funkwerk
enterprise communications

Secure Client Parameter

des FEC Secure IPSec Clients

Copyright

Alle Rechte sind vorbehalten. Kein Teil dieses Handbuches darf ohne schriftliche Genehmigung der Firma Funkwerk Enterprise Communications GmbH in irgendeiner Form reproduziert oder weiterverwendet werden. Auch eine Bearbeitung, insbesondere eine Übersetzung der Dokumentation, ist ohne Genehmigung der Firma Funkwerk Enterprise Communications GmbH nicht gestattet.

Marken

Funkwerk Enterprise Communications, FEC und das FEC Logo sind eingetragene Warenzeichen. Erwähnte Firmen- und Produktnamen sind in der Regel eingetragene Warenzeichen der entsprechenden Hersteller.

Haftung

Alle Programme und das Handbuch wurden mit größter Sorgfalt erstellt und nach dem Stand der Technik auf Korrektheit überprüft. Alle Haftungsansprüche infolge direkter oder indirekter Fehler, oder Zerstörungen, die im Zusammenhang mit dem Programm stehen, sind ausdrücklich ausgeschlossen. Funkwerk Enterprise Communications GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslastungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie Änderungen zu diesem Produkt finden Sie unter www.funkwerk-ec.com.

Wie Sie Funkwerk Enterprise Communications erreichen:

Funkwerk Enterprise Communications GmbH

Südwestpark 94
D-90449 Nürnberg
Germany
Telephone: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.funkwerk-ec.com

Die Parameter des Secure Clients

In diesem Handbuch sind alle Konfigurationsparameter der Profil-Einstellungen und IPSec-Konfiguration des Secure IPSec Clients beschrieben.

Die Reihenfolge der Parameterbeschreibungen wurde an der Reihenfolge der Konfigurationsfelder in den Profil-Einstellungen ausgerichtet und ist in der Inhaltsübersicht unten dargestellt.

Von dort aus können die Konfigurationsfelder per Mausklick direkt angewählt werden, ohne das Dokument durchblättern zu müssen.*

Inhaltsübersicht

Am komfortabelsten erhalten Sie die gewünschten Informationen über **Client-Navigator**. In dieser PDF-Datei sind alle aktuell verfügbaren Dokumente zu Ihrem Produkt verzeichnet.

Vom Navigator aus können Sie alle relevanten Dokumente direkt anspringen und – falls sie noch nicht in Ihrem Navigatorverzeichnis gespeichert sind – von der Funkwerk-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, HTTP-Anmeldung oder X.31). Zum anderen können einzelne Konfigurationsfelder oder Parameter, die Sie für Ihre Arbeit mit dem Client nicht benötigen, vom Systemadministrator durch eine* **Konfigurationssperre** *ausgeblendet worden sein.*

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.

Verbindungstyp

Alternativ stehen zwei Verbindungstypen zur Wahl:

VPN zu IPSec-Gegenstelle

In diesem Fall verbinden Sie sich über den IPSec Client mit dem Firmennetz (bzw. mit dem Gateway). Dazu wird ein VPN-Tunnel aufgebaut.

Internet-Verbindung ohne VPN

In diesem Fall nutzen Sie den IPSec Client nur zur Einwahl in das Internet. Dabei wird Network Address Translation (IPNAT) weiterhin im Hintergrund genutzt, sodass nur Datenpakete akzeptiert werden, die angefordert wurden.

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. Beachten Sie dazu die PDF-Dateien **Mobile Computing** und **Secure Client Monitor**.

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;

Unter Windows 2000/XP und Vista kann der WLAN-Adapter 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.

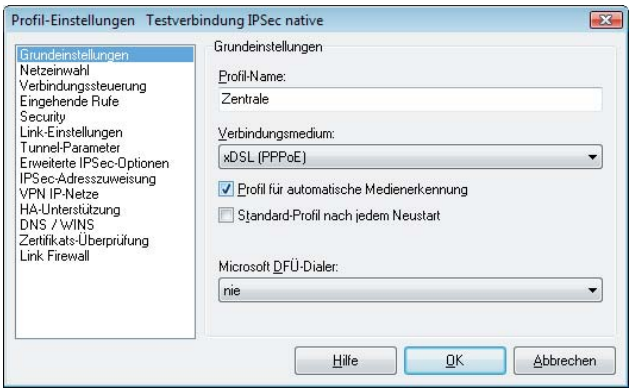
Je nach installiertem Dialer (iPass oder T-Online) muss in der Konfigurationsdatei EXTDIAL.INI für den Eintrag “ExeName” die EXE-Datei des Dialers eingetragen werden. Um nicht den kompletten Pfad für den Dialer in der DAT-Datei angeben zu müssen, kann optional der Pfad aus der Registry gelesen und in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

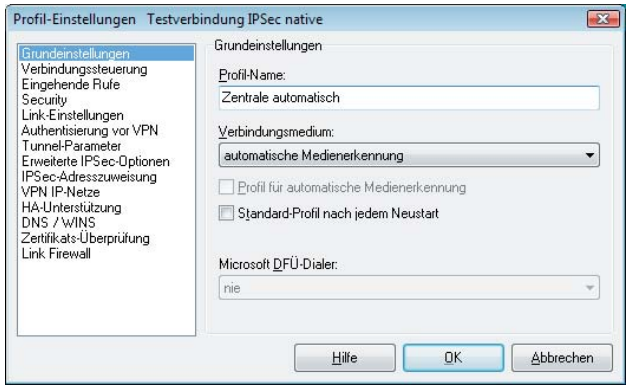
Automatische Medienerkennung

Werden wechselweise unterschiedliche Verbindungsmedien genutzt, wie zum Beispiel Modem und ISDN, so kann die manuelle Auswahl des Profils mit dem jeweils zur Verfügung stehenden Medium entfallen, wenn ein Profil für automatische



Medienerkennung konfiguriert wurde und je ein Profil mit den alternativ verfügbaren Verbindungsmedien wie zum Beispiel Modem und ISDN.

Dabei ist zu beachten, dass das Profil mit automatischer Medienerkennung mit allen für die Verbindung zum VPN Gateway nötigen Parametern konfiguriert ist (Abb. oben), wohingegen die Profile mit den alternativen Verbindungsmedien so konfiguriert sein müssen, dass das jeweils gewünschte Verbindungsmedium (evtl. auch die Modemparameter) eingestellt ist und die Funktion “Eintrag für



automatische Medienerkennung” aktiviert ist (Abb. unten). Außerdem müssen für das jeweilige Verbindungsmedium die Eingangsdaten zum ISP im Parameterfeld “Netzeinwahl” gesetzt sein.

Bei einem Verbindungsaufbau erkennt der Client automatisch, welche Verbindungsmedien aktuell zur Verfügung stehen und wählt davon das schnellste aus. In einer Suchroutine ist die Priorisierung der Verbindungsarten in folgender Reihenfolge

festgelegt: 1. LAN, 2. WLAN, 3. DSL, 4. UMTS/GPRS, 5. ISDN, 6. MODEM.

Die Zugangsdaten für die Verbindung zum ISP (siehe unten Netzeinwahl) werden aus den Profil-Einstellungen übernommen, die für die automatische Medienerkennung konfiguriert wurden.

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 potentiellen Verbindungsaufbau herangezogen. Beachten Sie dazu die Beschreibung zum Verbindungsmedium.

Dieses Profil kann auch manuell selektiert werden, um eine Verbindung herzustellen, sofern die Tunnel-Parameter für den Zugang zum VPN Gateway korrekt eingetragen sind.

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.

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).

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.

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

Die folgenden Parameter sind nur für eine Verbindung über GPRS / UMTS von Bedeutung. Beachten Sie bitte auch die Beschreibung: Mobile-Computing

APN

Der APN (Access Point Name) wird für die GPRS- und UMTS-Einwahl benötigt. Sie erhalten ihn von Ihrem Provider. Der APN wird insbesondere zu administrativen Zwecken genutzt.

SIM PIN AT-Befehl

Bei Verwendung einer GPRS/UMTS-Karte muss der jeweils spezifische AT-Befehl eingegeben werden. Dieses Kommando bewirkt, dass die SIM PIN richtig erkannt wird.

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.

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.

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.

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.

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.

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.

Authentisierung vor Tunnelaufbau

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**.

IPSec-Einstellungen

In diesem Konfigurationsfeld geben Sie die Adresse des Gateways an. Darüber hinaus legen Sie in Abstimmung mit den Vorgaben der Gegenstelle die Richtlinien fest, die für die IPSec-Verbindung in der Phase 1- und Phase 2-Verhandlung verwendet werden sollen. Sofern der automatische Modus genutzt wird, schlägt der Client eine Liste von Richtlinien vor, woraus ein Vorschlag zu einer Richtlinie am Gateway der Gegenstelle passen muss. Ist dies nicht der Fall müssen die Richtlinien in Abstimmung mit der Gegenstelle mit dem Richtlinien-Editor konfiguriert werden. Klicken Sie dazu auf **IPSec-Konfiguration**.

Die **erweiterten IPSec-Optionen** *können nach Abstimmung mit der Gegenstelle eingesetzt werden.*

Gateway (Tunnel-Endpunkt) | IPSec-Einst.

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.

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 | IPSec-Einstellungen

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 “Pre-shared Key verwenden” und “Shared Secret” im Konfigurationsfeld **Identität**).

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 | IPSec-Einstellungen

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 | IPSec-Einstellungen

Der Austausch-Modus (Exchange Mode) 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.

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.

PFS / DH-Gruppe

Mit Auswahl einer der angebotenen Diffie-Hellman-Gruppen wird festgelegt, ob ein kompletter Diffie-Hellman-Schlüsselaustausch (PFS, Perfect Forward Secrecy) in Phase 2 zusätzlich zur SA-Verhandlung stattfinden soll.

Der gewählte Diffie-Hellman-Schlüsselaustausch wird global für alle Richtlinien-Konfigurationen angewendet.

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

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

Gültigkeit

Die hier definierte **Richtlinien-Gültigkeit** gilt für alle IKE- bzw. alle IPSec-Richtlinien.

Die Art der Gültigkeit legt die Kriterien der Richtlinien-Gültigkeit fest, nach Dauer, nach übertragenen kBytes oder nach beidem. Die Menge der kBytes oder die Größe der Zeitspanne kann eigens eingestellt werden. Mit jeder neuen SA-Verhandlung wird der Zähler zurück gesetzt.

Editor

Sollen am IPSec Client spezielle Richtlinien verwendet oder die vorhandenen angepasst werden, so müssen sie mit dem Richtlinien-Editor konfiguriert werden. Klicken Sie dazu auf den Editor-Button.

Bitte beachten Sie, dass eine IPSec-Verbindung nur dann korrekt konfiguriert werden kann, wenn dem Benutzer des IPSec Clients die passenden Parameterwerte und -einstellungen von der zentralen Gegenstelle zur Verfügung gestellt werden!

Die zugehörigen Erklärungen erhalten Sie mit Klick auf **IPSec-Konfiguration**.

Erweiterte IPSec-Optionen

Mit diesen Parametern können Einstellungen für eine Client-Server-Verbindung mit IPSec native vorgenommen werden.

IPSec-Kompression

Die Datenübertragung mit IPSec kann ebenso komprimiert werden wie ein Transfer ohne IPSec. Dies ermöglicht eine Steigerung des Durchsatzes um maximal das 3-fache. Welche IPSec-Kompression verwendet wird, gibt die Gegenstelle vor. Der Entry Client unterstützt LZS- und Deflate-Kompression.

Deaktiviere DPD (Dead Peer Detection)

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 dieser Funktion kann DPD ausgeschaltet werden.

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).

Über eine GPRS / UMTS-Verbindung kann DPD daher ein Datenaufkommen erzeugen, das ungewollte Kosten verursacht.

UDP Encapsulation

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.

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.

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. [Dies ist die Standard-Einstellung für den Entry Client]

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.

DNS / WINS

An dieser Stelle 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.

VPN IP-Netze

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.

VPN IP-Netzwerke

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.

VPN IP-Netzmasken

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.

Identität

Entsprechend des Security-Modus IPSec können hier noch weitere Sicherheitseinstellungen vorgenommen werden.

IKE ID-Typ

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

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.

Pre-shared Key verwenden

Shared Secret
Der Pre-shared Key ist ein String beliebiger Zeichen in einer maximalen Länge von 255 Zeichen. Alle alphanumerischen Zeichen können verwendet werden. Wenn die Gegenstelle einen Pre-shared Key während der IKE-Verhandlung erwartet, dann muss dieser Schlüssel in das Feld “Shared Secret” eingetragen werden.

Bestätigung Secret
Bestätigen Sie das “Shared Secret” im darunter liegenden Feld. Der gleiche Pre-shared Key muss auf beiden Seiten verwendet werden.

Beachten Sie zur folgenden Zertifikatskonfiguration auch die Beschreibung Zertifikate.

Zertifikatskonfiguration

Hier kann ein Zertifikat für die Extended Authentication selektiert werden. Um die Beschreibung zu erhalten, klicken Sie auf **Zertifikatskonfiguration**.

Extended Authentication (XAUTH)

Extended Authentication (XAUTH Protokoll, Draft 6) ist standardmäßig *nicht* aktiv. Sie kann an dieser Stelle eingeschaltet werden wenn sie vom IPSec Gateway unterstützt wird. Zusätzlich zum Pre-shared Key können dann noch folgende Parameter zur Authentisierung genutzt werden:

Benutzername | Identität

Den Benutzernamen für XAUTH erhalten Sie von Ihrem Systemadministrator. Der Name kann 256 Zeichen lang sein.

Passwort | Identität

Das Passwort für XAUTH erhalten Sie von Ihrem Systemadministrator. Der Name kann 256 Zeichen lang sein.

Zugangsdaten aus ...

Als Zugangsdaten zum IPSec Gateway können statt Benutzername und Passwort aus obiger Konfiguration auch folgende Daten aus einem der folgenden Zertifkatsfelder ausgelesen und verwendet werden:

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

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

– Zertifikatsfeld (Seriennummer)
Dies bedeutet, dass statt “Benutzername” und “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.

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.

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-Dialers 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.

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.

IPSec-Konfiguration

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):

Austausch-Modus (IPSec-Einstellungen)

IKE ID-Typ und IKE ID (Identität)

IKE-Richtlinie und IPSec-Richtlinie (IPSec-Einstellungen)*

Gateway (Tunnel-Endpunkt) (IPSec-Einstellungen)

Zuweisung der privaten IP-Adresse (IPSec-Adresszuweisung)

Zugangsdaten für XAUTH (Identität)

Deaktiviere DPD (Dead Peer Detection) (Erweiterte IPSec-Optionen)

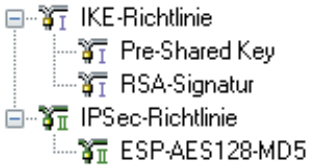
IPSec-Kompression (Erweiterte IPSec-Optionen)

PFS / DH-Gruppe (IPSec-Einstellungen)

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.

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

Die IPSec-Konfiguration wird geöffnet, indem in den Profil-Einstellungen unter “IPSec-Einstellungen” der [Editor]-Button gedrückt wird.



In dem sich öffnenden Konfigurationsfenster (Abb. links) 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. Unter der IPSec-Richtlinie finden sie die Richtlinie “ESP-3DES-MD5”. Auch diese können Sie statt der Standardeinstellung “automatischer Modus” selektieren.

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

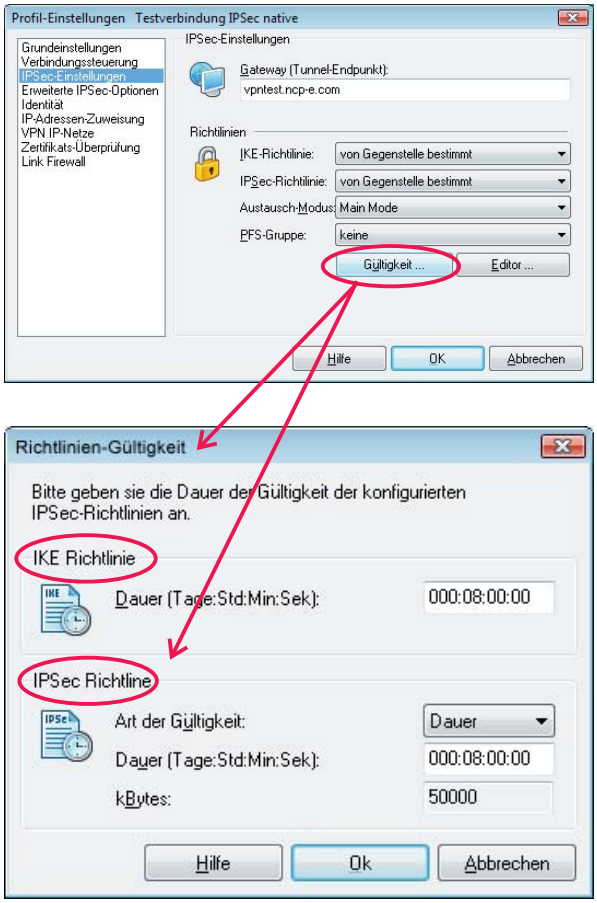
Wenn Sie das IPSec-Feld schließen, kehren Sie zum Monitor zurück. Die Daten werden so wie sie konfiguriert wurden behalten.

Speichern

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

Richtlinien-Gültigkeit

Die Gültigkeitsdauer wird global für alle Richtlinien eines Profils, sowohl IKE- als auch IPSec-Richtlinie, über den [Gültigkeit]-Button festgesetzt, der im Konfigurationsfenster **IPSec-Einstellungen** gedrückt werden kann. (Abb. unten)



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.

Dauer

Die Größe der Zeitspanne kann eigens eingestellt werden.

kBytes

Die Menge der kBytes kann eigens eingestellt werden.

IKE-Richtlinie

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 im Konfigurationsfeld **Identität** *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.

Name

Geben Sie dieser Richtlinie einen Namen. Über diesen Namen kann sie in den **IPSec-Einstellungen** ausgewählt werden.

Authentisierung | IKE-Richtlinie

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

Zur gegenseitigen Authentisierung wird der gemeinsame Pre-shared Key verwendet.

Diesen Schlüssel legen Sie im Konfigurationfeld **Identität** fest.

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) als Austausch-Modus gefahren wird. (Der Austausch-Modus wird im Konfigurationsfeld **IPSec-Einstellungen** eingestellt.)

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

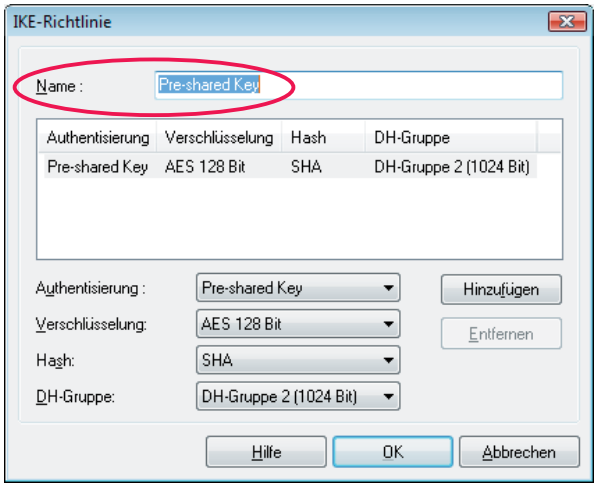


Abb. oben: IKE-Richtlinie "Pre-shared Key", deren Einstellungen und Name abgeändert werden können.

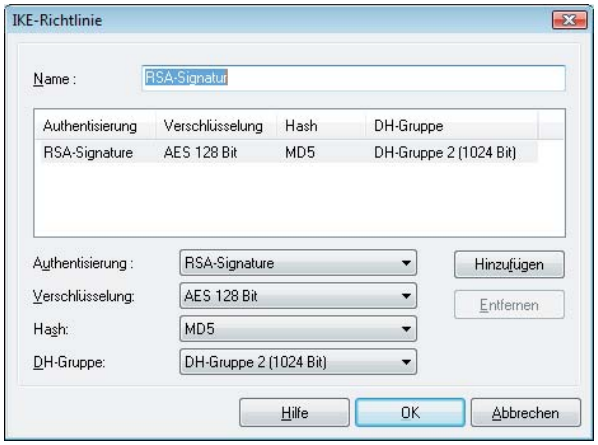


Abb. oben: IKE-Richtlinie "RSA-Signatur", deren Einstellungen und Name abgeändert werden können.

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

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.

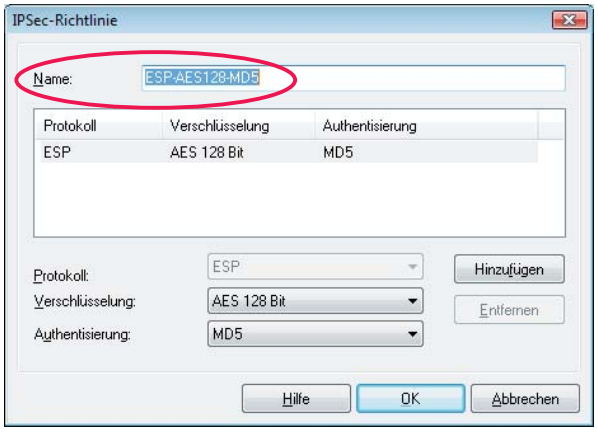


Abb. oben: Vorkonfigurierte IPSec-Richtlinie "ESP-AES128-MD5", deren Einstellungen und Name abgeändert werden können.

Name

Geben Sie dieser Richtlinie einen Namen. Über diesen Namen kann sie in den **IPSec-Einstellungen** ausgewählt werden.

Protokoll | IPSec-Richtlinie

Der fest eingestellte Standardwert ist ESP.

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).

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.