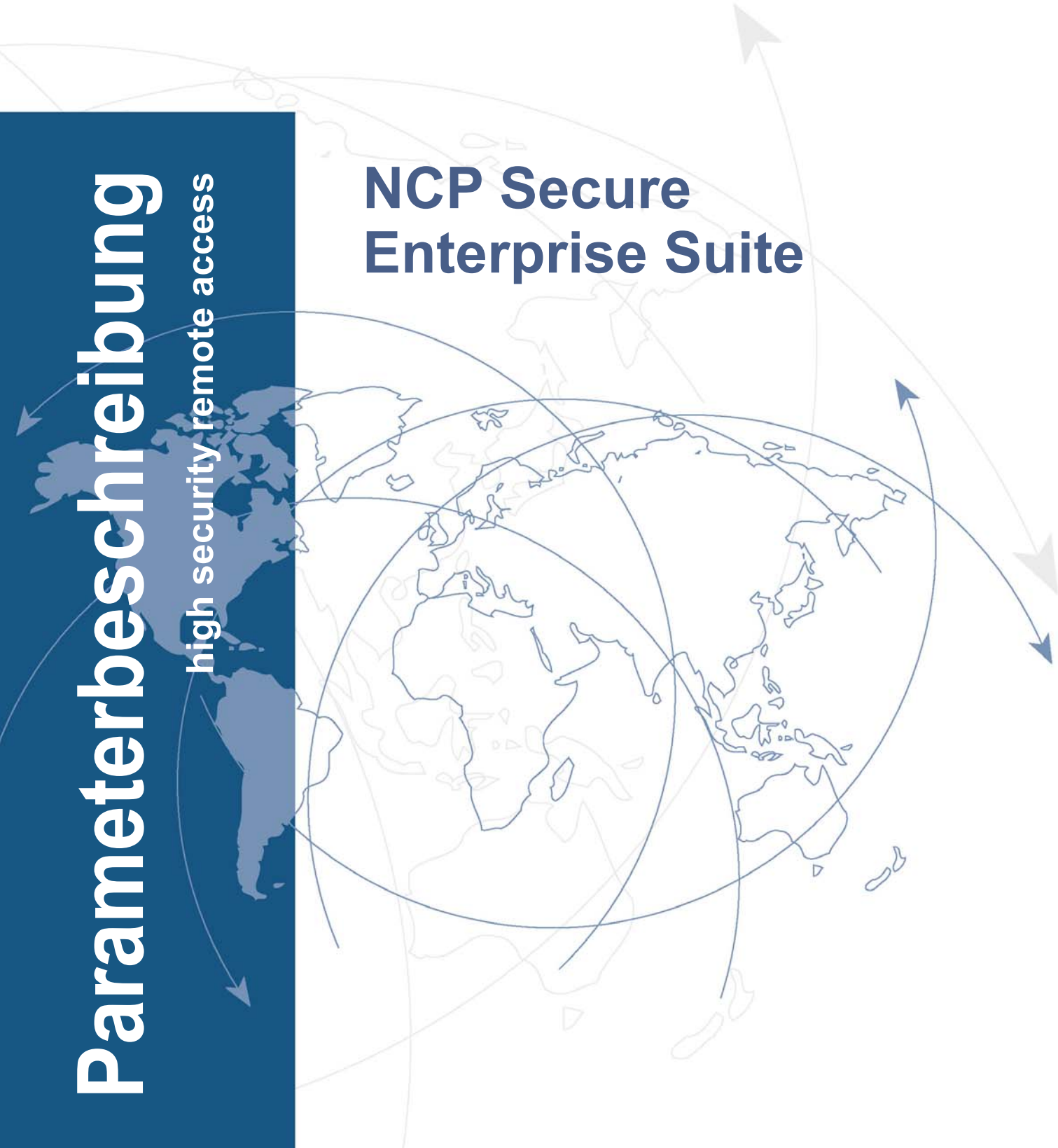
SECURE COMMUNICATIONS

Parameterbeschreibung

high security remote access

NCP Secure Enterprise Suite



Secure Enterprise Suite Parameter

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

Copyright

NCP Hotline auf Abruf

Sie erreichen unsere NCP Experten unter folgenden Hotlines:

Kunden mit Hotline Service Vertrag
Sie erhalten sofortigen Support unter der vertraglich angegebenen Rufnummer.
Ihnen steht das komplette Serviceportfolio zur Verfügung.

Kunden ohne Hotline Service Vertrag
Sie können wählen zwischen:
Kostenpflichtige Service-Rufnummer 09001996800 (-,80 Euro / Minute)
E-Mail an support@ncp-e.com

Dienstleistungsauftrag (Berechnung nach Aufwand)
mit festen Reaktionszeiten und Zusatzservices.
Bitte nutzen Sie zur Anfrage das NCP Service-Formular von der Website
http://www.ncp-e.com/de/service-support/support.html

Sie möchten mehr über den NCP Hotline Service Vertrag wissen?
Bitte senden Sie eine E-Mail an:
vertrieb@ncp-e.com

Enterprise Suite Parameter

In diesem Dokument sind alle Konfigurationsparameter der Profil-Einstellungen und IPsec-Konfiguration der Secure Enterprise Suite beschrieben.

Die Reihenfolge der Parameterbeschreibungen wurde an der Reihenfolge der Konfigurationsfelder zu den Profilen im Enterprise Client ausgerichtet.

Alle Parameter sind alphabetisch im **Index** gelistet.

Auf der folgenden Seite wurden die **Konfigurationsfelder der Profil-Einstellungen** aufgelistet. Von dieser Seite aus können die Konfigurationsfelder per Mausklick direkt angewählt werden, ohne das Dokument durchblättern zu müssen. Ein Mausklick auf das Enterprise-Icon führt Sie auf diese Seite zurück.*

Per Mausklick auf einen der fett gedruckten roten Begriffe, springen Sie in dieser Dokumentation zur jeweils angegebene Stelle (z. B. auf die Gegenüberstellung der Konfigurationsfelder auf der nächsten Seite).

Ist neben dem roten Begriff das Icon für ein NCP-PDF angebracht (links), öffnet sich mit einem Mausklick das entsprechende weiterführende Dokument, vorausgesetzt es befindet sich im gleichen Verzeichnis wie diese Parameterbeschreibung.

Am komfortabelsten erhalten Sie die gewünschten Informationen über die **Enterprise Suite Navigation**. Dort sind alle aktuell verfügbaren Dokumente zu Ihrem Produkt verzeichnet.

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

** Bitte beachten Sie, dass in der Oberfläche Ihres Secure Clients nicht immer alle Parameter und Konfigurationsfelder angezeigt werden müssen. Zum einen werden sie nach dem jeweils gewählten Verbindungsmedium automatisch ein- oder ausgeblendet (z. B. Modem oder HTTP-Anmeldung). Zum anderen können einzelne Konfigurationsfelder oder Parameter, die Sie für Ihre Arbeit mit dem Client nicht benötigen, von Ihrem Systemadministrator ausgeblendet worden sein.*

Konfigurationsfelder der Profil-Einstellungen

IPsec-Konfiguration

Grundeinstellungen

Die Client Software gestattet die Einrichtung individueller Profile, die den Benutzeranforderungen entsprechend konfiguriert werden können. Um Profil-Einstellungen voneinander unterscheiden zu können, muss in diesem Parameterfeld zunächst ein Name für das Profil vergeben werden. Danach kann das Verbindungsmedium zur Gegenstelle genauer definiert werden.

Profil-Name

Wenn Sie ein neues Profil definieren, sollten Sie zunächst einen unverwechselbaren Namen für dieses Profil eintragen (z. B. IBM London). Der Name darf jeden gewünschten Buchstaben wie auch Ziffern beinhalten und darf, Leerzeichen mitgezählt, bis zu 39 Zeichen lang sein.

Verbindungsmedium

Das Verbindungsmedium kann für jedes Profil eigens über den Auswahl-Button eingestellt werden, vorausgesetzt Sie haben die entsprechende Hardware angeschlossen und in Ihrem System installiert. Folgende Verbindungsmedien können eingestellt werden:

ISDN

Hardware: ISDN-Hardware
(Karte, ISDN-Box oder PCMCIA-Karte)
mit Capi 2.0-Unterstützung;
Netze: ISDN-Festnetz;
Gegenstellen: ISDN-Hardware;

Modem

Hardware: Asynchrone Modems (PCMCIA oder GSM-Karte) mit Com Port-Unterstützung;
Netze: Analoges Fernsprechnetz (PSTN)
(auch GSM und GPRS);
Gegenstellen: Modem oder ISDN-Karte mit digitalem Modem;

LAN (over IP)

Hardware: LAN-Adapter;
Netze: LAN mit Ethernet oder Token Ring;
Gegenstellen: Die Gegenstellen des lokalen Multiprotokoll-Routers im LAN;

xDSL (PPP over Ethernet)

Hardware: Ethernet-Adapter, xDSL-Modem, Splitter;
Netze: xDSL;
Gegenstellen: Access-Router im xDSL;

xDSL (AVM - PPP over CAPI)

Diese Verbindungsmedium 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.
Netze: xDSL;
Gegenstellen: Access-Router im xDSL;
xDSL (AVM - PPP over CAPI);

GPRS / UMTS

Dieses Medium wählen Sie, wenn die Einwahl über das Mobilfunknetz (GPRS oder UMTS) erfolgen soll. Siehe **Mobile Computing**.

PPTP

Microsoft Point-to-Point Tunnel Protocol;
Angeschlossene Hardware: Ethernet-Adapter, xDSL-Modem;
Netze: xDSL;
Gegenstellen: Access-Router im xDSL;

Wird dieses Protokoll gewählt, so muss im Parameterfeld **Netzeinwahl** unter “PPTP-Endpunkt” die IP-Adresse des Access-Routers im xDSL eingetragen werden.

WLAN

Hardware: WLAN-Adapter;
Netze: Funknetz;
Gegenstellen: Access Point;

Der WLAN-Adapter kann mit der Verbindungsart “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 in der Monitor-Oberfläche zusätzlich die Feldstärke und das WLAN-Netz dargestellt. Beachten Sie dazu die PDF-Dateien **Mobile Computing**.und **Secure Client Monitor**.

Externer Dialer

Ist die Verbindungsart “Ext.Dialer” (über externen Dialer) eingestellt, wird beim Drücken des Verbinden-Buttons eine vorkonfigurierte EXE-Datei (z. B. der iPass-Dialer) gestartet. Über diese EXE-Datei wird die Verbindung zum Internet hergestellt und anschließend über “RWSCMD/connect” der VPN-Verbindungsaufbau des Clients angestoßen. Der NCP Dialer arbeitet unter dieser Konfiguration im LAN-Modus.

Diese Verbindungsart funktioniert nur, wenn im Parameterfeld “Verbindungssteuerung” der Verbindungsaufbau auf “manuell” geschaltet wird.

Je nach installiertem Dialer (iPass oder T-Online) muss in der Konfigurationsdatei EXTDIAL.INI für den Eintrag “ExeName” die EXE-Datei des Dialers eingetragen werden. Um nicht den kompletten Pfad für den Dialer in der DAT-Datei angeben zu müssen, kann optional der Pfad aus der Registry gelesen und in die INI-Datei eingetragen werden. Der genaue Wortlaut der Kopfzeile des Dialers, unter Beachtung der Groß- und Kleinschreibung muss in der INI-Datei unter “Caption” eingetragen werden.

Beispiel der INI-Datei für IPass (in der Registry findet sich unter “InstallPath” der Installations-Pfad des IPass-Dialers “Software\Ipass\iPassConnectEngine”):

```
DialerInstallPathKey = Software\Ipass\
                       iPassConnectEngine
DialerInstallPathValue = InstallPath
DialerExec = IPassConnectGUI.exe
Caption = iPassConnect
```

Automatische Medienerkennung

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

Standard-Profil nach jedem Neustart

Normalerweise wird der Client-Monitor nach einem Neustart mit dem zuletzt genutzten Profil geöffnet. Wird diese Funktion aktiviert, wird nach einem Neustart des Systems immer das hierzu gehörige Profil geladen, unabhängig davon, welches Profil zuletzt genutzt wurde.

Einwahl über Windows-DFÜ

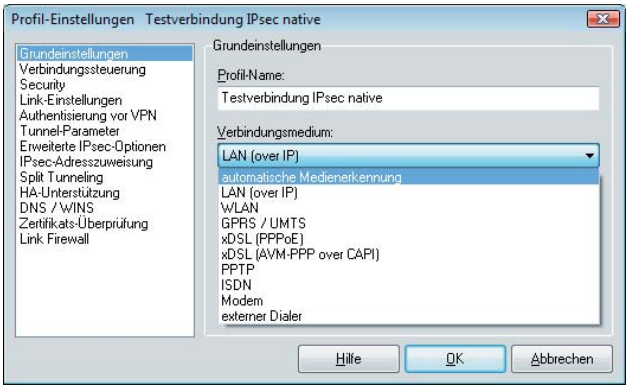
Zur Einwahl am ISP (Internet Service Provider) kann der Microsoft DFÜ-Dialer genutzt werden. Dies ist immer dann nötig, wenn der Einwahlpunkt ein Einwahl-Script benötigt. Der DFÜ-Dialer unterstützt dieses Script. Im Parameterfenster “Netzeinwahl” wird anschließend die Script-Datei unter Eingabe von Pfad und Namen zur eingespielten Script-Datei eingetragen (siehe unten Script-Datei).

Mit der Einstellung “nie” wird ausschließlich der NCP Dialer zur Einwahl verwendet. Soll der DFÜ-Dialer “nur bei Script-Einwahl” verwendet werden, so wählen Sie diese Option. Bei einem Einwahlpunkt, der kein Script verlangt, wird automatisch auf den NCP Dialer umgeschaltet. Soll der DFÜ-Dialer immer verwendet werden, muss die entsprechende Einstellung vorgenommen werden.

Automatische Medienerkennung

Werden wechselweise unterschiedliche Verbindungmedien 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 das 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.

Das Profil mit automatischer Medienerkennung (vormals LAN oder WLAN) muss mit allen für die Verbindung zum VPN Gateway nötigen Parametern (insbesondere der IP-Adresse des VPN Gateways im Parameterfeld “Tunnel-Parameter”) konfiguriert sein (Abb. unten).



Die alternativen Profile müssen die Parameter für das jeweilige Verbindungsmedium enthalten - und sie benötigen im Parameterfeld “Netzeinwahl” die Zugangsdaten für den Internet Diensteanbieter sowie im Parameterfeld “Grundeinstellungen” die Einstellung ihres Verwendungszwecks als “Profil für automatische Medienerkennung” (Abb. unten).

Vor einem Verbindungsaufbau muss das Profil mit dem Verbindungsmedium “automatische Medienerkennung” selektiert sein. Der Client erkennt dann automatisch, welche Verbindungsmedien genutzt werden können und wählt von den alternativ zur Verfügung stehenden Profilen das schnellste aus (bzw. benutzt für eine LAN oder WLAN-Verbindung das für “automatische Medienerkennung” für eine LAN-Verbindung).

Die Priorisierung der Verbindungsmedien ist in folgender Reihenfolge festgelegt: 1. DSL, 2. UMTS / GPRS, 3. ISDN, 4. MODEM.

Konfigurationsanweisung

1. Konfigurieren Sie ein Profil für die Verbindung über LAN oder WLAN zum VPN Gateway innerhalb Ihres Firmennetzes. Dazu benötigen Sie die IP-Adresse des VPN Gateways und Ihre Authentisierungsdaten (u. a. VPN-Benutzername, VPN-Passwort), ggf. auch die Zertifikatskonfiguration.

2. Schalten Sie das Verbindungsmedium von LAN oder WLAN auf “automatische Medienerkennung”. (Die Verbindung zum VPN Gateway im Firmennetz muss damit genauso möglich sein!)

3. Konfigurieren Sie ein alternatives Profil, worin Sie die Zugangsdaten für den Internet-Diensteanbieter und die Parameter für ein alternatives Verbindungsmedium eintragen und bestimmen Sie den Verwendungszweck dieses Profils als “Profil für automatische Medienerkennung”.

4. Das alternative Profil kann für weitere alternative Verbindungsmedien kopiert werden, wonach nur die medienspezifischen Parameter entsprechend eingestellt werden müssen.

5. Achten Sie darauf, dass vor dem Verbindungsaufbau das Profil mit dem Verbindungsmedium “automatische Medienerkennung” in der Profilauswahl selektiert ist.

Profil für automatische Medienerkennung

Mit Aktivierung dieser Funktion wird dieses Profil an das Profil für automatische Medienerkennung gebunden und bei Verfügbarkeit des entsprechenden Mediums automatisch für einen potenziellen Verbindungsaufbau herangezogen.

Netzeinwahl

Über dieses Parameterfeld werden die Angaben zur Netzeinwahl ausgewertet. Es beinhaltet Benutzername und Passwort, die für die PPP-Verhandlung zum Internet-Dienstanbieter (ISP) benötigt werden.

In der Verbindungsart "PPP over Ethernet" entfällt in diesem Parameterfeld die "Rufnummer". Das Parameterfeld erscheint überhaupt nicht, wenn der Client in der Verbindungsart "LAN over IP" betrieben wird.

Betreiben Sie mobile Computing über das Verbindungsmedium GPRS / UMTS, so beachten Sie bitte die Beschreibung **Mobile-Computing**.

Benutzername

Mit dem Benutzernamen weisen Sie sich gegenüber dem Network Access Server (NAS) aus, wenn Sie eine Verbindung zur Gegenstelle aufbauen wollen. Der Name für den Benutzer kann bis zu 255 Zeichen lang sein. Für gewöhnlich wird Ihnen ein Benutzername vom Zielsystem zugewiesen, da Sie von dort auch erkannt werden müssen. Sie erhalten ihn von Ihrem Stammhaus, vom Internet Service Provider oder dem Systemadministrator.

Passwort

Das Passwort benötigen Sie, um sich gegenüber dem Network Access Server (NAS) ausweisen zu können, wenn die Verbindung aufgebaut ist. Das Passwort darf bis zu 128 Zeichen lang sein. Für gewöhnlich wird Ihnen ein Passwort vom Zielsystem zugewiesen, da Sie von dort auch erkannt werden müssen. Sie erhalten es von Ihrem Stammhaus, vom Internet Service Provider oder dem Systemadministrator.

Hinweis: Wenn Profile für die "automatische Medienerkennung" konfiguriert werden, ist es zwingend erforderlich, dass für alle diese Profile ein (NAS-)Passwort eingegeben wird, andernfalls kommt der Verbindungsaufbau nicht zustande.

Wenn Sie das Passwort eingeben, werden alle Zeichen als Stern (*) dargestellt, um sie vor ungewünschten Beobachtern zu verbergen. Es ist wichtig, dass Sie das Passwort genau nach der Vorgabe eintragen und dabei auch auf Groß- und Kleinschreibung achten.

Hinweis: Für den Fall, dass Sie den Parameter "Passwort speichern" nicht aktiviert haben, gilt: Auch wenn Sie für den Verbindungsmodus "automatisch" gewählt haben, müssen Sie die Verbindung beim ersten Mal manuell aufbauen. Dabei werden Sie nach dem Passwort gefragt. Für jeden weiteren automatischen Verbindungsaufbau wird dieses Passwort selbständig übernommen, bis Sie den PC erneut booten oder Sie das Profil wechseln.

Passwort speichern

Dieser Parameter muss aktiviert (angeklickt) werden, wenn gewünscht wird, dass das Passwort (sofern es eingegeben ist) gespeichert wird. Andernfalls werden die Passwörter gelöscht, sobald der PC gebootet oder ein Profil gewechselt wird. Standard ist die aktivierte Funktion.

Wichtig: Bitte beachten Sie, dass im Falle gespeicherter Passwörter, jedermann mit Ihrer Client Software arbeiten kann – auch wenn er die Passwörter nicht kennt.

Rufnummer (Ziel)

Bei einer Wählverbindung muss hier die Rufnummer für das Ziel eingetragen sein. Diese Rufnummer muss genauso eingetragen werden, als würden Sie diese Telefonnummer per Hand wählen. D.h. Sie müssen alle notwendigen Vorwahlziffern berücksichtigen: Landesvorwahl, Ortsvorwahl, Durchwahlziffern, etc. Insgesamt kann die Rufnummer bis zu 30 Ziffern beinhalten.

Tragen Sie jedoch nicht die Amtsholung ein, auch wenn Sie an einer Nebenstellenanlage angeschlossen sind! Die Amtsholung wird unter dem Monitor-Menüpunkt "Konfiguration" eingetragen und hat auf diese Weise Gültigkeit für alle Profile.

Beispiel: Sie wollen eine Verbindung von Deutschland nach England herstellen
00 (für die internationale Verbindung, wenn Sie von Deutschland aus wählen)
44 (dies ist die landesspezifische Vorwahl für England)
171 (Vorwahl für London)
1234567 (die Nummer, die Sie zu erreichen wünschen)

Nach diesem Beispiel wird folgende Nummer in den Profil-Einstellungen gespeichert und für die Anwahl verwendet: 00441711234567.

Hinweis: Wenn eine Gegenstelle eine Verbindung zu Ihrem PC über Rückruf aufbauen will, benötigt der Client diese Rufnummer in diesem Feld, um den Rückruf, entsprechend des gewählten Rückrufmodus annehmen zu können.

Alternative Rufnummern

Möglicherweise ist das Zielsystem ein Network Access Server (NAS), der mit mehreren Anschlüssen für verschiedene Rufnummern ausgestattet ist. In diesen Fall empfiehlt es sich, alternative Rufnummern einzugeben – falls zum Beispiel die erste

Nummer besetzt ist. Die alternativen Rufnummern werden der ersten Nummer angehängt, nur mit einem Doppelpunkt (:) oder einem Semikolon (;) getrennt. Maximal werden 8 alternative Rufnummern unterstützt.

Die erste Nummer ist die Standard-Rufnummer und wird immer zuerst gewählt. Kann keine Verbindung hergestellt werden, weil besetzt ist, wird die zweite Nummer gewählt, usw.

Wichtig: Bitte beachten Sie, dass der Verbindungsaufbau nur funktionieren kann, wenn die Protokoll-Eigenschaften für die Anschlüsse der alternativen Rufnummern die gleichen sind.

PPTP-Endpunkt

Dieser Parameter wird nur eingeblendet, wenn in den Grundeinstellungen das Verbindungsmedium PPTP gewählt wurde. Wird dieses Protokoll gewählt, so muss hier die IP-Adresse des Access-Routers im xDSL eingetragen werden.

Script-Datei

Wenn Sie den Microsoft DFÜ-Dialer benutzen, tragen Sie hier die Script-Datei unter Eingabe von Pfad und Namen ein. (Siehe oben Grundeinstellungen / Einwahl über Windows-DFÜ).

Unterstützung der internationalen Einwahl für verschiedene Dienstanbieter

Folgende Provider stellen Auslandstelefonbücher mit den entsprechenden Einwahlpunkten zur Verfügung, die vom Secure Client unterstützt werden: Gric, InfoNet, iPass, T-Online und UUNet. Soll ein Auslandstelefonbuch genutzt werden, muss das Software-Modul für “Internationale Einwahl” installiert werden. (Dieses Modul erhalten Sie auf Anfrage von NCP.)

Die Auswahl des gewünschten Telefonbuchs erfolgt im Setup-Programm. Damit im Telefonbuch die Rufnummer der Internationalen Einwahl benutzt wird, muss statt der “Rufnummer (Ziel)” der jeweilige Name des Providers eingetragen werden:

Provider	Eintrag “Rufnummer (Ziel)”
T-Online	T-Online
UUNet	UUNET
InfoNet	INFONET
Gric	GRIC

Modem

Dieses Parameterfeld erscheint ausschließlich, wenn Sie als Verbindungsmedium ”Modem” gewählt haben. Alle nötigen Parameter zu diesem Verbindungsmedium sind hier gesammelt.

Achten Sie darauf, dass Ihr Modem bereits vor der Konfiguration installiert ist. Normalerweise haben Sie auf Ihrem Rechner bzw. Notebook bereits ein (integriertes) Modem installiert. Legen Sie nun über den Assistenten für ein neues Profil einen neuen Eintrag mit dem Verbindungsmedium Modem an, so können Sie bereits in diesem Assistenten aus einer Auswahlbox Ihr Modem auswählen. Alle zugehörigen Parameter werden dabei automatisch von der Client Software übernommen, sodass für Sie eine Konfiguration in diesem Parameterfeld entfällt.

Anschluss

Sind bereits Modems installiert, so wird der während dieser Installation festgesetzte Com Port automatisch übernommen, sobald das entsprechende Gerät unter “Modemtyp” selektiert ist.

Baudrate

Die Baudrate beschreibt die Übertragungsgeschwindigkeit zwischen Com Port und Modem. Sie wird bei selektiertem Modemtyp automatisch übernommen. Sollte die Baudrate des Modesm nicht mit einem der hier möglichen Werte übereinstimmen, wählen Sie die nächsthöhere Baudrate. Folgende Baudraten können gewählt werden: 1200, 2400, 4800, 9600, 19200, 38400, 57600 und 115200.

Com Port freigeben

Wenn Sie für Ihren Client ein analoges Modem verwenden, kann es wünschenswert sein, dass der Com Port nach Beendigung der Kommunikation für andere Applikationen freigegeben wird (z. B. Fax). In diesem Fall stellen Sie den Parameter auf “Ein”. Solange der Parameter in der Standardstellung auf ”Aus” bleibt, wird der Com Port ausschließlich von der Client Software genutzt.

Modemtyp

Die Geräte, die Sie in der Windows-Systemsteuerung unter “Modems” konfiguriert haben, werden für dieses Konfigurationsfeld zur Auswahl gestellt. Je nachdem, welches Modem Sie wählen, werden die zugehörigen Parameter ”Com Port” und “Modem Init. String” automatisch in die Konfigurationsfelder aus der Treiberdatenbank des Systems übernommen.

Modem Init. String

Sofern Ihr Modem korrekt im Windows-System installiert ist, wird der entsprechende “Modem Init. String” automatisch in dieses Feld übernommen. In Ausnahmefällen kann der String mit (Hayes-) Befehlen erweitert werden.

Jeder AT-Befehl innerhalb des Initialisierungs-Strings muss mit <cr> abgeschlossen werden, da ansonsten das Kommando nicht abgesetzt wird. Dies bedeutet, dass in jedem Fall der Init-String mit <cr> abgeschlossen werden muss.

Dial Prefix

Dieses Feld ist optional. Ist das Modem korrekt installiert und steht der Software als Standardtreiber zur Verfügung, so muss hier kein Eintrag vorgenommen werden. Der Dial Prefix ist nur in seltenen Ausnahmefällen nötig. Ziehen Sie dazu das Modem-Handbuch zu Rate. Im folgenden einige Beispiele für Dial Prefix:
ATDT
ATDP
ATDI
ATDX

GPRS / UMTS

Wenn Sie das Verbindungsmedium GPRS / UMTS verwenden, wird dieses Parameterfeld eingeblendet. Beachten Sie auch die Beschreibung zu **Mobile-Computing**.

Hier stehen drei Konfigurationsmodi zur Auswahl. In der Standardeinstellung kann aus einer Provider-Liste der gewünschte Anbieter ausgewählt werden. (Sollte Ihr Provider noch nicht aufgeführt sein, so können Sie die Liste mit den Daten zu Ihrem Provider erweitern; sie befindet sich als APN.INI-Datei im Installationsverzeichnis).

Im zweiten Modus wird die APN aus der SIM-Karte gelesen (derzeit nur für T-Mobile). Schließlich kann der benutzerdefinierte Konfigurationsmodus eingestellt werden, wobei alle Daten manuell eingegeben werden müssen.

APN

Den APN erhalten Sie von Ihrem Provider. Er kann auch manuell eingetragen oder aus der Provider-Liste gelesen werden. Für Vodafone lautet er “web.vodafone.de”, für T-Mobile “internet.td1.de”. Der APN (Access Point Name) wird insbesondere zu administrativen Zwecken genutzt.

Benutzername, Passwort

Als Zugangsdaten für den Internetdienstanbieter (Mobilfunk-Provider) muss im Modus “APN von SIM-Karte” und im benutzerdefinierten Konfigurationsmodus ein beliebiger Benutzername und ein beliebiges Passwort eingegeben werden, es sei denn, Sie haben vom Provider spezielle Kennwörter erhalten. Bei Vodafone und T-Online genügen Dummy-Werte.

Einwahlnummer

Als “Einwahlnummer” muss je nach Funkkarte und Provider eine bestimmte Zeichenfolge eingegeben werden, die der Multifunktions-Karte (UMTS-Karte) mitteilt, welche Art Datenverbindung aufgebaut werden soll. Im Regelfall lautet diese *99# (sollte der Verbindungsaufbau nicht möglich sein, kontaktieren Sie die Hotline Ihres Mobilfunkanbieters).

SIM PIN

Benutzen Sie eine SIM-Einsteckkarte für GPRS oder UMTS, so geben Sie hier die PIN für diese Karte ein. Wird die SIM PIN nicht eingetragen, so wird sie beim Verbindungsaufbau mit diesem Profil abgefragt. Dabei können Sie entscheiden; ob sie für dieses Profil gespeichert werden soll.

Benutzen Sie ein Mobiltelefon, so wird die SIM PIN bei Einschalten des Handys bereits eingegeben.

HTTP-Anmeldung

Mit den Einstellungen in diesem Parameterfeld wird die Anmeldung am Hotspot automatisiert. Zentral erstellte Anmelde-Scripts und die hinterlegten Anmeldedaten können vom Access Point (Hotspot) übernommen werden, ohne dass ein Browserfenster geöffnet wird.

Die Automatisierung der Hotspot-Anmeldung geschieht in der Weise, dass bei einem Verbindungsaufbau zum Access Point von dort ein HTTP Redirect an den Client mit einer Website zur Anmeldung erfolgt. Anstatt eines Browser-Starts zur HTTP-Authentisierung, erfolgt mit den hier gemachten Eingaben die Authentisierung automatisch im Hintergrund.

Bitte beachten Sie, dass die Verbindung über einen Hotspot-Betreiber gebührenpflichtig ist. Sie müssen den Geschäftsbedingungen des Hotspot-Betreibers zustimmen, wenn die Verbindung aufgebaut werden soll.

Für die script-gesteuerte Anmeldung kann ein Script aus dem Installationsverzeichnis
`<install>\scripts\samples`
für weitere Hotspots entsprechend angepasst werden.

Bei der Verbindungsart WLAN werden die Authentisierungsdaten für den Hotspot aus den WLAN-Einstellungen übernommen, bzw. wenn diese deaktiviert sind, aus dem Management Tool der WLAN-Karte.

Benutzername | HTTP-Anmeldung

Dies ist der Benutzername, den Sie von Ihrem Hotspot-Betreiber erhalten haben.

Passwort | HTTP-Anmeldung

Dies ist das Passwort, das Sie von Ihrem Hotspot-Betreiber erhalten haben. Das Passwort wird mit verdeckter Schreibweise (mit *) eingegeben.

Passwort speichern | HTTP-Anmeldung

Nachdem das Passwort eingegeben wurde, kann es gespeichert werden

HTTP Authentisierungs-Script | HTTP-Anm.

Hier kann nach Klick auf den Suchen-Button [...] das hinterlegte Anmelde-Script selektiert werden.

Um eingehende Zertifikate bei der HTTP-Authentisierung überprüfen zu können, muss im Script die Variable CACERTDIR gesetzt worden sein. Desweiteren können auch Inhalte des WEB Server-Zertifikats überprüft werden. Hierzu stehen weitere Variablen zur Verfügung:

`CACERTVERIFY_SUBJECT`
überprüft den Inhalt des Subjects (z.B. cn=WEB Server 1)

`CACERTVERIFY_ISSUER`
Überprüft den Inhalt der Issuers

`CACERTVERIFY_FINGERPRINT`
überprüft den MD5 Fingerprint des Aussteller-Zertifiats

Stimmt der Inhalt der Variable mit dem eingegebenen Zertifikat nicht überein, wird die SSL-Verbindung nicht hergestellt und eine Log-Meldung im Monitor ausgegeben.

Verbindungssteuerung

In diesem Parameterfeld bestimmen Sie, wie der Verbindungsaufbau erfolgen soll und stellen die Timeout-Werte ein. Zudem können Sie Kompression aktivieren und die Art der Kompression bestimmen. Mit Kompression kann der Datendurchsatz um den Faktor 3 bis 5 erhöht werden, je nachdem um welche Daten es sich handelt.

Wird das Verbindungsmedium ISDN eingesetzt, kann eine Kanalbündelung aktiviert werden. Bitte beachten Sie dabei, dass die Kanalbündelung nur funktionieren kann, wenn sowohl der Client als auch die Gegenstelle über gleich viele mögliche B-Kanäle verfügen.

Verbindungsaufbau

Für den Verbindungsaufbau zur Gegenstelle stehen drei Modi zur Wahl. (Beachten Sie dazu auch die Beschreibung Secure-Client-Monitor-d.pdf):

automatisch (Standard) Dies bedeutet, dass die Client Software die Verbindung automatisch herstellt. Das Trennen der Verbindung erfolgt je nach Protokoll Ihres Systems, entsprechend den Anforderungen der Anwendung und entsprechend weiterer Einstellungen im Profil.

manuell Dies bedeutet, dass die Verbindung zur Gegenstelle manuell hergestellt werden muss. Ein Trennen der Verbindung erfolgt je nach eingestelltem Wert für den Timeout.

wechselnd Wird dieser Modus gewählt, muss zunächst die Verbindung “manuell” aufgebaut werden. Danach wechselt der Modus je nach Verbindungsabbau:
– Wird die Verbindung mit Timeout beendet, so wird die Verbindung bei der nächsten Anforderung “automatisch” hergestellt,
– wird die Verbindung manuell abgebaut, muss sie auch wieder manuell aufgebaut werden.

Ist der Timeout auf Null (0) gesetzt, d. h. ist kein Timeout eingestellt, so müssen Sie in jedem Fall die Verbindung manuell trennen.

Wichtig: Sollten Sie den Verbindungsaufbau auf “manuell” setzen, so sollten Sie den Timeout aktivieren, um den Verbindungsabbau zu automatisieren. Andernfalls könnten unnötige Verbindungskosten für Sie entstehen.

IP-Adr. halten bei man. Verbindungsaufbau

Wird eine Verbindung getrennt – auch durch Timeout – so verliert der Client standardmäßig die IP-Adresse, die ihm das VPN Gateway aus dem Firmennetz für die Session zugewiesen hatte. Ist die Funktion “IP-Adr. halten bei manuellem Verbindungsaufbau” aktiviert, so behält der Client die IP-Adresse nach Beendigung der Verbindung bis zum nächsten manuellen Verbindungsaufbau, sodass die logische Verbindung ununterbrochen bestehen bleibt.

Diese Funktionalität kann nur für manuellen oder wechselnden Verbindungsaufbau genutzt werden.

Bei Booten verbinden

In manchen Fällen kann es wünschenswert sein, dass die Verbindung zu einer bestimmten Gegenstelle bereits während der Boot-Phase aufgebaut wird – besonderswenn der Remote-PC genauso gebootet werden soll wie der Büro-PC, der an ein LAN angeschlossen ist. Bitte beachten Sie, dass in diesem Fall der Remote-PC so vorkonfiguriert sein muss, dass der Client in den Boot-Prozess einbezogen wird. Wenn Sie “Bei Booten verbinden” aktivieren wollen, schalten Sie dieses Feature auf ”Ein”. Die Standardeinstellung ist “Aus”.

Timeout

Mit diesem Parameter wird der Zeitraum festgelegt, der nach der letzten Datenbewegung (Empfang oder Versenden) verstreichen muss, bevor automatisch ein Verbindungsabbau erfolgt. Der Wert wird in Sekunden zwischen 0 und 65535 angegeben. Der Standardwert ist “100".

Wenn Ihr Anschluss (ISDN oder analog) einen Gebührenimpuls erhält, verwendet die Client Software das Impulsintervall, um den optimalen Zeitpunkt des Verbindungsabbaus bezüglich dem von Ihnen gesetzten Wert zu ermitteln. Der nach Gebührentakt optimierte Timeout läuft im Hintergrund und hilft die Verbindungskosten zu reduzieren.

Hinweis: Um den Timeout zu aktivieren, ist es nötig, einen Wert zwischen 1 und 65356 einzutragen. Der Wert ”0" bedeutet, dass das Trennen der Verbindung manuell durchgeführt werden muss.

Wichtig: Der Timer für das gewählte Zeitintervall läuft erst dann an, wenn keine Datenbewegung oder Handshaking mehr auf der Leitung stattfindet.

Timeout-Richtung

Mit diesem Parameter bestimmen Sie, für welche Übertragungsrichtung der Timeout gelten soll. Drei verschiedene Einstellungen sind möglich:

TxRx (Standard) Der Client achtet sowohl auf das Ende der gesendeten (out) als auch der empfangenen (in) Daten, bevor der Timer angestoßen wird.
Tx Nur die Senderichtung (out) wird beobachtet.
Rx Nur die Empfangsrichtung (in) wird beobachtet.

Kompression

Mit diesem Parameter bestimmen Sie den Typ der eingesetzten Kompression. Drei Einstellungen sind möglich:

Aus (Standard)
STAC (ohne History)
STAC mit History Cisco-kompatibel

Wichtig: Der hier gewählte Typ der Kompression muss auch vom Network Access Server (NAS) unterstützt werden.

Bitte beachten Sie, dass es sich hier nicht um die Kompression einer Übertragung mit IPsec-Daten handelt. Die IPsec-Kompression wird unter den Vorschlägen zur **IPsec-Richtlinie** eingestellt.

Ziehen Sie zu weiteren Informationen bitte Ihren Internet Provider oder Ihren Systemadministrator zu Rate.

Dynamische Linkzuschaltung

Mit dynamischer Linkzuschaltung (für ISDN) kann die Client Software bis zu 8 ISDN B-Kanäle bündeln. Um diese Funktion in vollem Umfang nutzen zu können, muss allerdings der PC wie auch die Gegenstelle mit der nötigen Anzahl von So-Schnittstellen (4) ausgestattet sein.

Mit dynamischer Linkzuschaltung erhöhen sich zwar die Kosten für jeden zugeschalteten B-Kanal, gleichzeitig verringern sie sich jedoch in gleichem Maße, weil sich die Übertragungsdauer entsprechend verkürzt!

Mit diesem Parameter bestimmen Sie, wie die Linkzuschaltung erfolgen soll. Drei Möglichkeiten stehen zur Auswahl:

Aus (Standard)

Tx Links werden zugeschaltet, entsprechend der Bitrate abgehender Daten.

Rx Links werden zugeschaltet, entsprechend der Bitrate eingehender Daten.

TxRx Links werden sowohl nach der Bitrate sowohl eingehender als auch abgehender Daten zugeschaltet.

Schwellwert für Linkzuschaltung

Der Wert dieses Parameters teilt der Client Software die Bitrate mit, ab der ein weiterer Link (Kanal) zugeschaltet werden soll. Der Wert entspricht Prozenten der maximalen Bitrate. Mögliche Werte sind von 1 bis 100 (Prozent). Standardwert ist “20". Diese Einstellung gilt für Sender und Empfänger.

OTP-Token

Wird ein OTP-Token verwendet, so kann statt “Benutzername” und “Passwort” die PIN und das One-time-Passwort des Tokens eingegeben werden. Wofür der OTP-Token genutzt wird, wird mit folgenden Einstellungen bestimmt:

Aus (Standard) OTP wird nicht genutzt

NAS-Einwahl Wird ein OTP für die Verbindung zu einem NAS geutzt, wird das Feld für “Passwort” unter “Netzeinwahl” inaktiv geschaltet.

VPN-Einwahl Wird ein OTP für die Verbindung zum VPN Gateway genutzt, wird entsprechend das Feld für “VPN-Passwort” unter “Tunnel-Parameter” inaktiv geschaltet. Bei

Bei Verbindungsaufbau erscheint ein Dialogfenster für die Eingabe des “Einmalpassworts”, in welches PIN und **Passwort für OTP-Token** eingetragen werden müssen. Werden vom ACE-Server auf Grund des RSA-Tokens Nachrichten versendet, werden diese am Monitor in einem Informationsfenster mit Eingabefeld angezeigt (z. B. “Ablauf der gültigen PIN” oder “Ablauf des OTP-Passworts”). Geben Sie die neue PIN oder das neue Passwort von Ihrem Token in das Eingabefeld ein.

Rückruf

Die Rückruf-Funktion kann nur für Wählverbindungen über die Verbindungsmedien ISDN oder Modem genutzt werden!

Rückruf für ausgehende Verbindungen (Gateway ruft zurück)

Voraussetzungen

Die Art des Rückrufs hängt von den Rechten des Clients ab, die ihm (über seine Benutzer-ID und sein Passwort) vom zentralen Gateway zugewiesen sind.

Bei einer zentralseitig eingerichteten Rückruf-Option kann zwischen zwei Methoden unterschieden werden, welche von den meisten Gateways unterstützt werden. Welche der Methoden eingesetzt wird, wird vom Gateway bestimmt:

1. Fester Rückruf, der immer zu einem Client mit fester Rufnummer ausgeführt wird. Diese Rückruf-Methode wird zum Beispiel bevorzugt dann angewendet, wenn der Teleworker immer vom Home Office aus kommuniziert.

2. Variabler Rückruf wird dann genutzt, wenn sich die Rufnummer ändert (variiert). Diese Methode wird zum Beispiel von mobilen Teleworkern bevorzugt, die den Einsatzort häufig wechseln.

Verhandle PPP Callback

Sie aktivieren die PPP Callback-Verhandlung nur, wenn ein Rückruf vom Gateway erfolgen soll und das Gateway den Rückrufmodus PPP Callback verwendet. Erst dann können Sie auch eine Rückrufnummer eintragen.

Rückrufnummer

Hier tragen Sie die komplette Rufnummer des Clients (max. 30 Stellen) für einen variablen Rückruf ein. Diese Rufnummer wird mit der PPP-Verhandlung beim Verbindungsaufbau vom Client zum Gateway übertragen.

Für einen festen Rückruf muss die Rückrufnummer nicht eingetragen sein, da sie am Gateway hinterlegt ist.

Rückruf für eingehende Verbindungen (Client ruft zurück)

Rückrufmodus

Dieser Parameter wird nur für den Rückruf benötigt, den die Client-Software an das Gateway ausführt. Folgende Modi stehen zur Wahl:

aus (Standardeinstellung) Die Client-Software führt keinen Rückruf aus.

PPP (RFC 1570 konform) wird von den meisten Gateways unterstützt.

NCP (-spezifisch) kann mit dem Secure Enterprise Server eingesetzt werden.

COSO (Charge-One-Side-Only) auch Low-Level- oder D-Kanal-Rückruf. Im ISDN D-Kanal fallen keine (lokalen) Gebühren für den Client an. COSO ist auch Cisco-kompatibel.

Damit die Client-Software einen Rückruf an das Gateway ausführen kann, ist es unbedingt notwendig im Parameterfeld **Eingehende Rufe** folgende Einstellungen vorzunehmen:

☑ Die Client-Software muss abgehende und eingehende Rufe abarbeiten können. Deshalb muss der Parameter **Richtung** in **Eingehende Rufe** auf **bidirektional** gesetzt sein.

☑ Das Gateway muss sich zuerst gegenüber dem Client mit **Benutzername der Gegenstelle** und **Passwort der Gegenstelle** authentisieren (Parameterfeld **Eingehende Rufe**).

☑ Die Client-Software führt den Rückruf an die Rufnummer aus, die im Parameterfeld Netzeinwahl für ”Rufnummer (Ziel)” eingetragen wurde.

☑ Dabei muss sich die Client-Software auch gegenüber dem Gateway ausweisen. Dies geschieht mit Benutzer und Passwort im Parameterfeld “Netzeinwahl”.

Zu weitergehenden Fragen zu diesem Thema befragen Sie bitte Ihren Systemadministrator.

Security

Im Parameterfeld "Security" sind die Konfigurationsparameter zu L2Sec und IPsec für den Einsatz in Remote Access-Umgebungen gesammelt. Je nach eingestelltem Security-Modus, L2Sec oder IPsec, kann eine weitergehende Parametrisierung vorgenommen werden, wobei IPsec sowohl in einem L2TP-Tunnel (over L2TP) als auch ohne L2TP-Tunnel (IPsec native, auch IPsec-Tunneling) gefahren werden kann.

L2Sec*: Dieser Security-Modus wurde in früheren Versionen der Secure Software standardmäßig immer eingesetzt, wenn eine der angebotenen Verschlüsselungsarten gewählt wurde! (In früheren Versionen der Software hieß dieses Konfigurationsfeld "Verschlüsselung").*

IPsec native *oder* **IPsec over L2TP***: Sofern IPsec für Remote Access eingesetzt wird, wird die Secure Policy Database (SPD) nach Vorgabe der hier eingestellten Parameter intern dynamisch aufgebaut (siehe Beschreibung* **IPsec-Funktionalität***). Alle IP-Pakete für dieses Ziel werden über die dynamische SPD abgearbeitet.*

Verschlüsselung: Mit der Verschlüsselung werden wichtige Datenbestände eines Computer-Netzwerks und -Systems geschützt. Vor allem bei der Übertragung sensibler Daten über öffentliche Netze, die jedermann nutzen kann, ist die Verschlüsselung von größter Bedeutung. In der Secure Client Software ist eine Reihe von Sicherheitsmechanismen implementiert, um den Zugriff unautorisierter Personen zu verhindern und eine unbefugte Nutzung auszuschließen. Obwohl Standards zur Verschlüsselung existieren (DES oder AES), sind bislang noch keine ausreichenden Sicherheits-Standards entwickelt worden, die auch für die Interoperabilität zwischen verschiedenen Systemen ähnlich hohe Sicherheit gewähren. Daher ist es unbedingt erforderlich, dass die Gegenstelle des Secure Clients die entsprechend gleichen Standards unterstützt. Weiterhin ist NCP bemüht neu verfügbare Verschlüsselungs-Standard zu implementieren.

Security-Modus

Hier legen Sie den Sicherheits-Standard für eine Verbindung fest, L2Sec oder IPsec. Bitte beachten Sie dabei, dass nur mit L2Sec neben IP-Paketen auch NetBios-, IPX- und SNA-Daten übertragen werden können.

inaktiv
Verschlüsselung und Authentisierung sind ausgeschaltet.

L2Sec
NCP Standard. Alle Sicherheits-Verhandlungen erfolgen verschlüsselt und sicher in einem End to End-Tunnel (Layer 2) zwischen Client und Secure Server. **L2Sec** kann dann eingesetzt werden, wenn als **VPN-Protokoll L2TP** gewählt wird.

IPsec
Dieser Modus ist dann voreingestellt, wenn als **VPN-Protokoll IPsec** gewählt wird (IPsec native). Zusätzlich kann mit dieser Option auch der Standard "IPsec im Tunnel-Modus" (Layer 3) eingesetzt werden, wenn das **VPN-Protokoll L2TP** gewählt wird. Dies bewirkt, dass über jeden Provider-Medientyp auf Layer-2 (dies sind alle Verbindungsmedien mit L2TP) zwischen Client und Secure Server zusätzlich IPsec gefahren wird, d. h. **IPsec over L2TP**.

Zertifikatskonfiguration

Ein über die Zertifikatskonfiguration des Client-Monitors eingesetztes Zertifikat, kann hier für die Verschlüsselung und Authentisierung im Security-Modus L2Sec oder für die erweiterte Authentisierung (Extended Authentication) im Security-Modus IPsec selektiert werden. (Siehe Beschreibung **Zertifikate**.)

Sind mehrere Zertifikatskonfigurationen angelegt, so kann für dieses Profil über den Namen der Zertifikatskonfiguration das gewünschte Zertifikat selektiert werden. (siehe unten **Extended Authentication** und **VPN-Benutzername**).

keine
Für Datenverschlüsselung und Authentisierung wird kein Zertifikat eingesetzt.

Standard PKI-Konfiguration
Die Zertifikatskonfiguration eines Clients älter als Version 9.1 wird bei einem Update auf diese Version automatisch in die Standard PKI-Konfiguration konvertiert. Ebenso wird die Standard PKI-Konfiguration nach einer Erstinstallation der Version 9.1 eingerichtet wenn eine Testverbindung mit Zertifikat angelegt wird.

Verschlüsselung (L2Sec)

In diesem Feld bestimmen Sie, ob im Security-Modus L2Sec eine Verschlüsselung eingesetzt wird, und welche Art der Verschlüsselung verwendet werden soll.

keine
Verschlüsselung nicht aktiv (standard)

von Gegenstelle bestimmt
Die Daten werden je nach Verschlüsselungstechnik des Gateways (Zielsystems) nach Blowfish 128 / 448 oder Triple DES verschlüsselt übertragen.

SSL mit Zertifikat
Mit dieser Verschlüsselung ist ein Verbindungsaufbau nur möglich, wenn vorher eine gültige PIN eingegeben wurde. Diese Verschlüsselungsart (wie auch Blowfish und 3DES unter " Von Gegenstelle bestimmt") wird vom zentralen Gateway vorgegeben.

Statischer Schlüssel | Security

Der Schlüssel kann nur eingegeben werden, wenn vorher die Verschlüsselung aktiviert wurde. Der Schlüssel muss abgestimmt sein mit dem in der Konfiguration der Gegenstelle (Gateway). Er ist ein String mit 16 hexadezimalen Zahlen, die durch einen Punkt (.) getrennt sind. Standard ist:
00.11.22.33.44.55.66.77.88.99.AA.BB.CC.DD.EE.FF

Pre-shared Key | Security

Der Pre-shared Key ist ein String beliebiger Zeichen in einer maximalen Länge von 255 Zeichen. Der Pre-shared Key muss nur dann eingegeben werden, wenn eine Verbindung mit "IPsec-Tunneling" zu einem fremden IPsec Gateway aufgebaut werden soll und diese Gegenstelle als IKE-Richtlinie "Pre-shared Key" erwartet.

Richtlinien

Bitte beachten Sie zur Auswahl der Richtlinien auch die Beschreibung zur IPsec-Konfiguration. Standardmäßig werden mit der Client Software die Richtlinien mitgeliefert, die modifiziert werden können, sofern der IPsec Client spezielle Richtlinien verwenden soll. Klicken Sie dazu auf IPsec-Konfiguration.

IKE-Richtlinie | Security

Die IKE-Richtlinie wird aus der Listbox selektiert. (Vorkonfiguriert befinden sich dort: "Pre-shared Key" und "RSA-Signatur"). In der Listbox werden namentlich alle IKE-Richtlinien aufgeführt, die bei der IPsec-Konfiguration angelegt wurden.

automatischer Modus
In diesem Fall kann die Konfiguration der IKE-Richtlinie über die IPsec-Konfiguration entfallen.

Pre-shared Key
Diese vorkonfigurierte Richtlinie kann ohne PKI-Unterstützung genutzt werden. Beidseitig wird der gleiche "Pre-shared Key" verwendet (siehe oben "Pre-shared Key").

RSA-Signatur
Diese vorkonfigurierte Richtlinie kann nur mit PKI-Unterstützung eingesetzt werden. Als zusätzliche, verstärkte Authentisierung ist der Einsatz der RSA-Signatur nur sinnvoll unter Verwendung einer Smartcard oder eines Soft-Zertifikats.

IPsec-Richtlinie | Security

Die IPsec-Richtlinie wird aus der Listbox selektiert. (Vorkonfiguriert befindet sich dort: "ESP - 3DES - MD5"). In der Listbox werden namentlich alle IPsec-Richtlinien aufgeführt, die bei der IPsec-Konfiguration angelegt wurden.

automatischer Modus
In diesem Fall kann die Konfiguration der IPsec-Richtlinie über die IPsec-Konfiguration entfallen.

ESP - 3DES - MD5
Wird diese vorkonfigurierte IPsec-Richtlinie gewählt, muss die gleiche Richtlinie mit ihren Vorschlägen für alle Benutzer gültig sein. Dies bedeutet, dass sowohl auf Client- als auch auf Server-Seite die gleichen Vorschläge für die Richtlinien zur Verfügung stehen müssen.

Austausch-Modus | Security

Der Austausch-Modus bestimmt in welcher Weise der Internet Key Exchange vonstatten gehen soll. Zwei unterschiedliche Modi stehen zur Verfügung, der Main Mode, auch Identity Protection Mode und der Aggressive Mode. Die Modi unterscheiden sich durch die Anzahl der Messages und durch deren Verschlüsselung (siehe **IPsec-Funktionalität**).

Main Mode
Im Main Mode (Standard-Einstellung) werden sechs Meldungen über den Kontrollkanal geschickt, wobei die beiden letzten, welche die User ID, das Zertifikat die Signatur und ggf. einen Hash-Wert beinhalten, verschlüsselt werden – daher auch "Identity Protection Mode".

Aggressive Mode
Im Aggressive Mode gehen nur drei Meldungen ohne Verschlüsselung über den Kontrollkanal.

Entsprechend des Security-Modus IPsec können noch detailliertere Sicherheitseinstellungen vorgenommen werden.

IKE ID-Typ | Security

Bei native IPsec wird zwischen abgehenden und eingehenden Verbindungen unterschieden. Der Wert, den der Initiator als ID für eine abgehende Verbindung gewählt hat, muss bei der Gegenstelle als ID für eingehende Verbindungen gewählt sein. Folgende ID-Typen stehen zur Auswahl:

– IP-Adresse
– Fully Qualified Domain Name
– Fully Qualified Username
– IP Subnet-Adresse
– ASN1 Distinguished Name
– ASN1 Gruppen-Name
– String für Gruppenidentifikation

IKE ID | Security

Der Wert, den der IPsec-Initiator als ID für eine abgehende Verbindung gewählt hat, muss bei der Gegenstelle als ID für eingehende Verbindungen gewählt sein.

Entsprechend dem ID-Typ muss die zugehörige ID als String eingetragen werden.

Link-Einstellungen

Die Einstellungen in diesem Parameterfeld hängen vom Network Access Server der jeweiligen Gegenstelle ab. Um weitere Informationen zu bekommen, konsultieren Sie dazu Ihren Systemadministrator oder Ihren Internet Service Provider.

Eingehende Verbindungen blockieeren

In der Standardeinstellung ist dieser Schalter gesetzt und eine Verbindung von einem Rechner aus dem angebundenen Netz auf diesen Rechner ist nicht möglich!

Wenn dieser Schalter entfernt wird, kann eine Verbindung aktiv von außerhalb aufgebaut werden, und die Gegenstelle kann auf den Rechner zugreifen.

Bitte beachten Sie, dass es nur sinnvoll ist, diesen Schalter zu entfernen wenn der Zugriff von einer definierten Gegenstelle aus erfolgt, z. B. aus dem Firmennetz, da mit dem Setzen dieses Schalters der Schutzmechanismus der Stateful Inspection Firewall aufgehoben wird. D. h. potentiell kann jeder Teilnehmer aus dem angebundenen Netz auf den Rechner mit der Client Software zugreifen.

IP Broadcast erlaubt

Mit diesem Parameter entscheiden Sie, ob die Client Software die Übertragung von IP-Broadcasts zulassen soll. IP-Broadcasts werden z. B. dann eingesetzt, wenn ein LAN-Client (wie etwa die Client Software) im Netz nach einem File Server sucht. Im Fall des Clients wäre das Netz ein Remote-LAN, an welches der Client angeschlossen ist.

IP-Broadcasts werden unterdrückt, wenn das Feld nicht angeklickt ist (standard).

IP-Broadcasts müssen Sie zulassen, wenn Sie DHCP nutzen um eine IP-Adresse vom Zielsystem anfordern zu können.

NetBIOS über IP

Mit diesem Parameter wird ein Filter aufgehoben, der Microsoft NetBIOS-Frames unterdrückt. Dies ist immer dann zweckmäßig, wenn Sie zum Beispiel Microsoft Networking über den Client nutzen.

In der Standardeinstellung ist dieser Filter gesetzt, das heißt der Checkbutton ist *nicht* mit einem Haken markiert, so dass Microsoft NetBIOS-Frames unterdrückt werden, damit sie den Datenverkehr nicht unnötig belasten. Markieren Sie den Checkbutton mit einem Haken, werden NetBIOS-Frames over IP erlaubt.

Voice over IP (VoIP) priorisieren

Wird dieser Client für Kommunikation mit Voice over IP genutzt, so sollte diese Funktion aktiviert werden, um die Sprachdaten verzögerungs- und verzerrungsfrei senden und empfangen zu können.

MAC-Adresse

Die MAC-Adresse ist die Adresse des Netzwerk-Adapters im LAN. Sie kann zum Zweck der Identifikation (DHCP) eingesetzt werden. Sie ist eine Adresse mit 6 hexadezimalen Zahlen, die durch einen Punkt “.” getrennt sind.

Die Standardadresse ist 00.00.00.00.00.00

Ziehen Sie bei diesem Parameter Ihren Internet Provider oder Ihren Systemadministrator zu Rate.

Authentisierung vor VPN

Dieses Konfigurationsfeld ist nur für die Verbindungsmedien "LAN" oder "WLAN" von Bedeutung, bzw. dann wenn ein externer Dialer eingesetzt wird oder das Profil für die automatische Medienerkennung konfiguriert wurde. Welche Authentisierung vor dem Tunnelaufbau erforderlich ist, ist vom jeweiligen Netzwerk abhängig.

Bitte beachten Sie im WLAN, dass die Verbindung über einen Hotspot-Betreiber gebührenpflichtig ist und Sie den Geschäftsbedingungen des Hotspotbetreibers zustimmen müssen, wenn die Verbindung aufgebaut werden soll. Beachten Sie auch die Beschreibungen zu **Grundeinstellungen** *und* **Verbindungsmedium**.

EAP-Authentisierung

Muss sich der Client mit EAP (Extensible Authentication Protocol) authentisieren, so muss diese Funktion aktiviert werden. Sie bewirkt, dass für dieses Profil die EAP-Konfiguration im Monitor-Menü unter "EAP-Optionen" eingesetzt wird.

Bitte beachten Sie, dass die EAP-Konfiguration im Monitor-Menü für *alle* Zielsysteme gültig ist und aktiv geschaltet sein muss, wenn diese linkspezifische Einstellung wirksam sein soll.

EAP wird dann eingesetzt, wenn für das wireless LAN ein Access Point verwendet wird, der 802.1x-fähig ist und eine entsprechende Authentisierung verlangt.

EAP kann aber auch dann eingesetzt werden, wenn der Client über einen Router auf ein anderes Netzsegment des Firmennetzes zugreifen möchte.

Generell wird mit EAP verhindert, dass sich unberechtigte Benutzer über die Hardware-Schnittstelle in das LAN einklinken.

Nach Konfiguration des EAP muss eine Statusanzeige im grafischen Feld des Monitors erscheinen. Ist dies nicht der Fall, so muss die EAP-Konfiguration im Monitor-Menü aktiv geschaltet werden. Durch einen Doppelklick auf das EAP-Symbol kann das EAP zurückgesetzt werden. Anschließend erfolgt die EAP-Verhandlung erneut.

Siehe dazu auch die Beschreibung **Secure-Client-Monitor**.

HTTP-Authentisierung

Für die automatische HTTP-Authentisierung am Access Point (Hotspot) muss diese Funktion aktiviert werden.

Damit wird ein weiteres Konfigurationsfeld in den Profil-Einstellungen zugeschaltet, in welches die Authentisierungsdaten eingegeben werden können. (Klicken Sie dazu auf **HTTP-Anmeldung**)

Bei einem Link mit der Verbindungsart WLAN wird die HTTP-Anmeldung nicht zugeschaltet!

Statt dessen wird mit der Aktivierung dieser Funktion bewirkt, dass für dieses Profil die Authentisierungsdaten aus den WLAN-Einstellungen im Monitor-Menü zum Einsatz kommen.

Beachten Sie dazu die Beschreibung **WLAN-und-Hotspot-Anmeldung**.

Tunnel-Parameter

Diese Parameter sind nur von Bedeutung, wenn zwischen dem Client und dem VPN-Gateway ein Tunnel (VPN) aufgebaut werden soll, d.h. das Zielsystem IPsec oder L2TP unterstützt. Die jeweiligen Einstellungen hängen vom Network Access Server des Zielsystems (VPN-Gateway) ab. Wenn Sie unsicher bei der jeweiligen Einstellung sind, wenden Sie sich bitte an Ihren Systemadministrator oder Ihren Internet Service Provider.

VPN-Protokoll

Nicht benutzen

Zwischen dem Client und dem Zielsystem wird kein Tunnel aufgebaut.

L2TP

Mit diesem Schalter bestimmen Sie, ob das L2TP-Protokoll (Layer 2 Tunneling Protokoll) gefahren werden soll. Wird dieses VPN-Protokoll genutzt, können Sie wahlweise den Security-Modus **L2Sec** oder **IPsec** zuschalten. Setzen Sie zum VPN-Protokoll L2TP den Security-Modus IPsec ein, beachten Sie bitte die Beschreibung **IPsec over L2TP**.

IPsec-Tunneling

Wird IPsec-Tunneling als VPN-Protokoll gewählt, so wird die native IPsec-Verbindung ohne einen Layer 2-Tunnel (L2TP) zu einem reinen IPsec Gateway hergestellt.

Beachten Sie bei Einsatz von native IPsec die Beschreibung zur IPsec-Konfiguration in diesem Handbuch, sowie die PDF-Datei IPsec Funktionalität und Konfiguration.

Verbindung zu reinen IPsec Gateways

Bei Auswahl von IPsec-Tunneling werden Sie darauf hingewiesen, dass im Security-Konfigurationsfeld automatisch folgende Einstellungen vorgenommen werden:

Security-Modus = IPsec
IKE-Richtlinie = automatischer Modus
IPsec-Richtlinie = automatischer Modus
Austausch-Modus = Main Mode

*Diese automatisch vorgenommenen Einstellungen können entsprechend den Anforderungen des IPsec Gateways auch modifiziert werden. (Klicken Sie dazu auf **Security**). Weiterhin ist für den Einsatz von IPsec-Tunneling folgendes zu beachten:*

Im Konfigurationsfeld Security werden die Parameter IKE ID-Typ und IKE ID zur Konfiguration eingeblendet. Entsprechend den Vorgaben durch die Gegenstelle kann als IKE-Richtlinie die automatisch vorgenommene Einstellung "von Gegenstelle bestimmt" auf Pre-shared Key oder RSA Signatur (Zertifikat) abgeändert werden. Erwartet die Gegenstelle Pre-shared Key, so muss der Schlüssel in das Feld eingetragen werden. (Der Pre-shared Key muss in diesem Fall für alle Clients identisch sein.)

*IP-Adressen und DNS-Server werden über das Protokoll IKE-Config Mode (Draft 2) zugewiesen (kompatibel derzeit nur gegen Cisco). Für die NAS-Einwahl können alle bisherigen WAN-Schnittstellen verwendet werden. (Klicken Sie auf **IPsec-Adresszuweisung**.)*

*Wird IPsec-Tunneling genutzt, so erfolgt die Authentisierung in der Standardeinstellung des Enterprise Clients über Extended Authentication (XAUTH Protokoll, Draft 6). [Extended Authentication kann ausgeschaltet werden im Konfigurationsfeld **Erweiterte IPsec-Optionen**.] Dazu müssen noch folgende Parameter gesetzt werden:*

VPN-Benutzername = Benutzername des IPsec-Benutzers
VPN-Passwort = Kennwort des IPsec-Benutzers
Verwende VPN-Benutzername und -Passwort von = optional

(Siehe nächste Seite)

Bei IPsec-Tunneling wird im Hintergrund automatisch DPD (Dead Peer Detection) und NAT-T (NAT Traversal) ausgeführt, falls dies von der Gegenstelle unterstützt wird. Mit DPD prüft der IPsec Client in bestimmten Abständen, ob die Gegenstelle noch aktiv ist. Bei inaktiver Gegenstelle erfolgt ein automatischer Verbindungsabbau. Der Einsatz von NAT Traversal erfolgt beim IPsec Client automatisch und ist immer nötig wenn auf der Remote-Seite ein Gerät mit Network Address Translation zum Einsatz kommt.

VPN-Benutzername

Den Benutzernamen für das VPN-Gateway erhalten Sie von Ihrem Systemadministrator. Der Name kann bis zu 255 Zeichen lang sein.

VPN-Passwort

Das Passwort für das VPN-Gateway erhalten Sie von Ihrem Systemadministrator. Das Passwort kann bis zu 128 Zeichen lang sein.

Tunnel Secret

Dies ein Passwort, das für den Tunnelaufbau benötigt wird. Nur wenn dieses Passwort beim VPN-Gateway und dem VPN-Client übereinstimmt, wird der Tunnel aufgebaut. Das Passwort kann bis zu 16 Zeichen lang sein.

Gateway (Tunnel-Endpunkt)

An dieser Stelle muss die Adresse bzw. der Tunnel-Endpunkt des Gateways eingetragen werden. Sie erhalten sie von Ihrem Administrator entweder als IP-Adresse oder als Namens-String.

IP-Adresse
Wenn das Gateway über eine feste offizielle IP-Adresse verfügt, kann die IP-Adresse eingetragen werden.

Namens-String
Wenn das Gateway wechselnde IP-Adressen von einem Internet Service Provider erhält, so wird hier der Namns-String eingetragen. Es handelt sich dabei um den DNS-Namen des Gateways, der beim DynDNS Service Provider hinterlegt wurde.

In der gleichen Syntax kann ein zweites Gateway, nach dem ersten durch ein Semikolon getrennt, eingetragen werden.

Separates IPsec Gateway für Enterprise Clients
Wird ein L2TP-Tunnel aufgebaut, so ist dies der Endpunkt des L2TP-Tunnels.

Wird IPsec over L2TP genutzt, also sowohl ein Layer 3- als auch ein Layer 2-Tunnel aufgebaut, so ist dies für beide Tunnel der Endpunkt, sofern zu *keinem separaten* IPsec Gateway mit dem Layer 3-Tunnel eine Verbindung hergestellt werden soll.

Wird für IPsec ein separates Gateway eingesetzt, so ist die hier eingegebene IP-Adresse der Tunnel-Endpunkt für den L2TP-Tunnel und der Tunnel-Endpunkt bzw. die Zieladresse des IPsec Gateways wird im Konfigurationsfeld **Erweiterte IPsec-Optionen** eingegeben. (Klicken Sie dazu hier.)

Zugangsdaten aus ...

Als Zugangsdaten für ein VPN können folgende Einträge ausgelesen und verwendet werden:

Konfiguration
Dies bedeutet, dass VPN-Benutzername und VPN-Passwort aus diesem Konfigurationsfeld zur VPN-Authentisierung verwendet werden.

Zertifikatsfeld (E-Mail)
Dies bedeutet, dass statt VPN-Benutzername und VPN-Passwort der E-Mail-Eintrag des Zertifikats verwendet wird.

Zertifikatsfeld (Common Name)
Dies bedeutet, dass statt VPN-Benutzername und VPN-Passwort der Benutzer-Eintrag des Zertifikats verwendet wird.

Zertifikatsfeld (Seriennummer)
Dies bedeutet, dass statt VPN-Benutzername und VPN-Passwort die Seriennummer des Zertifikats verwendet wird.

Zertifikatsfeld (Universal Principal Name, UPN)
Dies bedeutet, dass statt “Benutzername” und “Passwort” der Universal Principal Name (Anmeldename@Domain-Name) verwendet wird, vorausgesetzt das Attribut ist im Zertifikat vorhanden.

Beachten Sie, dass diese Einträge auch für den Einsatz von **Extended Authentication** bei IPsec-Verbindungen genutzt werden können.

Vergleichen Sie dazu die obige Beschreibung **Verbindung zu reinen IPsec Gateways** und die Beschreibung zu Extended Authentication im Konfigurationsfeld **Erweiterte IPsec-Optionen**. (Klicken Sie dazu hier.)

Beachten Sie dazu auch die Beschreibung **Zertifikate**.

Erweiterte IPsec-Optionen

Bei Einsatz des Security-Modus IPsec wird dieses Konfigurationsfeld eingeblendet. Mit diesen Parametern können Einstellungen für eine Client-Server-Verbindung mit IPsec native und IPsec over L2TP vorgenommen werden. Wird IPsec over L2TP eingesetzt, so kann hier für den Layer 3 IPsec-Tunnel eine andere Zieladresse angegeben werden wie für den Layer 2 L2TP-Tunnel, sodass ein eigenes IPsec Gateway eingesetzt werden kann, das nicht von NCP stammt.

Deaktiviere DPD (Dead Peer Detection)

Mit dieser Funktion kann DPD ausgeschaltet werden.

DPD (Dead Peer Detection) und NAT-T (NAT Traversal) werden automatisch im Hintergrund ausgeführt, sofern dies das Ziel-Gateway unterstützt. Der IPsec Client nutzt DPD, um in regelmäßigen Intervallen, die in Sekunden eingestellt werden können, zu prüfen, ob die Gegenstelle noch aktiv ist. Ist dies nicht der Fall, erfolgt ein automatischer Verbindungsabbau.

Mit DPD (Dead Peer Detection) wird das VPN Gateway (nach eingestelltem Zeitintervall), unabhängig vom tatsächlichen Nutzdatenverkehr, “angepingt” und der Tunnel abgebaut, wenn keine Antwort vom Gateway erfolgt oder der Timeout abgelaufen ist (unabhängig vom Datenaufkommen).

Zieladresse IPsec Gateway

Bei Verbindungen mit IPsec over L2TP können für den Layer 3- und den Layer 2-Tunnel getrennte Zieladressen zu den jeweiligen Gateways angegeben werden. An dieser Stelle kann der Endpunkt des Layer 3-Tunnels bzw. die Zieladresse des IPsec Gateways eingetragen werden, im Konfigurationsfeld **Tunnel-Parameter** wird der Tunnel-Endpunkt (Ziel) für den Layer 2-Tunnel eingetragen. (Klikken Sie dazu hier.)

Wird hier *keine* separate Zieladresse für das IPsec Gateway eingetragen, so wird auch für das IPsec Gateway der Tunnel-Endpunkt (Ziel) verwendet, der auf jeden Fall eingetragen werden muss.

Bei Verbindungen mit IPsec native wird diese Option ausgegraut, da als Zieladresse für das IPsec Gateway der Tunnel-Endpunkt (Ziel) aus dem Konfigurationsfeld “Tunnel-Parameter” verwendet wird.

Die erweiterte Authentisierung kann nur für Verbindungen mit IPsec native eingesetzt werden und ist am Enterprise Client bei diesem Tunnel-Protokoll standardmäßig aktiviert. In diesem Konfigurationsfeld kann sie deaktiviert werden.

Extended Authentication (XAUTH)

Um Extended Authentication (XAUTH Protokoll, Draft 6) mit IPsec native nutzen zu können, muss es vom IPsec Gateway unterstützt werden. Wird XAUTH vom Gateway nicht unterstützt, so muss es hier ausgeschaltet werden, da ansonsten keine Verbindung zustande kommt.

Wird XAUTH vom Gateway unterstützt, so belassen Sie die erweiterte Authentisierung (XAUTH) aktiviert. Zusätzlich zum Pre-shared Key werden dann noch folgende Parameter aus dem Konfigurationsfeld Tunnel-Parameter zur Authentisierung genutzt:

VPN-Benutzername
Benutzername des IPsec-Benutzers, max. 255 Zeichen.

VPN-Passwort
Kennwort des IPsec-Benutzers, max. 128 Zeichen.

VPN-Benutzername und VPN-Passwort werden im Konfiguratiuonsfeld **Tunnel-Parameter** eingegeben, wo alternativ auch bestimmt werden kann, dass sie aus einer Zertifikatskonfiguration ausgelesen werden. (Klicken Sie dazu hier.)

Standard IPsec / UDP Encapsulation

Standard IPsec (Port 500) und UPD Encapsulation können alternativ verwendet werden.

Mit UDP-Encapsulation muss an der externen Firewall nur der Port 4500 freigeschaltet werden (anders bei NAT Traversal oder UDP 500 mit ESP). Wird die UDP-Encapsulation verwendet, so kann der Port frei gewählt werden.

Standard für IPsec mit UDP ist der Port 4500, für IPsec ohne UDP der Port 500.

Das NCP Gateway erkennt die UDP-Encapsulation automatisch.

VPN Path Finder

Der VPN Path Finder setzt als Gegenstelle ein NCP Gateway (>= V. 8) voraus. Dort muss in den VPN / IPsec-Einstellungen des lokalen Systems ein “alternativer” Port konfiguriert sein.

Der VPN Path Finder schaltet automatisch auf das alternative Verbindungsprotokoll TCP Encapsulation mit SSL Header (Port 443) um, sobald Standard IPsec über Port 500 bzw. UDP Encapsulation über einen frei konfigurierbaren Port nicht möglich ist.

Dies ist dann von Bedeutung, wenn für den Client nur der HTTPS Port 443 zur Verfügung steht und eine reine IPsec-Verbindung nicht möglich ist, wie dies z. B. in Hotels oder an Hotspots der Fall sein kann.

Wenn für die Verbindung ein Proxy Server vorgeschaltet sein muss, kann dieser im Konfigurationsmenü unter “Proxy für VPN Path Finder” eingestellt oder konfiguriert werden.

IPsec-Adresszuweisung

Unter Einsatz von native IPsec können die IP-Adressen des Clients auf unterschiedliche Weisen, die hier konfiguriert werden können, zugewiesen werden.

Zuweisung der privaten IP-Adresse

In diesem Parameterfeld kann angegeben werden, wie die IP-Adresse zugewiesen werden soll.

IKE Config Mode verwenden
IP-Adressen und DNS Server werden über das Protokoll IKE-Config Mode (Draft 2) zugewiesen.

Diese Standard-Einstellung wird für den Enterprise Client automatisch gesetzt, wenn das Tunnel-Protokoll IPsec gewählt wird, wie unter **Tunnel-Parameter** beschrieben.

Für die NAS-Einwahl können alle bisherigen WAN-Schnittstellen verwendet werden.

Bei IPsec-Tunneling wird im Hintergrund automatisch **DPD** (Dead Peer Detection) und **NAT-T** (NAT Traversal) ausgeführt, falls dies von der Gegenstelle unterstützt wird. Mit **DPD** prüft der Client in bestimmten Abständen, ob die Gegenstelle noch aktiv ist. Bei inaktiver Gegenstelle erfolgt ein automatischer Verbindungsabbau (siehe oben).

Der Einsatz von **NAT Traversal** erfolgt automatisch beim Client und ist immer nötig, wenn seitens des Zielsystems ein Gerät mit Network Address Translation zum Einsatz kommt.

Lokale IP-Adresse verwenden
In diesem Fall wird die aktuell in den Netzwerkeinstellungen des PCs konfigurierte IP-Adresse (auch DHCP) für den IPsec Client genutzt.

IP-Adresse manuell vergeben
Dies ist die IP-Adresse und die Subnet-Maske, die hier frei eingegeben werden können. In diesem Fall wird die hier eingetragene Adresse genutzt, unabhängig von der Konfiguration in den Netzwerkeinstellungen.

DHCP über IPsec
Alternativ zur Verwendung des IKE Config Modes kann auch ein DHCP Server des Gateways genutzt werden. Dabei wird über den VPN-Tunnel dem Client in einer DHCP-Verhandlung die IP-Adresse zugewiesen.

Split Tunneling

Hier können genau die IP-Netze definiert werden, über die der Client via VPN-Tunnel komunizieren kann. Wenn Tunneling genutzt wird und hier keine Einträge erfolgen, so wird die Verbindung immer zum Tunnel-Endpunkt des Gateways aufgebaut. Soll alternierend einerseits ein Tunneling zur Zentrale erfolgen, andererseits über das Internet kommuniziert werden, so müssen hier die IP-Netze eingetragen werden, die vom Client erreicht werden sollen. Sie können dann zwischen dem Internet und dem Gateway der Firmenzentrale hin und her springen. Dies wird auch als "Split Tunneling" bezeichnet.

Klicken Sie auf den Button "Neu", so können Sie in das daraufhin erscheinende Fenster IP-Adresse und Netzmaske einzelner Netze eintragen.

Remote Networks

Hier tragen Sie die Adresse des IP-Netzes ein, das vom Client über das VPN-Gateway erreicht werden soll. Sie erhalten die Adresse(n) von Ihrem Systemadministrator.

Machen Sie in dieser Liste keinen Eintrag, so werden alle IP-Pakete über den VPN-Tunnel gesendet.

Bitte achten Sie ferner darauf, daß die IP-Adresse des VPN-Gateways nicht im Bereich der Netz-Adresse liegt.

Remote Net Masks

Hier tragen Sie die zugehörige Netzmaske des IP-Netzes ein. Sie erhalten die Adresse(n) von Ihrem Systemadministrator.

Bitte achten Sie darauf, daß die IP-Adresse des VPN-Gateways nicht im Bereich der Netz-Adresse liegt.

Auch lokale Netze im Tunnel weiterleiten

Wenn der Datenverkehr des lokalen Netzes über VPN-Tunneling weitergeleitet werden soll, so muss diese Funktion aktiviert werden.

HA-Unterstützung

Dieses Parameterfeld ist nur von Bedeutung, wenn das Zielsystem ein HA-Server (High Availability) ist, der das Tunnelaufkommen je nach Konfiguration an VPN-Gateways weiterleitet. Außerdem erscheint dieses Konfigurationsfeld nur in den Profil-Einstellungen wenn ein VPN-Protokoll für die Verbindung zur Gegenstelle selektiert wurde.

DVE-Funktionalität

Ein DVE (Dynamic VPN Endpoint) kann zum Lastausgleich (Loadbalancing) oder zur Ausfallsicherung (Backup) eines Virtual Private Networks mit zwei VPN-Gateways genutzt werden. Mit DVE wird je nach Konfiguration im HA-Manager der Gegenstelle sichergestellt, dass kein Engpass beim Tunnelaufbau auftritt. Je nach Lastaufkommen wird vom HA-Server zum Tunnelaufbau zwischen den Tunnel-Endpunkten der VPN-Gateways gewechselt. (Beachten Sie dazu die Beschreibung **HA-Funktionsbeschreibung**).

Aktivierung

Mit diesem Parameter wird die DVE-Funktionalität eingechaltet (Dynamic Virtual Endpoint). Im Konfigurationsfeld Tunnel-Parameter wird daraufhin der Tunnel-Endpunkt (Ziel) ausgeblendet. Stattdessen muss die IP-Adresse des HA-Servers (Erster / Zweiter HA-Server) angegeben werden. Dieser HA-Server führt den Tunnel dann je nach Konfiguration weiter an eines der VPN-Gateways.

Erster / Zweiter HA-Server

Hier tragen Sie die IP-Adresse der HA-Server ein. Die Adresse erhalten Sie von Ihrem System-Administrator.

DVE Secret

Hier tragen Sie das Passwort für die Verbindung des DVE-Clients zum Zielsystem (DVE-Server) ein. Sie erhalten es von Ihrem System-Administrator.

Zuletzt zugewiesenes Gateway benutzen

Ist im Gateway die Option “IP-Adressen aus Pool” gewählt und wird ein HA-Server mit Load Balancing verwendet, sollte der Client immer zu dem Gateway verbunden werden, aus dessen IP-Pool er seine IP-Adresse erhalten hat. Um dies zu gewährleisten, aktivieren Sie diese Funktion.

DNS / WINS

In diesem Konfigurationsfenster kann der durch die PPP-Verhandlung automatisch zugewiesene Server durch alternative Server ersetzt werden. Dazu muss in den Netzwerk-Einstellungen des Betriebssystems der DNS-Modus eingestellt sein.

Je nach Anwendung können Sie ein oder zwei DNS- oder WINS-Server eintragen. Genutzt wird immer der jeweils erste. Wird am Client kein WINS / DNS-Server eingetragen, wird der über die PPP-Verhandlung zugewiesene Server genutzt.

DNS-Server

Erster / Zweiter DNS-Server
Der zuerst eingetragene DNS-Server wird anstatt des über PPP-Verhandlung ermittelten Servers genutzt. Der zweite DNS-Server dient als Backup-DNS-Server.

WINS-Server

Erster / Zweiter WINS-Server
Der zuerst eingetragene WINS-Server wird anstatt des über PPP-Verhandlung ermittelten Servers genutzt. Der zweite WINS-Server dient als Backup-WINS-Server.

Domain Name

Dies ist der Domain Name der sonst per DHCP dem System in den Netzwerkeinstellungen übergeben wird.

Der Enterprise Client kann zentral gemanagt werden und kann vom Management-System automatisch Updates erhalten. Normalerweise wird der Kontakt zum Management-System über ein VPN Gateway von NCP hergestellt. Diese IP-Adresse ist nur nötig wenn die Gegenstelle kein NCP Gateway ist.

Management Server

Die IP-Adresse des NCP Secure Enterprise Managers SEM (genau: Enterprise Management Servers) muss hier eingetragen werden, wenn das Gateway der Gegenstelle kein NCP-Gateway ist und somit kein NCP Management Server automatisch über die PPP-Verhandlung bekannt gegeben werden kann.

Wird die IP-Adresse eines Management Servers eingetragen, obwohl die Gegenstelle ein NCP-Gateway ist, so wird unabhängig von der eingetragenen IP-Adresse der Management-Server des NCP Secure Enterprise Managements genutzt, welcher bei der PPP-Verhandlung zwischen NCP-Gateway und NCP Secure Client bekannt gegeben wird. Die eingetragene IP-Adresse wird in diesem Fall ignoriert.

Zertifikats-Überprüfung

In diesem Konfigurationsfeld kann pro Link-Profil am Secure Client vorgegeben werden, welche Einträge in einem Zertifikat der Gegenstelle (Secure Server) vorhanden sein müssen.

Beachten Sie dazu auch die Beschreibung **Zertifikate**.

Benutzer des eingehenden Zertifikats

Als Einträge des Benutzer-Zertifikats der Gegenstelle (Server) können alle Attribute des Benutzers, soweit bekannt – auch unterVerwendung von Wildcards – eingegeben werden. Vergleichen Sie dazu, welche Einträge im Monitor-Verbindungsmenü unter “eingehendes Zertifikat anzeigen” für den Benutzer aufgeführt sind.

Verwenden Sie die Kürzel der Attributtypen. Die Kürzel der Attributtypen für Zertifikatseinträge haben folgende Bedeutung:

```
cn     = Common Name / Name
s      = Surname / Nachname
g      = Givenname / Vorname
t      = Title / Titel
o      = Organisation / Firma
ou     = Organization Unit / Abteilung
c      = Country / Land
st     = State / Bundesland, Provinz
l      = Location / Stadt, Ort
email  = E-mail
```

Beispiel:
`cn=VPNGW*, o=NCP, c=de`
Der Common Name des Security Servers wird hier nur bis zur Wildcard “” überprüft. Alle nachfolgenden Stellen können beliebig sein, etwa 1 - 5 als Nummerierung. Die Organzation Unit muss in diesem Fall immer NCP sein und das Land Deutschland.*

Aussteller des eingehenden Zertifikats

Als Einträge des Benutzer-Zertifikats der Gegenstelle (Server) können alle Attribute des Ausstellers, soweit bekannt – auch unterVerwendung von Wildcards – eingegeben werden. Vergleichen Sie dazu, welche Einträge im Monitor-Verbindungsmenü unter “eingehendes Zertifikat anzeigen” beim Aussteller aufgeführt sind. Die Kürzel der Attributtypen für Zertifikatseinträge haben die gleiche Bedeutung wie oben unter “Benutzer des eingehenden Zertifikats”.

Beispiel:
`cn=NCP engineering GmbH`
Hier wird nur der Common Name des Ausstellers überprüft.

Fingerprint des Aussteller-Zertifikats

Um zu verhindern, dass ein Unberechtigter, der die vertrauenswürdige CA imitiert, ein gefälschtes Aussteller-Zertifikat verwenden kann, kann zusätzlich der Fingerprint des Ausstellers, soweit bekannt, eingegeben werden.

Benutze SHA1 Fingerprint statt MD5

Der Algorithmus zur Erzeugung des Fingerprints kann whlweise MD5 (Message Digit 5) oder SHA1 (Secure Hash Algorithm 1) sein.

Link Firewall

Die Link Firewall kann für alle Netzwerkadapter wie auch für RAS-Verbindungen genutzt werden. Die aktivierte Firewall wird in der grafischen Oberfläche des Clients oder in der Taskleiste als Symbol (Mauer mit Pfeil) dargestellt.

(Siehe dazu **Secure-Client-Monitor***.)*

Grundsätzliche Aufgabe einer Firewall ist es, zu verhindern, dass sich Gefahren aus anderen bzw. externen Netzen (Internet) in das eigene Netzwerk ausbreiten. Deshalb wird eine Firewall auch am Übergang zwischen Firmennetz und Internet installiert. Sie prüft alle ein- und ausgehenden Datenpakete und entscheidet auf der Basis vorher festgelegter Konfigurationen, ob ein Datenpaket durchgelassen wird oder nicht.

Die hier zu aktivierende Firewall arbeitet nach dem Prinzip der Stateful Inspection. Stateful Inspection ist die Firewall-Technologie mit dem derzeit höchstmöglichen Sicherheitsstandard für Internet-Verbindungen und somit das Firmennetz. Sicherheit wird in zweierlei Hinsicht gewährleistet. Zum einen wird der unbefugte Zugriff auf Daten und Ressourcen im zentralen Datennetz verhindert. Zum anderen überwacht sie als Kontrollinstanz den jeweiligen Status aller bestehenden Internet-Verbindungen. Die Stateful Inspection Firewall erkennt darüber hinaus, ob eine Verbindung "Tochterverbindungen" geöffnet hat, wie beispielsweise bei FTP oder Netmeeting, deren Pakete ebenfalls weitergeleitet werden müssen. Für die Kommunikationspartner stellt sich eine Stateful Inspection-Verbindung als eine direkte Leitung dar, die nur für einen den vereinbarten Regeln entsprechenden Datenaustausch genutzt werden darf.

(Siehe dazu **Secure-Client-Personal-Firewall***.)*

Stateful Inspection

aus
Die Sicherheitsmechanismen der Firewall werden nicht in Anspruch genommen.

immer
Die Sicherheitsmechanismen der Firewall werden immer in Anspruch genommen, d. h. auch wenn keine Verbindung aufgebaut ist, ist der PC vor unberechtigten Zugriffen geschützt.

bei bestehender Verbindung
Der PC ist dann nicht angreifbar, wenn eine Verbindung besteht.

Ausschließlich Kommunikation im Tunnel zulassen

Bei aktivierter Firewall kann diese Funktion zusätzlich eingeschaltet werden, um in ein- und ausgehender Richtung ausschließlich VPN-Verbindungen zuzulassen.

In Kombination mit dem Microsoft DFÜ-Dialer nur Tunnel-Kommunikation

Ist der Client-Monitor aktiv, wird verhindert, dass eine Kommunikation über den DFÜ-Dialer zum Internet stattfinden kann.

Bitte beachten Sie, dass bei Einsatz der Link Firewall der komplette IP-Datenverkehr entsprechend gesperrt wird – auch wenn der Client-Monitor *nicht* gestartet ist. Dies kann zur Folge haben, dass z. B. ein Drucker, der im lokalen Netz über IP adressiert wird, nicht reagiert.

IPsec-Konfiguration des Secure Clients

Die wichtigsten Einstellungen für eine IPsec-Verbindung werden in den Konfigurationsfeldern der Profil-Einstellungen vorgenommen und wurden oben bereits beschrieben. Dabei handelt es sich um folgende Parameter, die mit Mausklick im entsprechenden Konfigurationsfeld angesprungen werden können (hinter dem Parameter ist in Klammern das jeweilige Konfigurationsfeld angegeben):

IPsec-Tunneling (Tunnel-Parameter)

Austausch-Modus (Security)

IKE ID-Typ und IKE ID (Security)

IKE-Richtlinie und IPsec-Richtlinie (Security)*

Gateway (Tunnel-Endpunkt) (Tunnel-Parameter)

Zieladresse IPsec Gateway (Erweiterte IPsec-Optionen)

Zuweisung der privaten IP-Adresse (IPsec-Adresszuweisung)

Zugangsdaten für XAUTH (Tunnel-Parameter)

Deaktiviere DPD (Erweiterte IPsec-Optionen)

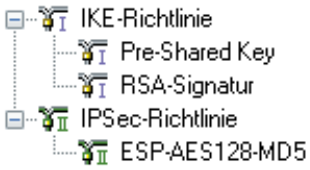
IPsec-Kompression (IPsec-Konfiguration)*

PFS / DH-Gruppe (IPsec-Konfiguration)*

** Nur die mit Stern* gekennzeichneten Parameter können in der IPsec-Konfiguration detaillierter justiert werden.*

Die IPsec-Konfiguration wird in der Regel nur dann benötigt wenn eine Anpassung der IKE- oder IPsec-Richtlinie vorgenommen werden muss, weil aus der Vorschlagsliste des Clients keine Richtlinie zu der IPsec-Konfiguration am Gateway passt. Sofern die Standardeinstellung zu den Richtlinien “von Gegenstelle bestimmt” genutzt wird, schlägt der Client eine Liste von Richtlinien vor, woraus lediglich ein Vorschlag zur Richtlinien-Konfiguration am Gateway der Gegenstelle passen muss, um eine korrekte IPsec-Verbindung zum Gateway herstellen zu können. Diese Vorschlagslisten wie auch Erläuterung dazu und zu den meisten oben genannten Parametern finden Sie im Dokument **IPsec-Funktionalität und Konfiguration**.

Die IPsec-Konfiguration erfolgt über den Menüpunkt “IPsec” im Monitor-Konfigurationsmenü.



In dem sich öffnenden Konfigurationsfenster (Abb. linnks) finden Sie zwei Konfigurationsknoten: einen zur IKE-Richtlinie und einen zur IPsec-Richtlinie. Unter der IKE-Richtlinie liegen die Richtlinien “Pre-shared Key” und “RSA-Signatur” die Sie statt der **Standardeinstellung** “**automatischer Modus**” auswählen können. (Beachten Sie dazu auch die Hinweise zu den **Vorschlagslisten für IKE-Richtlinien**). Unter der IPsec-Richtlinie finden sie die Richtlinie “ESP-3DES-MD5”. Auch diese können Sie statt der Standardeinstellung “automatischer Modus” selektieren. (Beachten Sie dazu auch die Hinweise zu der **Vorschlagsliste für IPsec-Richtlinie**).

Um die Standardeinstellung durch eine der vorgeschlagenen Richtlinien zu ersetzen, benötigen Sie noch keine IPsec-Konfiguration! Sie kann im jeweiligen Konfigurationsfeld vorgenommen weden! (Siehe vorige Seite.)

Nach Maßgabe der **IKE-Richtlinie** wird die Authentisierungsverhandlung zwischen Client (IPsec-Initiator) und Gegenstelle durchgeführt und ein verschlüsselter Kontrollkanal zwischen ihnen hergestellt.

Nach Maßgabe der **IPsec-Richtlinie** wird festgelegt, wie die Nutz-Daten gemäß des IPsec-Protokolls bearbeitet werden sollen.

Editieren der Richtlinien

Um die (Standard-)Werte innerhalb der Richtlinien zu editieren, d. h. Parameter so einzustellen oder abzuändern, wie es den Verbindungsanforderungen zur Gegenstelle entspricht, wählen Sie mit der Maus die Richtlinie, deren Werte Sie ändern möchten – die Buttons zur Bedienung werden dann aktiv.

Konfigurieren

Um eine Richtlinie abzuändern, wählen Sie mit der Maus den Namen der Richtlinie deren Werte Sie ändern möchten und klicken auf “Konfigurieren”. Dann öffnet sich das entsprechende Konfigurationsfeld.

Neuer Eintrag

Wenn Sie eine neue Richtlinie anlegen möchten, selektieren Sie eine der Richtlinien und klicken auf “Neuer Eintrag”. Die neue Richtlinie wird erzeugt. Alle Parameter sind auf Standardwerte gesetzt, bis auf den Namen.

Kopieren

Um die Parameter-Einstellungen eines bereits definierten Richtlinie zu kopieren, markieren sie die zu kopierende Richtlinie und klicken auf “Kopieren”. Daraufhin wird das Parameterfeld geöffnet. Ändern Sie nun den Namen und klicken Sie anschließend Ok. Die neue Richtlinie ist nun angelegt. Die Parameterwerte sind zu denen der kopierten identisch, bis auf den Namen.

Löschen

Wenn Sie eine Richtlinie aus dem Konfigurationsbaum löschen wollen, selektieren Sie sie und klikken auf “Löschen”. Die Richtlinie damit auf Dauer aus der IPsec-Konfiguration gelöscht.

Schließen

Wenn Sie das IPsec-Feld schließen, kehren Sie zum Monitor zurück. Die Daten werden so wie sie konfiguriert wurden behalten.

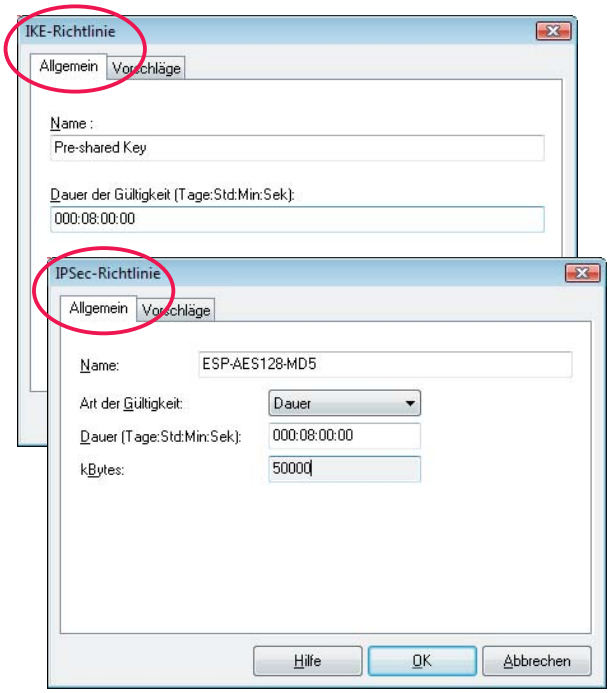
Speichern

Jede Änderung in der IPsec-Konfiguration wird mit “OK” gespeichert.

Richtlinien-Gültigkeit / Allgemein

Wenn Sie die Einstellungen zu einer Richtlinie am Client öffnen, werden zunächst allgemeine Parameter eingeblendet, die für alle Vorschläge dieser Richtlinie Gültigkeit haben. Dazu gehört der Richtlinien-Name – in der Standardeinstellung “Pre-shared Key” oder “RSA-Signatur” – worunter die Vorschläge (Proposals) gesammelt werden, aber auch Einstellungen für die Gültigkeit dieser Richtlinie.

Allgemein



Die Richtlinien-Gültigkeit wird im Konfigurationsfenster Allgemein spezifisch pro einzelner Richtlinie, unterschieden auch nach IKE- und IPsec-Richtlinie, festgelegt. (Abb. oben)

Art der Gültigkeit

Bestimmt nach welchen Kriterien die Art der Schlüsselgültigkeit festgelegt wird, nach Dauer, nach übertragenen kBytes oder nach **beiden**. Mit jeder neuen SA-Verhandlung wird der Zähler zurück gesetzt. (Siehe dazu SA-Verhandlung und Richtlinien in der PDF-Datei IPsec-Funktionalität und Richtlinien.)

Dauer

Die Größe der Zeitspanne kann eigens eingestellt werden.

kBytes

Die Menge der kBytes kann eigens eingestellt werden.

Name

Geben Sie dieser Richtlinie einen Namen. Über diesen Namen kann sie beim Enterprise Client im Konfigurationsfeld Security ausgewählt werden.

IKE-Richtlinie / Vorschläge

Die Parameter in diesem Feld beziehen sich auf die Phase 1 des Internet Key Exchange (IKE) mit dem der Kontrollkanal für die SA-Verhandlung aufgebaut wird.

Die IKE-Richtlinien, die Sie hier konfigurieren, werden zur Auswahl gelistet.

Funktional unterscheiden sich zwei IKE-Richtlinien, die standardmäßig mit der Software ausgeliefert werden: "Pre-shared Key" und "RSA-Signatur". Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu Authentisierung und Verschlüsselungsalgorithmus auf (IKE-Richtlinie, Authentisierung, Verschlüsselung), d. h. eine Richtlinie kann aus verschiedenen Vorschlägen bestehen.

Für alle Benutzer sollten die gleichen Richtlinien einschließlich zugehöriger Vorschläge (Proposals) gelten. D. h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

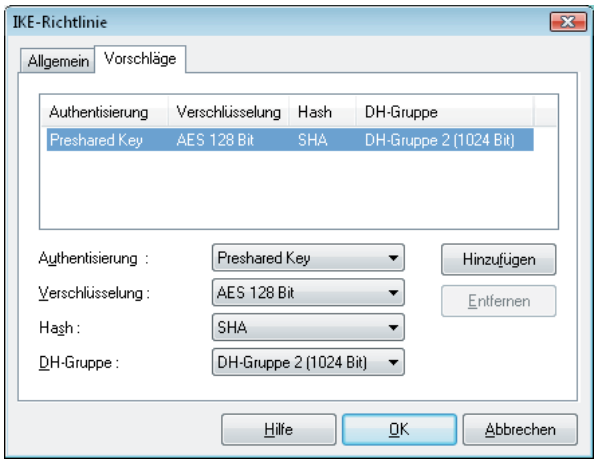


Abb. oben: Parameterfeld für die Vorschläge zur IKE-Richtlinie am Enterprise Client.

Authentisierung | IKE-Richtlinie

Bevor der Kontrollkanal für die Phase 1-Verhandlung (IKE Security Association) aufgebaut werden kann, muss beidseitig eine Authentisierung stattgefunden haben.

Pre-shared Key
Zur gegenseitigen Authentisierung wird der gemeinsame Pre-shared Key verwendet.
Der Pre-shared Key wird unter **Security** festgelegt.

RSA Signatur
Zur gegenseitigen Authentisierung wird das Zertifikat verwendet, das Sie für die Erweiterte Authentisierung (XAUTH) konfiguriert haben. Im Main Mode wird das Zertifikat zusätzlich verschlüsselt. Dies ist nur mit PKI-Unterstützung des Systems möglich.

Verschlüsselung | IKE-Richtlinie

Nach einem der optionalen Verschlüsselungsalgorithmen erfolgt die symmetrische Verschlüsselung der Messages 5 und 6 im Kontrollkanal, sofern der Main Mode (Identity Protection Mode) gefahren wird.

Zur Wahl stehen: DES, Triple DES, Blowfish, AES 128, AES 192, AES 256.

Der Austausch-Modus wirc im Konfigurationsfeld **Security** eingestellt.

Hash | IKE-Richtlinie

Modus, wie der Hash-Wert über die ID bzw. das Zertifikat der Messages im Kontrollkanal gebildet wird.

Zur Wahl stehen: MD5 (Message Digest, Version 5), SHA (Secure Hash Alogrithm), SHA 256, SHA 384 und SHA 512 Bit

DH-Gruppe | IKE-Richtlinie

Mit der Wahl einer der angebotenen Diffie-Hellman-Gruppen wird festgelegt, wie sicher der Internet Key Exchange im Kontrollkanal (Phase 1) erfolgen soll, nach dem der spätere symmetrische Schlüssel erzeugt wird. Je höher die DH Group desto sicherer ist der Key Exchange.

IPsec-Richtlinie / Vorschläge

Die Parameter in diesem Feld beziehen sich auf die Phase 2 der SA-Verhandlung.

Die IPsec-Richtlinien die Sie hier konfigurieren, werden zur Auswahl für die intern erzeugte SPD gelistet.

Nur eine IPsec-Richtlinie mit ESP (Encapsulating Security Payload) wird standardmäßig mit der Software ausgeliefert. Da der IPsec-Modus mit AH-Sicherung für flexiblen Remote Access ungeeignet ist, wird nur eine IPsec-Richtlinie mit ESP-Protokoll ausgeliefert. Jede IPsec-Richtlinie listet mindestens einen Vorschlag (Proposal) zu IPsec-Protokoll und Authentisierung auf, d. h. eine Richtlinie kann aus verschiedenen Vorschlägen bestehen.

Für alle Benutzer sollten die gleichen Richtlinien einschließlich zugehöriger Vorschläge (Proposals) gelten. D. h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Protokoll | IPsec-Richtlinie

Der fest eingestellte Standardwert ist ESP.

IPsec-Kompresssion
Die Datenübertragung mit IPsec kann ebenso komprimiert werden wie ein Transfer ohne IPsec. Dies ermöglicht eine Steigerung des Durchsatzes um maximal das 3-fache. Nach Selektion von “IPsec-Kompression” kann als Transformation zwischen LZS- und Deflate-Kompression gewählt werden.

Die IPsec-Kompression wird für die Vorschläge der IPsec-Richtlinie des Clients erst aktiv wenn die Vorschlagsliste mit dem Vorschlag zur Kompression abgeschlossen wird.

Verschlüsselung

Für das Sicherheitsprotokoll ESP kann hier definiert werden wie mit ESP verschlüsselt werden soll.

Zur Wahl stehen die gleichen Verschlüsselungsalgorithmen wie für Layer 2: DES, Triple DES, Blowfish, AES 128, AES 192, AES 256, none (NULL).

Nach Selektion von “IPsec-Kompression” kann als Transformation zwischen LZS- und Deflate-Kompression gewählt werden.

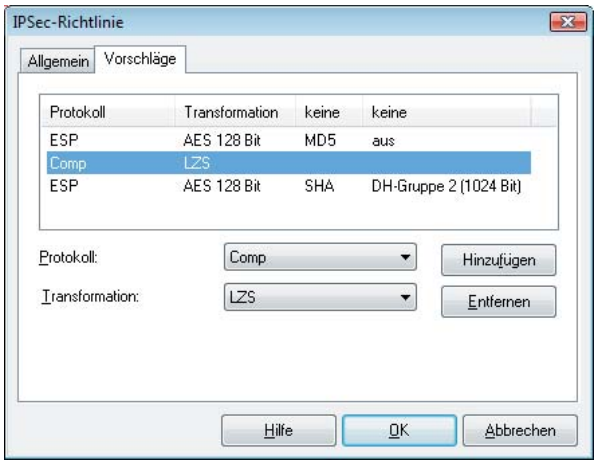


Abb. oben: IPsec-Richtlinie am Enterprise Client mit mit IPsec-Kompression. Die Kompression gilt in diesem Beispiel für den Vorschlag ESP- AES 128 Bit - MD5. Der nachfolgende Vorschlag der Richtlinie wird unkomprimiert gesendet.

Authentisierung | IPsec-Richtlinie

Für das Sicherheitsprotokoll ESP kann der Modus der Authentisierung eigens eingestellt werden. Zur Wahl stehen: MD5, SHA, SHA 256, SHA 384 und SHA 512 Bit.

PFS / DH-Gruppe

Mit der Wahl einer der angebotenen Diffie-Hellman-Gruppen wird festgelegt, dass zusätzlich in Phase 2 mit der SA-Verhandlung ein kompletter Schlüsselaustausch (PFS) stattfinden soll.

Standard-Einstellung ist “keine”. Möglich sind folgende DH-Gruppen:

DH-Gruppe 1 (768 Bit)
DH-Gruppe 2 (1024 Bit)
DH-Gruppe 5 (1536 Bit)

Index