern (min. 128 MB RAM) mit den Betriebssystemen Windows XP, Windows Vista oder Windows 7 installiert werden.

Gegenstelle

Die Gegemstelle muss eines der folgenden Verbindungsmedien unterstützen: ISDN, PSTN (analoges Modem), GSM, GPRS/UMTS, LAN over IP, WLAN oder PPP over Ethernet. (Im folgenden sind die Verbindungsmedien aufgeführt, wovon jeweils eines pro Profil der Gegenstelle am Secure Client eingestellt sein muss. Mit Mausklick auf einen der rot markierten Begriffe springen Sie in das Dokument **Client-Parameter** oder **Mobile-Computing** zur jeweiligen Konfigurationsbeschreibung.)

Secure Client

Eine der folgenden Kommunikationsschnittstellen muss am Client PC verfügbar sein.

ISDN-Adapter (ISDN)

Der ISDN-Adapter muss die **ISDN** CAPI 2.0 unterstützen. Wenn Sie **PPP Multilink** nutzen, kann die Software bis zu 8 ISDN B-Kanäle (je nach Kanalanzahl des Adapters) bündeln. Prinzipiell kann jeder ISDN-Adapter, der die ISDN-Schnittstelle CAPI 2.0 unterstützt, eingesetzt werden. (Für gewöhnlich wird die CAPI bei der Installation eines ISDN-Adapters automatisch eingerichtet.)

Analoges Modem (Modem)

Für die Kommunikation über **Modem** muss das Modem korrekt installiert sein, sowie Modem Init. String und COM-Port Definition zugewiesen sein. Das Modem muss den Hayes-Befehlssatz unterstützen.

Ebenso können Mobiltelefone für die Datenkommunikation genutzt werden, nachdem die zugehörige Software installiert wurde, die sich für den Client genauso darstellt wie ein analoges Modem. Als Schnittstelle zwischen Handy und PC kann die serielle Schnittstelle, die IR-Schnittstelle (Infrarot) oder Bluetooth genutzt werden. Je nach Übertragungsrat (GSM, V.110, GPRS oder HSCSD) muss die Gegenstelle über die entsprechende Einwahlplattform verfügen. Der in die Modemkonfiguration des Secure Clients einzutragende Initialisierungs-String ist vom ISP oder dem Hersteller des Mobiltelefons zu beziehen.

LAN-Adapter (LAN over IP)

Um die Client-Software mit der Verbindungsart **LAN (over IP)** in einem Local Area Network betreiben zu können, muss zusätzlich zum bereits installierten LAN-Adapter (Ethernet) kein weiterer Adapter installiert werden. Die Verbindung der LAN-Clients ins WAN stellt ein beliebiger Access Router her. Einzige Voraussetzung: IP-Verbindung zum Zielsystem muss möglich sein. Die VPN-Funktionalität liefert die Client Software.

Adapter für ein wireless LAN (WLAN-Adapter) werden genauso behandelt wie normale LAN-Adapter.

xDSL (xDSL (PPPoE))

Das Verbindungsmedium **PPP over Ethernet** setzt voraus, dass eine Ethernet-Karte installiert und darüber ein xDSL-Modem mit Splitter korrekt angeschlossen ist.

xDSL (AVM - PPP over CAPI)

Das Verbindungsmedium **AVM - PPP over CAPI** kann gewählt werden, wenn eine AVM Fritz! DSL-Karte eingesetzt wird. Im Feld “Rufnummer (Ziel)” in der Gruppe “Netzeinwahl” können für die Verbindung über CAPI noch AVM-spezifische Intitialisierungskommandos eingetragen werden. Unter Windows Betriebssystemen wird jedoch empfohlen den Standard “xDSL (PPPoE)” zu verwenden, da damit direkt über die Netzwerkschnittstelle mit der Karte kommuniziert wird.Bei Verwendung der AVM Fritz! DSL-Karte wird keine separate zusätzliche Netzwerkkarte benötigt.

Multifunktionskarte

Wird eine Mobilfunkkarte (für: GRPS / UMTS / HSDPA / HSUPA) eingesetzt, so können mit der Client Software spezielle Features des Mobile Computings unter Einbeziehung der Karteneigenschaften genutzt werden. Aufgrund der direkten Unterstützung einer **Multifunktionskarte** durch den Secure Client kann die Installation einer Management-Software von der eingesetzten Karte entfallen.

Der NCP Secure Client vereint alle kommunikations- und sicherheitstechnischen Mechanismen für eine wirtschaftliche Datenkommunikation auf Basis

des Ende-zu-Ende Sicherheitsprinzips. Der Client-Monitor verfügt über optische Anzeigen aller Verbindungsstatus der Feldstärke, des selektierten Netzes und Providers.

Ab der Version 9.02 Build 5 unterstützt der Secure Client nach Einspielen der Datei g3detect.dll neue PCMCIA-Funkkarten, die Sie bitte der neuesten Kompatibilitätsliste entnehmen unter:

http://www.ncp-e.com/de/service-support/kompatibilitaeten/mobile-connect-cards.html

WLAN-Adapter (WLAN)

Der WLAN-Adapter wird mit dem Verbindungsmedium **WLAN** betrieben werden. Im Monitormenü erscheint eigens der Menüpunkt “WLAN-Einstellungen”, worin die Zugangsdaten zum Funknetz in einem Profil hinterlegt werden können. Wird diese “WLAN-Konfiguration aktiviert”, so muss das Management-Tool der WLAN-Karte deaktiviert werden. (Alternativ kann auch das Management-Tool der WLAN-Karte genutzt werden, dann muss die WLAN-Konfiguration im Monitormenü deaktiviert werden.)

Wird die Verbindungsart WLAN für ein Profil eingestellt, so wird unter dem grafischen Feld des Monitors eine weitere Fläche eingeblendet, auf der die Feldstärke und das WLAN-Netz dargestellt werden.

Bitte beachten Sie zur Konfiguration der WLAN-Einstellungen die Beschreibung zum **Mobile Computing**.

Automatische Medienerkennung

Die **automatische Medienerkennung** kann nur eingesetzt werden, wenn alternative Verbindungsmedien zur Verfügung stehen.

Werden wechselweise unterschiedliche Verbindungsmedien genutzt, wie zum Beispiel LAN oder WLAN (im Firmennetz), Modem und ISDN (von remote), so kann die manuelle Auswahl des Profils mit dem jeweils zutreffenden Verbindungsmedium entfallen, wenn ein Profil mit dem Verbindungsmedium LAN auf “automatische Medienerkennung” umkonfiguriert wurde und je ein Profil mit einem alternativ verfügbaren Verbindungsmedium, wie zum Beispiel Modem, ISDN, DSL oder GPRS/UMTS vorhanden ist.

Beachten Sie zur Konfiguration die Beschreibung im PDF **Enterprise Client Parameter**.

Voraussetzungen für Zertifikatsverwendung

Sollen Zertifikate für die erweiterte Authentisierung eingesetzt werden, so beachten Sie bitte das Dokument **Secure-Client-Zertifikate**.

Unterstützte Schnittstellen und Formate

Der Secure Client kann in Public Key Infrastrukturen nach **X.509 V.3** Standard eingesetzt werden. Die Enterprise-Version besitzt außerdem die Entrust Ready-Funktionalität, womit der Client alle wichtigen Richtlinien von Entrust hinsichtlich des Zertifikatseinsatzes und deren Benutzung unterstützt (siehe die Beschreibung **Entrust-Ready**).

Der Secure Client unterstützt folgende Schnittstellen / Formate:
– Smartcards, USB-Token:
PKCS#11, TCOS 1.2 und 2.0, CSP
– Soft-Zertifikate: **PKCS#12-Datei**
– PC/SC-konforme **Chipkartenleser**:
Die Client Software unterstützt alle Chipkartenleser, die PC/SC-konform sind. Diese Chipkartenleser werden in einer Liste des Clients aufgenommen, wenn der Leser angeschlossen und die zugehörige Treiber-Software installiert wurde.
– **Automatische Erkennung des angeschlossenen PC/SC-Lesers**: Ist für das PKI-Umfeld die Verwendung eines PC/SC Chipkartenlesers am Client konfiguriert, so erkennt und verwendet der Client automatisch den jeweils angeschlossenen.
Durch diesen Automatismus wird das Anlegen von Profilen am Enterprise Management-System vereinfacht, da in der zentralen Zertifikats-Konfiguration keine benutzerspezifischen Chipkartenleser vorkonfiguriert werden müssen.
Erhält der Benutzer vom Management System eine Konfiguration ohne Eintrag für einen Chipkartenleser und ist ein Zertifikat vorkonfiguriert, so liest der Client automatisch die Daten des PC/SC-Lesers ein, der am Benutzer-PC installiert ist und verwendet diesen Leser.
Dieses Feature ist nur nutzbar in Verbindung mit Smartcards die ohne Schnittstellen-Software direkt angesprochen werden können, wie NetKey-Chipkarten (Telesec).
– **PKCS#11-Modul**: Mit der Software für die Smartcards oder den Tokens werden Treiber in Form einer PKCS#11-Bibliothek (DLL) mitgeliefert. Diese Treiber-Software muss zunächst installiert werden. Anschließend kann über einen Assistenten das entsprechende PKCS#11-Modul selektiert werden.

CA-Zertifikate

Der Administrator des Firmennetzes legt fest, welchen Ausstellern von Zertifikaten vertraut werden kann. Dies geschieht dadurch, dass er die CA-Zertifikate seiner Wahl in das Installationsverzeichnis unter <CACERTS> einspielt. Das Einspielen kann bei der Software-Distribution automatisiert stattfinden, wenn sich die Aussteller-Zertifikate bei der Installation der Software von einem Datenträger dort im Verzeichnis <DISK1> befinden. Beachten Sie dazu die Beschreibung zur **erweiterten Installation**.

Nachträglich können Aussteller-Zertifikate automatisch über den Secure Management Server (nur zu Enterprise Clients) verteilt werden oder, sofern der Benutzer über die notwendigen Schreibrechte in genanntem Verzeichnis verfügt, von diesem selbst eingestellt werden.

Derzeit werden die Formate *.pem und *.crt für Aussteller-Zertifikate unterstützt. Sie können im Monitor unter dem Hauptmenüpunkt “Verbindung / Zertifikate / **CA-Zertifikate anzeigen**” eingesehen werden.

Wird am Secure Client das Zertifikat einer Gegenstelle empfangen, so ermittelt der NCP Client den Aussteller indem er das Aussteller-Zertifikat, zunächst auf Smartcard bzw. USB-Token oder in der PKCS#12-Datei, anschließend im Installationsverzeichnis unter <CACERTS> sucht. Kann das Aussteller-Zertifikat nicht gefunden werden, kommt die Verbindung nicht zustande. Sind keine Aussteller-Zertifikate vorhanden, wird keine Verbindung zugelassen.

Werden Soft-Zertifikate mit dem PKI Plug-in des Management Servers erstellt, so wird das Aussteller-Zertifikat in der PKCS#12-Datei gespeichert.

Verwendung von Sperrlisten (CRL)

Zu jedem Aussteller-Zertifikat kann dem Secure Client die zugehörige CRL (Certificate Revocation List) zur Verfügung gestellt werden. Sie wird in das Installationsverzeichnis unter <CRLS> gespielt. Ist eine CRL vorhanden, so überprüft der Secure Client eingehende Zertifikate daraufhin, ob sie in der CRL geführt sind. Der Client lädt die zugehörige CRL automatisch herunter wenn das eingehende Benutzer-Zertifikat des Servers die **Zertifikatserweiterung CDP** enthält.

Installation der Software

Die vorliegende Version und künftige Versionen des Clients werden von der Qualitätssicherung nur noch für die Windows-Betriebssysteme Windows XP, Windows Vista und Windows 7 getestet. Für Windows NT sowie Windows 98 oder älter kann somit keine Gewähr mehr für die volle Funktionsfähigkeit der Client Software übernommen werden.

Sie können die Software in Form einer ZIP-Datei als Download von der NCP- Internetseite unter www.ncp-e.com beziehen.

Bitte achten Sie darauf, ob Sie von Festplatte, CD oder Diskette installieren.

Installation von der CD

Nachdem Sie die CD in das Laufwerk Ihres Computers eingelegt haben, erscheint eine Maske in der Sie unter “Programm installieren” ncpsetup.exe ausführen.

Das weitere Verfahren ist mit der Standard-Installation ab “Wählen der Setup-Sprache” identisch.

Nachdem die NCP-Begrüßungsmaske erscheint, wählen Sie aus, welches Produkt Sie installieren möchten und klicken anschließend auf “Installieren”.

Standard-Installation

Wenn Sie die Software als Testversion nach einem Download installieren möchten, entpacken Sie zunächst die ZIP-Datei. Beim Entpacken wird automatisch das Verzeichnis <DISK1> angelegt.

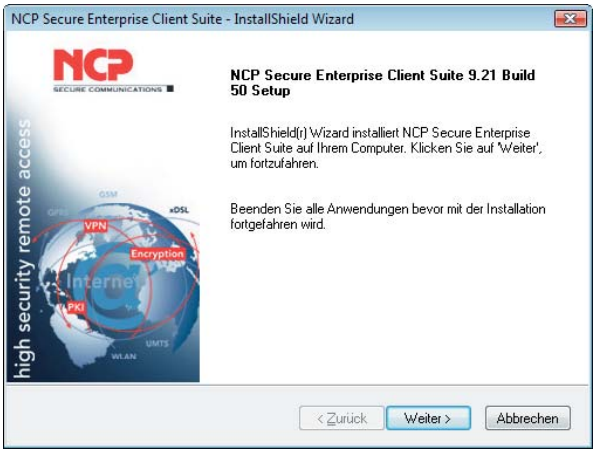
Starten Sie die Installation unter dem Windows Explorer mit Aufruf von Setup.exe aus dem Disk1-Verzeichnis.

Wählen der Setup-Sprache

Im folgenden Fenster können Sie die Setup-Sprache auswählen. Klicken Sie danach auf “OK”.

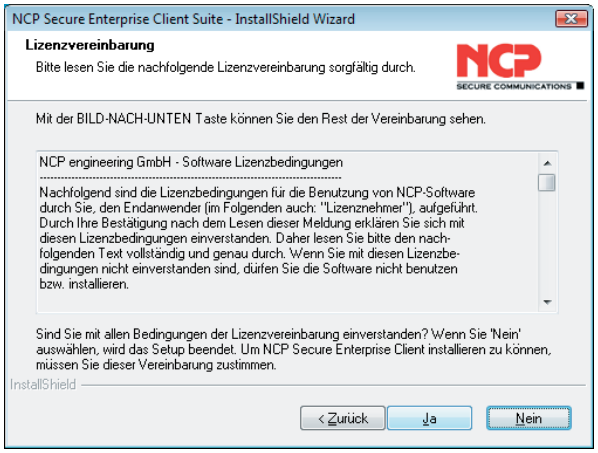
Anschließend bereitet das Setup-Programm den Install-Shield Assistenten vor, mit dessen Hilfe die Installation fortgesetzt wird.

Lesen Sie bitte die Hinweise im Willkommen-Fenster des Setup-Programms bevor Sie auf “Weiter” klicken (Abb. unten).



(Bitte beachten Sie ggf. Hinweise auf VPN Client und Personal Firewall eines fremden Herstellers und deaktivieren Sie diese, um Instabilität oder Datenverlust zu vermeiden.)

Anschließend werden die Lizenzbedingungen gezeigt. Stimmen Sie dem Vertag mit “Ja” zu, sonst wird die Installation abgebrochen (Abb. rechts oben).



Testversion

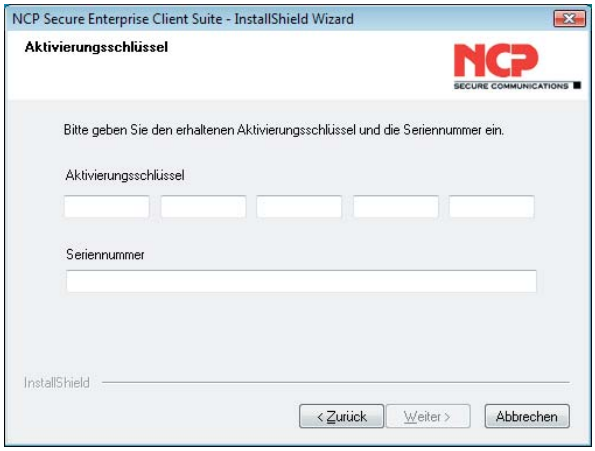
Haben Sie noch keine Lizenz erworben, so wählen Sie in diesem Fenster die Installation einer Testversion. (Sollten Sie eine Testversion installieren, so ist diese vom Zeitpunkt der Installation für 30 Tage gültig und kann danach nicht mehr gestartet werden.)

Der NCP Secure Enterprise Client lässt sich durch Auswahl wahlweise als
NCP Dynamic Personal Firewall oder
NCP Secure Enterprise Client
installieren (Abb. unten).

Lizenzierung

Haben Sie eine Lizenz für die Software erworben, so wählen Sie “Installation als Vollversion” und klicken “Weiter”.

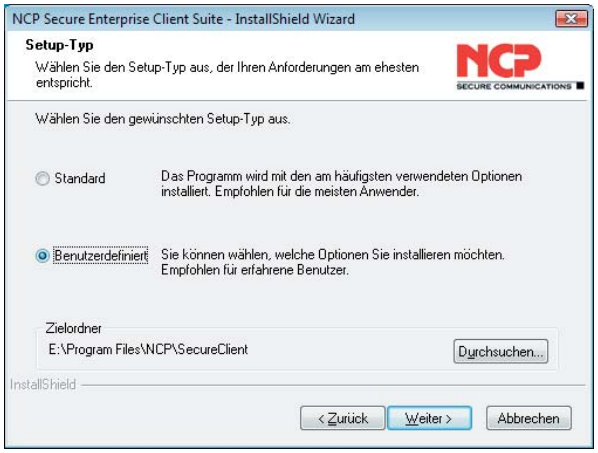
Die Vollversion der Software wird aktiviert, indem Sie anschließend Aktivierungsschlüssel und Seriennummer Ihrer Software-Lizenz in die dafür vorgesehenen Felder eintragen. Sind diese Codes korrekt eingetragen, wird der “Weiter”-Button in diesem Fenster aktiviert. Mit “Weiter” schalten Sie die Software für den uneingeschränkten Funktionsumfang frei. Ihre Software ist damit voll einsatzfähig.



Wählen Sie im folgenden Fenster eine Standard-Installation, so ist das Setup mit dieser Wahl abgeschlossen.

Benutzerdefinierte Installation

Nehmen Sie eine “Benutzerdefinierte Installation” vor, so können Sie weitere Einstellungen machen.



Im ersten Fenster der benutzerdefinierten Installation (Abb. oben) kann ein beliebiges Installationsverzeichnis für die Software gewählt werden. Dies ist insbesondere dann wichtig, wenn der Benutzer keine Rechte auf das System-Root-Verzeichnis hat. Standard-Installationsverzeichnis ist: %Programme%\NCP\SecureClient.

Im folgenden Fenster der “Benutzerdefinierten Installation” bestimmen Sie den Programmordner. (Standard ist “NCP Secure Client”).

Sie können das Icon auf den Desktop setzen.

Firewall-Option für den Enterprise Client

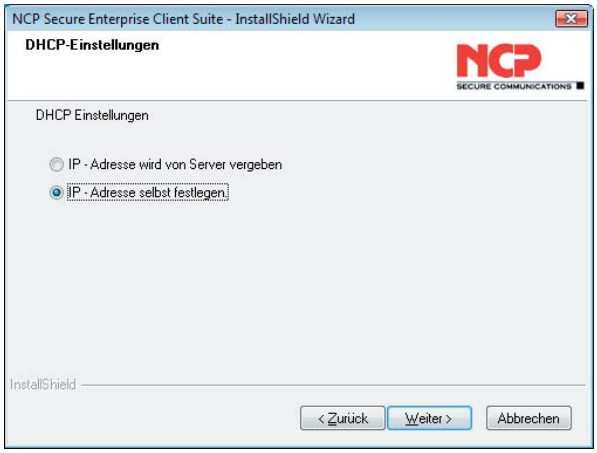
Nur in der benutzerdefinierten Installation des Enterprise Clients kann auch die Firewall-Funktion dauerhaft aktiviert werden, sodass nur noch eine Kommunikation im Tunnel möglich ist.

Wird diese Einstellung während der Installation vorgenommen, so gilt sie global für alle Profile und ist auch wirksam wenn der Client gestoppt ist. Die Einstellung der Personal Firewall im Monitor **Firewall bei gestopptem Client weiterhin aktivieren** kann nicht ausgeschaltet werden.

Eine Deaktivierung der Firewall ist nach dieser Intallationseinstellung nur möglich wenn die Client Software deinstalliert und danach neu installiert wird.

Weitere benutzerdefinierte Einstellunngen

Zu den weiteren Einstellungen bezüglich Ihres Kommunikations-Gateways sind nähere Informationen von Ihrem Administrator oder Internet Service Provider nötig.



Mit DHCP (Dynamic Host Control Protocol) zu kommunizieren, bedeutet, dass Sie für jede Session automatisch eine IP-Adresse zugewiesen bekommen. In diesem Fall klicken Sie auf “IP-Adresse wird von Server vergeben”.

Wenn Sie die “IP-Adresse selbst festlegen”, geben Sie in nachfolgendem Fenster die IP-Adressen ein.

Bitte beachten Sie: Ist bereits eine Netzwerkkarte mit Default Gateway installiert, so muss der Eintrag “Default Gateway” hier gelöscht werden. Es darf nur eine Netzwerkkarte mit Default Gateway installiert sein. Die DNS-Adresse bitte nur eintragen, wenn Sie sie von Ihrem Provider oder Systemadministrator zur Verfügung gestellt bekommen haben.

Windows Logon-Optionen

Sie können anschließend entscheiden, ob vor dem Windows-Logon an einer remote Domain die Verbindung zum VPN Gateway aufgebaut werden soll.

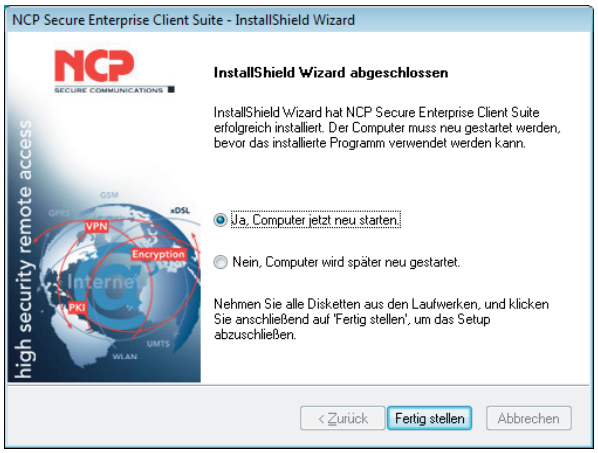
Für diesen Verbindungsaufbau müssen Sie gegebenenfalls die PIN für ihr Zertifikat und das (nicht gespeicherte) Passwort für die Client Software eingeben. Nachdem die Verbindung zum Gateway hergestellt wurde, können Sie sich an die remote Domain anmelden. Diese Anmeldung erfolgt dann bereits verschlüsselt über den VPN-Tunnel.

Aktivieren Sie diese Abfrage vor dem Windows Logon, so wird hiermit automatisch die Anmeldeoption (Gina / Credential) installiert. Über das Monitormenü des Clients unter “Konfiguration” können entsprechende Parameter gesetzt werden.

Wird die Logon-Option hier nicht aktiviert, soll sie jedoch zu einem späteren Zeitpunkt genutzt werden, so kann sie mit dem Kommando
`rwscmd / ginainstall`
dauerhaft installiert werden.

Setup abschließen

Nachdem alle benötigten Dateien eingespielt wurden und die Programmgruppe angelegt wurde, klicken Sie auf “Beenden”, um das Setup abzuschließen.



Assistent für erste Konfiguration

Nachdem Sie die Software installiert haben und zum Abschluss der Installation den Rechner gebootet haben, wird der Client Monitor automatisch nach dem Booten geladen (Abb. unten). Außerdem wird automatisch der “Assistent für die erste Konfiguration” gestartet – vorausgesetzt Sie haben den Secure Client zum ersten Mal installiert oder die Profil-Einstellungen gelöscht. Sie befinden sich im Installationsverzeichnis.

Der “Assisitent für erste Konfiguration” (Abb. oben) bietet Ihnen die Möglichkeit, Test-Verbindungen anzulegen. Wenn Sie diese Möglichkeit nutzen, führt Sie der Assistent durch die Konfiguration der wichtigsten Parameter und legt nach der Vorgabe Ihrer Daten ein Profil für Testverbindungen an.

Für die Profil-Einstellungen, die Sie mit diesem Assistenten erstellt haben, werden die Zugangsdaten verwendet, die unter **Tests des Clients** beschrieben sind. Sie können diese Einträge anschließend zum Testen der Software benutzen.

Wenn Sie keine Test-Verbindungen anlegen und den “Assistent für erste Konfiguration” abbrechen, erstellen Sie die ersten Profile wie im Handbuch zum **Client-Monitor** beschrieben.

Secure Client-Programme

Wenn der Secure Client installiert wurde, finden Sie in der Windows Programmgruppe, die Sie zur Installation angegeben haben, drei Programme:

Secure Client Monitor
Secure Client Popup
Secure Client Tracer

Haben Sie kein **Programm-Icon** zum Start des Secure Clients auf dem Desktop angelegt (siehe oben), so kann der Secure Client über den Menüpunkt **Secure Client Monitor** gestartet werden (siehe **Client-Monitor**).

Das **Secure Client Popup** zeigt an, ob es sich bei der Software um eine lizenzierte oder unlizenzierte Version handelt. Handelt es sich um eine unlizenzierte Testversion, so wird die Version der Software und die noch verbliebene Dauer der Gültigkeit in Tagen angezeigt. Die Software kann jederzeit nachträglich lizenziert werden. Dazu selektiern Sie im Hilfemenü des Monitors den Menüpunkt **Lizenzierung**.

Wurde die Software lizenziert, so wird die Seriennummer angezeigt, darunter die Software-Version einschließlich der Build-Nummer, sowie die Versionsnummer der lizenzierten Version. Zum Beispiel kann eine höhere Software-Version mit älteren Seriennummer und Aktivierungsschlüssel, sprich für eine niedrigere Version, lizenziert worden sein.

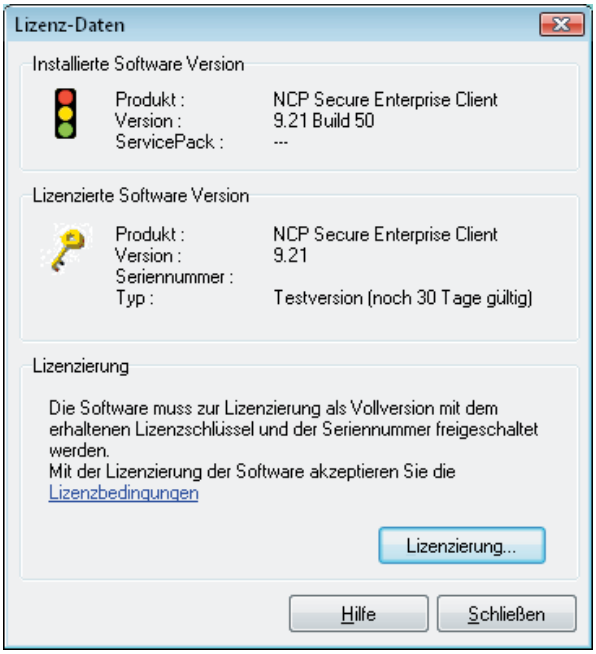
Der **Secure Client Tracer** ist ein eigenes kleines Anwendungsprogramm für qualifizierte Systemtechniker. Mit seiner Hilfe können Traces zur Fehlersuche erstellt werden.

Dynamic Personal Firewall

Die Dynamic Personal Firewall erscheint zunächst nur im Tray Icon. Der Monitor muss über das Menü der Firewall im Tray Icon eigens eingeblendet werden. Anschließend können die Features der Firewall auch über das Ansichtmenü angezeigt werden. Siehe dazu das PDF **Enterprise Client Firewall und FND**.

Lizenzierung

Im Hilfemenü des Client Monitors wird unter dem Menüpunkt Lizenzierung die eingesetzte Software-Version und gegebenenfalls die lizenzierte Version mit Seriennummer angezeigt.



Wir die Software als Testversion eingesetzt, so kann die verbliebene Dauer der Gültigkeit abgelesen werden.

Um eine zeitlich unbegrenzt gültige Vollversion nutzen zu können, muss die Software mit dem erhaltenen Lizenzschlüssel und der Seriennummer freigeschaltet werden.

Mit der Lizenzierung der Software akzeptieren Sie die Lizenzbedingungen, die nach einem Klick eingesehen werden können.

Die Eingabe von Lizenzschlüssel und Seriennummer kann erfolgen, nachdem Sie auf den Lizenzierungsbutton geklickt haben.

Korrekt eingegebene Lizenzdaten können zu einem späteren Zeitpunkt an dieser Stelle nicht mehr ausgelesen werden (siehe oben **Lizenzierung**).

Tests des Clients

Während der Installation wurde im Startmenü die Programmgruppe “NCP Secure Client” angelegt. Starten Sie nun aus der Programmgruppe “NCP Secure Client” das Programm “Client Monitor”.

Das Telefonbuch des Clients enthält folgende vorkonfigurierte Zielsysteme für Testzwecke:

Testverbindung
Testverbindung IPsec native
Testverbindung IPsec über L2TP
Testverbindung L2TP
Testverbindung L2Sec

Ebenfalls für Testzwecke wurde ein “X.509 Soft-Zertifikat” beigegeben. Es wird bei der Installation als PKCS#12-Datei im Installationsverzeichnis gespeichert. Der Dateiname ist “user1.p12" und die PIN ”1234". Dieses Zertifikat kann genutzt werden, um die Strong Security-Version PKI/VPN Client zu testen.

Testverbindung (testet ISDN, Modem, GSM)

```
Rufnummer            :   +4991199682663
Benutzer             :   ncpuser
Passwort             :   ncpuser
Verschlüsselung      :   keine
```

Testverbindung IPsec native (über LAN)

```
Gateway (Tunnel-Endpunkt):
vpntest.ncp-e.com
VPN-Protokoll       : IPsec
XAUTH-Benutzername  : ncpIPsecnative
XAUTH-Passwort      : ncpIPsecnative
```

Testverbindung IPsec native (über ISDN)

```
Gateway (Tunnel-Endpunkt):
172.16.12.36
VPN-Protokoll       : IPsec
XAUTH-Benutzername  : ncpIPsecnative
XAUTH-Passwort      : ncpIPsecnative
```

Testverbindung IPsec über L2TP (testet IPsec über L2TP mit Preshared Key)

```
Gateway (Tunnel-Endpunkt):
vpntest.ncp-e.com
VPN-Protokoll     : L2TP
Benutzer (VPN)    : ncpuserIPsec
Passwort (VPN)    : ncpuserIPsec
Tunnel Secret     : secret
Security-Modus    : IPsec
Statischer Schlüssel:
00.11.22.33.44.55.66.77.88.99.AA.BB.CC.DD.EE.FF
IKE-Richtlinie    : Pre-Shared Key
IPsec-Richtlinie  : ESP 3DES-BF-MD5
Austausch-Modus   : Main Mode
```

Testverbindung über L2TP (testet L2TP-Protokoll)

```
Gateway (Tunnel-Endpunkt):
vpntest.ncp-e.com
VPN-Protokoll     : L2TP
Benutzer (VPN)    : ncpuserl2tp
Passwort (VPN)    : ncpuserl2tp
Tunnel Secret     : secret
Verschlüsselung   : keine
```

Testverbindung L2Sec (testet SSL-Verschlüsselung und Zertifikat)

```
Gateway (Tunnel-Endpunkt):
vpntest.ncp-e.com
VPN-Protokoll     : L2TP
Benutzer (VPN)    : ncpuserssl
Passwort (VPN)    : ncpuserssl
Tunnel Secret     : secret
Verschlüsselung   : SSL mit Zertifikat
Außerdem muss im Monitor-Menü unter
Verbindung / Konfiguration / Zertifi-
kate /der Dateiname "client1.p12" ein-
getragen sein!
```

Testen mit Ping

```
Bei bestehendem Tunnel können Sie die IP-Adresse 172.16.12.100 anpingen.
Geben Sie dazu in einer DOS-Kommandozeile folgendes ein:
C:\>ping 172.16.12.100 (<ENTER>)
Bei erfolgreichem Ping sehen Sie folgende oder ähnliche Ausgaben:
Reply from 172.16.12.100: bytes=32 time=109ms TTL=128
Reply from 172.16.12.100: bytes=32 time=96ms TTL=128
Reply from 172.16.12.100: bytes=32 time=82ms TTL=128
Reply from 172.16.12.100: bytes=32 time=69ms TTL=128
Im Monitor werden die versendeten (Tx) und die empfangenen (Rx) Bytes
angezeigt.
```

Testen mit FTP

```
Bei bestehendem Tunnel können die FTP-Funktionalität testen.
Ihre Zugangsdaten:
IP-Adresse        :  172.16.12.100
Benutzer          :  anonymus
Geben Sie dazu in einer DOS-Kommandozeile folgendes ein:
C:\>ftp 172.16.12.100
Verbindung mit 172.16.12.100 wurde hergestellt
220 (vsFTPd 2.0.4)
Benutzer (172.16.12.100:(none)): anonymous
230 Login successful
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
SecEntryCl_Linux_de.pdf
SecEntryCl_WinCe_de.pdf
SecEntryCl_WinCe_en.pdf
SecEntryCl_Win_de.pdf
SecEntryCl_Win_en.pdf
226 Directory send OK.
FTP: 64d Bytes empfangen in 0,00Sekunden 407000,00KB/s
ftp> close
ftp> quit
```

Testen der Web-Funktionalität

```
Nachdem Sie eine Testverbindung aufgebaut haben, geben Sie an
Ihrem geöffneten Web-Browser folgende Adresse ein:
172.16.12.100
anschließend erhalten Sie die NCP-Website auf Ihrem Bildschirm.
```

Erweiterte Installation

Um zusätzliche, z. B. benutzerspezifische Dateien für bestimmte Benutzer oder eine Benutzergruppe bei der Installation der Client Software automatisch mit zu installieren, wurde folgende Möglichkeit geschaffen:

Werden unter dem Verzeichnis <DISK1> (oder auf der Disk1) nachfolgend genannte Unterverzeichnisse angelegt, so werden alle darin befindlichen Dateien mit dem Setup der Software automatisch mit kopiert:

```
Disk1\ncple     ->  <Installationsverzeichnis>
Disk1\system    ->  SYSTEM / SYSTEM32 - Verzeichnis
Disk1\CaCerts   ->  <Installationsverzeichnis>\CaCerts
```

Bitte beachten Sie, dass diese Dateien erst nach den Systemdateien der Software kopiert werden, sodass bei Namensgleichheit der Dateien die originalen Systemdateien überschrieben werden.

Beachten Sie außerdem, dass bei Einsatz dieser Methode eine Version verfälscht werden kann, sodass ein korrekter Support nicht mehr gewährleistet werden kann.

Deinstallation

Wenn Sie den Client deinstallieren, erhalten Sie die Möglichkeit Ihre Konfigurationen und Profil-Einstellungen im Installationsverzeichnis des Clients zu behalten. Wird zu einem späteren Zeitpunkt eine neuere Version des Clients im gleichen Verzeichnis installiert, so können diese persönlichen Daten wieder genutzt werden. Sollen die persönlichen Daten des Clients auch gelöscht werden, so müssen Sie dies eigens bestätigen. In diesem Fall werden restlos alle Daten und Verzeichnisse des Clients entfernt. (Abb. unten)