IPSec

Version 0.9

Ziel und Zweck

Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von BinTec Gateways ab Software-Release 7.1.1. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere **Release Notes** lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten **Release Notes** sind immer zu finden unter www.bintec.de.

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in Ihrem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Bintec Access Networks GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen, sowie Änderungen und **Release Notes** für Bintec-Gateways finden Sie unter www.bintec.de.

Als Multiprotokollgateways bauen Bintec-Gateways in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Bintec Access Networks GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken

Bintec und das Bintec-Logo sind eingetragene Warenzeichen der Bintec Access Networks GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright

Richtlinien und Normen

Bintec-Gateways entsprechen folgenden Richtlinien und Normen:

R&TTE-Richtlinie 1999/5/EG

CE-Zeichen für alle EU-Länder

Weitere Informationen finden Sie in den Konformitätserklärungen unter www.bintec.de.

Wie Sie Bintec erreichen

Bintec Access Networks GmbH
Südwestpark 94
D-90449 Nürnberg
Germany

Telephone: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.bintec.de

Bintec France
6/8 Avenue de la Grande Lande
F-33174 Gradignan
France

Telephone: +33 5 57 35 63 00
Fax: +33 5 56 89 14 05
Internet: www.bintec.fr

1 Hauptmenü

Im folgenden werden die Felder des Menüs *IPSEC* beschrieben.

Wenn Sie IPSec zum ersten Mal konfigurieren, wird ein ➤➤ **Setup Tool** Wizard gestartet, der Sie durch eine teilautomatisierte Konfiguration verschiedener Voreinstellungen führt. (Die Konfiguration mit dem Setup Tool Wizard wird beschrieben in "Untermenü WIZARD" auf Seite 91.)

Nach Beenden und Verlassen des IPSec Wizards, wird das IPSec Hauptmenü geöffnet. Es wird wie folgt angezeigt:

```
VPN Access Setup Tool                        Bintec Access Networks GmbH
[IPSEC]: IPsec Configuration - Main Menu                        MyGateway

  Enable IPSec     : yes

  Pre IPSec Rules >
  Configure Peers >
  Post IPSec Rules >

  IKE (Phase 1) Defaults   *autogenerated*        edit >
  IPsec (Phase 2) Defaults *autogenerated*        edit >
  Certificate and Key Management >

  Advanced Settings >
  Wizard >

  Monitoring >


          SAVE                              CANCEL
```

Hinweis

Beachten Sie, dass Sie dem IPSec Wizard zumindest bis zur ersten Eingabeaufforderung folgen müssen. Bei der ersten Eingabeaufforderung können Sie ggf. den IPSec Wizard abbrechen und die Konfiguration in den IPSec Menüs fortführen. Wir empfehlen jedoch, den ersten Peer vollständig mit dem IPSec Wizard zu erstellen.

Wenn der IPSec Wizard nicht die notwendigen ➤➤ **NAT**-Einstellungen vornehmen sowie die IKE- und IPSec-Proposals erstellen kann, werden weitere Konfigurationsschritte notwendig, die z. T. nur auf der ➤➤ **SNMP Shell** möglich, aber für eine IPSec-Konfiguration unbedingt notwendig sind.

Nur in dem Feld ***ENABLE IPSEC*** im ***IPSEC*** Hauptmenü können Sie direkt aus zwei Optionen wählen.

ENABLE IPSEC Dieses Feld enthält die folgenden Werte:

Wert	Bedeutung
no	IPSec ist nicht aktiviert unabhängig von jeglicher Konfiguration. Wenn IPSec derzeit aktiviert ist, wird es deaktiviert, sobald Sie mit **SAVE** bestätigen.
yes	IPSec ist aktiviert, sobald Sie mit **SAVE** bestätigen. Falls Sie keine gültige IPSec Lizenz haben, werden alle IP-Pakete abgewiesen, solange bis Sie IPSec wieder deaktivieren. Alle Geräte der VPN-Access-Linie verfügen per Default über eine IPSec-Lizenz.

Tabelle 1-1: Felder im Untermenü ***ENABLE IPSEC***

Darüber hinaus können Sie für die Felder ***IKE (PHASE 1) DEFAULTS*** und ***IPSEC (PHASE 2) DEFAULTS*** zwischen den jeweils im Menü ***EDIT*** konfigurierten Profilen wählen.

2 Untermenü *PRE IPSEC RULES*

Im folgenden wird das Untermenü *PRE IPSEC RULES* beschrieben.

Wenn Sie IPSec auf Ihrem Gateway konfigurieren, müssen Sie Regeln für die Handhabung des Datenverkehrs erstellen, bevor die IPSec SAs angewendet werden. Sie müssen zum Beispiel spezifischen Paketen erlauben, im Klartext zu passieren, um bestimmte Grundfunktionen zu erfüllen.

Im ersten Fenster des ***PRE IPSEC*** Menüs sind alle bereits erstellten Regeln aufgelistet:

```
VPN Access Setup Tool                        Bintec Access Networks GmbH
[Pre IPSEC TRAFFIC]: IPSec Configuration -
                           Configure Traffic List              MyGateway

Highlight an entry and type 'i' to insert new entry below,
'u'/'d' to move up/down, 'a' to select as active traffic list

Local Address  M/R Port Proto Remote Address  M/R   Port  A   Proposal
*0.0.0.0       M0  500  udp   0.0.0.0         M0    500   PA  default
own Address        80   tcp   198.16.13.1     M32   80    PA  default
own Address         -   tcp   198.16.13.1     M32   21    DR  default




     APPEND              DELETE              EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return>
to edit
```

Diese Werte können nur gelesen werden und sind abhängig von den Einstellungen, die in ***IPSEC*** ➜ ***PRE IPSEC RULES*** ➜ **APPEND/EDIT** vorgenommen wurden. Weitere Informationen zu den Einstellungen finden Sie im folgenden Kapitel (Siehe “Das Untermenü APPEND/EDIT” auf Seite 7.).

Folgende Einträge sind enthalten:

Feld	Wert
Local Address	Zeigt die lokale ➤➤ **IP-Adresse** der Regel an.

Feld	Wert
M/R	Zeigt die Länge der ➤➤ **Netzmaske** an (falls die Regel für ein Netzwerk definiert wurde) oder die Anzahl der aufeinanderfolgenden IP-Adressen, falls die Regel für einen IP-Adressbereich erstellt wurde. Somit steht *M32* für eine 32 Bit Netzmaske (255.255.255.255, d. h.einen einzelnen Host) und *R10* für eine Reihe von 10 IP-Adressen einschliesslich der spezifizierten Adresse.
Port	Zeigt die lokale, bzw. entfernte ➤➤ **Port**-Nummer an, die zum Filtern der Pakete verwendet wird; gilt nur für UDP und TCP Ports (*0* = jeder).
Proto	Zeigt das Protokoll an, das zum Filtern der Pakete anhand dieser Regel angewendet wird.
Remote Address	Zeigt die entfernte IP-Adresse dieser Regel an.
A	Zeigt die Aktion an, die durch diese Regel ausgelöst wird. Die gefilterten Pakete werden entweder abgelehnt (*DR*), oder können unverändert passieren (*PA*).
Proposal	Zeigt die angewendeten IPSec Proposals (=Vorschläge) an. Bei Pre IPSec Rules ist dieses ohne Bedeutung, da keine SAs (=Security Associations; Sicherheitsvereinbarungen) angewendet werden.

Tabelle 2-1: ***IPSEC ➜ PRE IPSEC RULES***

In diesem Menü können Sie lediglich eine Einstellung konfigurieren: Sie können definieren, welcher der Traffic-Listeneinträge die erste aktive Regel in der Regelkette sein soll. Zusätzlich können Sie die Regeln innerhalb der Liste nach oben oder unten verschieben, so dass Sie so die Pre IPSec Rules nach Ihren Bedürfnissen gestalten. Jede Regel vor der Regel, die als "active traffic list" definiert ist, wird ignoriert. Wie die Active Traffic List ausgewählt wird, wird im Hilfebereich des Menüfensters beschrieben.

2.1 Das Untermenü *APPEND/EDIT*

Pre IPSec Rules werden im Menü ***IPSec*** ➜ ***Pre IPSec Rules*** ➜ ***APPEND/EDIT*** bearbeitet oder hinzugefügt. In beiden Fällen wird das folgende Menüfenster geöffnet (wenn Sie einen bestehenden Eintrag bearbeiten, werden die bestehenden Werte dieses Eintrags angezeigt):

```
VPN Access Setup Tool                        Bintec Access Networks GmbH
[Pre IPSEC TRAFFIC][ADD]: Edit Traffic Entry                 MyGateway

Description:


     Protocol:      dont-verify

     Local:
          Type: net   Ip:                / 0

     Remote:
          Type: net   Ip:                / 0


     Action:        pass


                    SAVE                                  CANCEL
```

Das Menü besteht aus folgenden Feldern:

Feld	Wert
Description	Geben Sie eine Beschreibung ein, die die Art der Regel eindeutig erkennen läßt.
Protocol	Hier können Sie definieren, ob der für diese Regel geltende Datenverkehr nur für die Pakete mit einem bestimmten Protokoll gelten soll. Sie können wählen zwischen spezifischen Protokollen und der Option *dont-verify*, welches bedeutet, dass das Protokoll nicht als Filterkriterium angewendet wird.

Feld	Wert
Local: Type	Geben Sie die lokalen Adressdaten ein. Mögliche Werte siehe Tabelle "LOCAL/REMOTE: TYPE" auf Seite 9.
Remote: Type	Geben Sie die entfernten Adressdaten ein. die Optionen stimmen größtenteils mit den Optionen im Feld ***LOCAL: TYPE*** überein, mit einer Ausnahme: Die Option *own* gibt es nicht und wird durch die Option *peer* ersetzt. Dieses ist jedoch nur in Peer-Konfigurationen relevant.
Action	Sie können zwischen zwei Optionen wählen: ■ *pass:* Diese Option lässt IPSec-Pakete ungeändert passieren. ■ *drop:* Diese Option weist alle Pakete, die mit den eingestellten Filter übereinstimmen, ab.

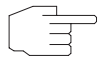
Tabelle 2-2: ***IPSEC ➜ PRE IPSEC RULES ➜ APPEND/EDIT***

LOCAL/REMOTE: TYPE Das Feld ***LOCAL/REMOTE: TYPE*** hat folgende Optionen:

Wert	Bedeutung
host	Definieren Sie die IP-Adresse einer einzelnen Maschine, auf die diese Regel angewendet werden soll. Wenn Sie bestimmte Protokolle ausgewählt haben, um den Datenverkehr einzuschränken, werden Sie evtl. aufgefordert, eine ***PORT***-Nummer einzutragen. Dieses gilt jedoch nur für UDP und TCP.

Wert	Bedeutung
net	Definieren Sie die IP-Adresse des Netzwerks und die entsprechende Netzmaske, auf die diese Regel angewendet werden soll. Die Eingabeaufforderung für die Netzmaske erscheint automatisch wenn Sie *net* auswählen. Sie ist von der IP-Adresse durch einen "/" abgetrennt. Sie werden erneut aufgefordert, eine ***PORT***-Nummer einzutragen.
range	Definieren Sie einen IP Adressbereich, auf den diese Regel angewendet werden soll. Die Eingabeaufforderung erlaubt automatisch, zwei IP-Adressen einzutragen. Diese werden durch"-" abgetrennt. Sie werden erneut aufgefordert, eine ***PORT*** Nummer einzutragen.
dhcp	Nur für ***REMOTE: TYPE***. Das entfernte Gateway bezieht seine IP-Konfiguration per ➤➤ **DHCP**.
own/peer	Wenn Sie diese Option wählen, wird die IP-Adresse des Gateways (falls anwendbar) automatisch als von der Regel betroffen eingestuft. Es sind keine weiteren Einstellungen nötig. Auch wenn dieser Eintrag hier ausgewählt werden kann, ist er dennoch nicht anwendbar auf Pre IPSec Regeln. Er ist anwendbar für die Peer Konfiguration (siehe “Untermenü TRAFFIC LIST SETTINGS” auf Seite 42).

TABELLE 2-3: LOCAL/REMOTE: TYPE



Hinweis

Stellen Sie sicher, dass die Pre IPSec Regeln sorgfältig konfiguriert wurden. Dieses ist ausschlaggebend für das einwandfreie Funktionieren jeglichen Datenverkehrs, der nicht über IPSec-Prozeduren gesichert werden soll.

Besonders wichtig ist es, dass man IKE Traffic im Klartext passieren lässt. Dieses kann erfüllt werden, indem eine Pre IPSec Regel mit den folgenden Spezifikationen konfiguriert wird:

- ***PROTOCOL***= *udp*
- ***LOCAL TYPE***: *net* (die Felder für die IP-Adresse und Netzmaske bleiben leer)
- ***LOCAL PORT***: *500*
- ***REMOTE TYPE***: *net* (die Felder für die IP-Adresse und Netzmaske bleiben ebenfalls leer)
- ***REMOTE PORT***: *500*
- ***ACTION***: *pass*

Der IPSec Wizard passt die Einstellungen wenn nötig an.

3 Untermenü *CONFIGURE PEERS*

Im folgenden wird das Untermenü *CONFIGURE PEERS* beschrieben.

Das Menü zum Erstellen eines Peers (gleich welchen Typs) sieht folgendermaßen aus:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[IPSEC][PEERS][ADD]                                              MyGateway

     Description:
     Admin Status:      up        Oper Status:   dormant

     Peer Address:
     Peer IDs:
     Pre Shared Key:    *

     IPSec Callback >
     Peer specific Settings >

     Virtual Interface: no
     Traffic List Settings >

               SAVE                              CANCEL
```

Es enthält folgende Felder:

Feld	Wert
Description	Hier geben Sie eine beliebige Beschreibung des Peers ein. Die maximale Länge des Eintrags beträgt 255 Zeichen.

Feld	Wert
Admin Status	Hier wählen Sie den Zustand aus, in den Sie den Peer nach dem Speichern der Konfiguration versetzen wollen. Die Einstellung gilt für jede Art von Peer. Zur Verfügung stehen: ■ *up* - Der Peer steht nach dem Speichern der Konfiguration sofort für den Aufbau eines Tunnels zur Verfügung. ■ *down* - Der Peer steht nach dem Speichern der Konfiguration zunächst nicht zur Verfügung. ■ *dialup* - Nach dem Speichern wird einmalig ein Tunnel aufgebaut. Dabei werden alle möglichen Verbindungsarten (also auch Callback) berücksichtigt. ■ *callback* - Nach dem Speichern wird ein Tunnel zum Peer aufgebaut. Dabei wird so verfahren, als sei ein initialer Callback-Ruf bereits eingegangen.
Oper Status	Hier wird der derzeitige Zustand des Peers angezeigt. Das Feld ist nicht editierbar.
Peer Address	Hier geben Sie die offizielle ➤➤ **IP-Adresse** des Peers bzw. seinen auflösbaren ➤➤ **Host-Namen** ein. Die Eingabe kann in bestimmten Konfigurationen entfallen.
Peer IDs	Hier geben Sie die ID des Peers ein. Die Eingabe kann in bestimmten Konfigurationen entfallen. Auf dem Peer-Gateway entspricht diese ID der ***LOCAL ID*** (***CONFIGURE PEERS*** ➜ ***APPEND/EDIT*** ➜ ***PEER SPECIFIC SETTINGS*** ➜ ***IKE (PHASE 1) DEFAULTS: EDIT*** ➜ ***ADD/EDIT***).

Feld	Wert
Pre Shared Key	Nur bei Authentifizierung über Preshared Keys. Hier geben Sie den mit dem Peer vereinbarten Passphrase ein. Die ***AUTHENTICATION METHOD*** kann im Menü ***CONFIGURE PEERS*** ➜ **APPEND/EDIT** ➜ ***PEER SPECIFIC SETTINGS*** ➜ ***IKE (PHASE 1) DEFAULTS: EDIT*** für den Peer angepasst werden.
Virtual Interface	Hier legen Sie fest, ob der Peer mit einer Traffic List oder als virtuelles Interface geführt wird. Zur Verfügung stehen: ■ *no* - Verbindungen zum Peer werden über eine Traffic List gesteuert. ■ *yes* - Der Peer wird als virtuelles Interface erstellt. Der Datenverkehr, der über dieses Interface geroutet wird, wird vollständig verschlüsselt. Default ist *no*.

Tabelle 3-1: ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***APPEND/EDIT***

Die Anpassung des Peers erfolgt in den folgenden Menüs:

- ***IPSEC CALLBACK*** (Informationen zur Konfiguration des IPSec Callback Siehe “Untermenü IPSEC CALLBACK” auf Seite 14.)
- ***PEER SPECIFIC SETTINGS*** (Siehe “Untermenü PEER SPECIFIC SETTINGS” auf Seite 23.)
- ***TRAFFIC LIST SETTINGS*** (für ***VIRTUAL INTERFACE*** = *no*, Informationen zur Konfiguration von Traffic Lists siehe “Untermenü TRAFFIC LIST SETTINGS” auf Seite 42).
- ***INTERFACE IP SETTINGS*** (für ***VIRTUAL INTERFACE*** = *yes*, siehe “Untermenü INTERFACE IP SETTINGS” auf Seite 46).

3.1 Untermenü *IPSEC CALLBACK*

Um Hosts, die nicht über feste IP-Adressen verfügen, eine sichere Verbindung über das ➤➤ **Internet** zu ermöglichen, unterstützt Bintec seit dem Release 6.2.2 den DynDNS-Dienst. Dieser Dienst ermöglicht die Identifikation eines Peers anhand eines durch DNS auflösbaren Host-Namens. Die Konfiguration der IP-Adresse des Peers ist nicht notwendig.

Der DynDNS-Dienst signalisiert aber nicht, ob ein Peer wirklich online ist, und kann einen Peer nicht veranlassen, eine Internetverbindung aufzubauen, um einen IPSec-Tunnel über das Internet zu ermöglichen. Diese Möglichkeit wird mit dem IPSec-Callback geschaffen: Mit Hilfe eines direkten ➤➤ **ISDN**-Rufs bei einem Peer kann diesem signalisiert werden, dass man online ist und den Aufbau eines IPSec-Tunnels über das Internet erwartet. Sollte der gerufene Peer derzeit keine Verbindung zum Internet haben, wird er durch den ISDN-Ruf veranlaßt, eine Verbindung aufzubauen. Dieser ISDN-Ruf verursacht (je nach Einsatzland) keine Kosten, da der ISDN-Ruf vom Gateway nicht angenommen werden muß. Die Identifikation des Anrufers durch dessen ISDN-Rufnummer genügt als Information, um einen Tunnelaufbau zu initiieren.

Um diesen Dienst einzurichten, muß zunächst im Menü ***ISDN0*** ➜ ***INCOMING CALL ANSWERING*** eine Rufnummer für den IPSec-Callback konfiguriert werden. Dazu steht für das Feld ***ITEM*** der Wert *IPSec* zur Verfügung. Dieser Eintrag sorgt dafür, dass auf diese Nummer eingehende Rufe an den IPSec-Dienst geleitet werden.

Die weitere Konfiguration erfolgt im Menü ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***APPEND/EDIT***. Dort findet sich das Untermenü ***ISDN CALLBACK***:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[IPSEC][PEERS][EDIT][Callback]                                   MyGateway

     ISDN Callback:       both

     Incoming ISDN Number:
     Outgoing ISDN Number:

     Transfer own IP Address over ISDN:  no


                          SAVE                            CANCEL
```

Das Menü enthält folgende Felder:

Feld	Wert
ISDN Callback	Hier wählen Sie den Callback-Modus aus. Zu den verfügbaren Optionen, siehe Tabelle “ISDN Callback” auf Seite 17.
Incoming ISDN Number	Nur für ***ISDN CALLBACK*** = *passive* oder *both*. Hier geben Sie die ISDN-Nummer an, von der aus das entfernte Gateway das lokale Gateway ruft (Calling Party Number).
Outgoing ISDN Number	Nur für ***ISDN CALLBACK*** = *active* oder *both*. Hier geben Sie die ISDN-Nummer an, unter der das lokale Gateway das entfernte Gateway ruft (Called Party Number).
Transfer own IP Address over ISDN	Hier können Sie die Funktion aktivieren, die eine Übermittlung der IP-Adresse des lokalen Gateways an das entfernte Gateway ermöglicht. Zu dieser Funktion siehe “Übermittlung der IP-Adresse über ISDN” auf Seite 18.

Tabelle 3-2: ***IPSEC ➜ CONFIGURE PEERS ➜ IPSEC CALLBACK***

Hinweis

Bedenken Sie, dass in den Feldern ***INCOMING ISDN NUMBER*** und ***OUTGOING ISDN NUMBER*** immer die Nummer des entfernten Gateways eingetragen wird. Im allgemeinen werden die beiden Nummern bis auf die führende "0" identisch sein. Diese darf für das Feld ***IN*** nicht mit eingegeben werden.

Unter bestimmten Umständen (z. B. beim Betrieb des Gateways an einer Telefonanlage mit Rufnummernunterdrückung) kann es notwendig sein, unterschiedliche Nummern anzugeben. Fragen Sie den Systemadministrator nach den zu konfigurierenden Rufnummern.

Das Feld ***ISDN Callback*** kann folgende Werte annehmen:

Wert	Bedeutung
disabled	Der ISDN-Callback ist deaktiviert. Das lokale Gateway reagiert weder auf eingehende ISDN-Rufe noch initiiert es ISDN-Rufe zum entfernten Gateway.
passive	Das lokale Gateway reagiert lediglich auf eingehende ISDN-Rufe und initiiert ggf. den Aufbau eines IPSec-Tunnels zum Peer. Es werden keine ISDN-Rufe an das entfernte Gateway abgesetzt, um dieses zum Aufbau eines IPSec-Tunnels zu veranlassen.
active	Das lokale Gateway setzt einen ISDN-Ruf an das entfernte Gateway ab, um dieses zum Aufbau eines IPSec-Tunnels zu veranlassen. Auf eingehende ISDN-Rufe reagiert das Gateway nicht.
both	Das Gateway kann auf eingehende ISDN-Rufe reagieren und ISDN-Rufe an das entfernte Gateway absetzen. Der Aufbau eines IPSec-Tunnels wird sowohl ausgeführt (nach einem eingehenden ISDN-Ruf) als auch veranlaßt (durch einen ausgehenden ISDN-Ruf).

Tabelle 3-3: ISDN Callback

Wenn Sie einen Callback für einen Peer eingerichtet haben, wird dieser stets ausgeführt. Bei aktivem Callback wird daher, sobald ein IPSec-Tunnel benötigt wird, der Peer durch einen ISDN-Ruf veranlaßt, diesen zu initiieren. Bei passivem Callback wird immer dann ein Tunnelaufbau zum Peer initiiert, wenn ein ISDN-Ruf auf der entsprechenden Nummer eingeht. Auf diese Weise wird sichergestellt, dass beide Peers erreichbar sind und die Verbindung über das Internet zustande kommen kann. Es wird lediglich dann kein Callback ausgeführt,

wenn bereits SAs (Security Associations) vorhanden sind, der Tunnel zum Peer also bereits besteht.

Hinweis

Wenn ein Tunnel zu einem Peer aufgebaut werden soll, wird vom IPSec-Daemon zunächst das Interface aktiviert, über das der Tunnel realisiert werden soll. Sofern auf dem lokalen Gateway DynIPSec konfiguriert ist, wird dann die IP-Adresse propagiert und erst dann der ISDN-Ruf an das entfernte Gateway abgesetzt. Auf diese Art ist sichergestellt, dass das entfernte Gateway das lokale auch tatsächlich erreichen kann, wenn er den Tunnelaufbau initiiert.

3.1.1 Übermittlung der IP-Adresse über ISDN

Mittels der Übertragung der IP-Adresse eines Gateways über ISDN (im D-Kanal und/oder im B-Kanal) eröffnen sich neue Möglichkeiten zur Konfiguration von IPSec-VPNs. Einschränkungen, die bei der IPSec-Konfiguration mit dynamischen IP-Adressen auftreten, können so umgangen werden.

Vor Systemsoftware Release 7.1.4 unterstützte der IPSec ISDN Callback einen Tunnelaufbau nur dann, wenn die aktuelle IP-Adresse des Initiators auf indirektem Wege (z. B. über DynDNS) ermittelt werden kann. DynDNS hat aber gravierende Nachteile, wie z. B. die Latenzzeit, bis die IP-Adresse in der Datenbank wirklich aktualisiert ist. Dadurch kann es dazu kommen, dass die über DynDNS propagierte IP-Adresse nicht korrekt ist. Dieses Problem wird durch die Übertragung der IP-Adresse über ISDN umgangen. Darüber hinaus ermöglicht es diese Art der Übermittlung dynamischer IP-Adressen, den sichereren ID-Protect-Modus für den Tunnelaufbau zu verwenden.

Funktionsweise

Um die eigene IP-Adresse an den Peer übermitteln zu können, stehen unterschiedliche Modi zur Verfügung: Die Adresse kann im ➤➤ **D-Kanal** kostenfrei übertragen werden oder im ➤➤ **B-Kanal**, wobei der Ruf von der Gegenstelle angenommen werden muss und daher Kosten verursacht.

Wenn ein Peer, dessen IP-Adresse dynamisch zugewiesen worden ist, einen anderen Peer zum Aufbau eines IPSec-Tunnels veranlassen will, so kann er seine eigene IP-Adresse gemäß der in “Konfiguration” auf Seite 20 beschriebenen Einstellungen übertragen. Nicht alle Übertragungsmodi werden von allen

Telefongesellschaften unterstützt. Sollte diesbezüglich Unsicherheit bestehen, kann mittels der automatischen Auswahl durch das Gateway sichergestellt werden, dass alle zur Verfügung stehenden Möglichkeiten genutzt werden.

Hinweis

Damit das Gateway des gerufenen Peers die Informationen über die IP-Adresse identifizieren kann, sollte die Callback-Konfiguration auf den beteiligten Gateways identisch vorgenommen werden.

Die Übertragung der IP-Adresse und der Beginn der IKE-Phase-1-Aushandlung verlaufen in folgenden Schritten:

1. Peer A (der Initiator des Callbacks) stellt eine Verbindung zum Internet her, um eine dynamische IP-Adresse zugewiesen zu bekommen und um für Peer B über das Internet erreichbar zu sein.
2. Das Gateway erstellt ein begrenzt gültiges Token und speichert es zusammen mit der aktuellen IP-Adresse im zu Peer B gehörenden ➤➤ **MIB**-Eintrag.
3. Das Gateway setzt den initialen Ruf an Peer B ab. Dabei werden die IP-Adresse von Peer A sowie das Token gemäß der Callback-Konfiguration übermittelt.
4. Peer B extrahiert die IP-Adresse von Peer A sowie das Token aus dem ISDN-Ruf und ordnet sie Peer A aufgrund der konfigurierten ➤➤ **Calling Party Number** (der ISDN-Nummer, die Peer A verwendet, um den initialen Ruf an Peer B abzusetzen) zu.
5. Der IPSec-Daemon auf Peer Bs Gateway kann die übermittelte IP-Adresse verwenden, um eine Phase-1-Aushandlung mit Peer A zu initiieren. Dabei wird der Token in einem Teil der Payload innerhalb der IKE-Aushandlung an Peer A zurückgesendet.
6. Peer A ist nun in der Lage, das von Peer B zurückgesendete Token mit den Einträgen in der MIB zu vergleichen und so den Peer zu identifizieren, auch ohne dessen IP-Adresse zu kennen.

Da Peer A und Peer B sich wechselseitig identifizieren können, können auch unter Verwendung von Preshared Keys Aushandlungen im ID-Protect-Modus durchgeführt werden.

Konfiguration

Die Konfiguration erfolgt im Kontext der IPSec-Callback-Konfiguration im Menü ***IPSEC ➜ CONFIGURE PEERS ➜ APPEND/EDIT ➜ IPSEC CALLBACK***. Wird für das Feld ***TRANSFER OWN IP ADDRESS OVER ISDN*** der Wert *yes* gewählt, ändert sich das Menü folgendermaßen (der Screenshot enthält Beispielwerte):

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[IPSEC][PEERS][EDIT][Callback]                                   MyGateway

ISDN Callback:       both

     Incoming ISDN Number:1234
     Outgoing ISDN Number:01234

     Transfer own IP Address over ISDN:  yes

     Mode :  autodetect best possible mode (D or B channel)


               SAVE                              CANCEL
```

Es enthält nun die folgenden Felder:

Feld	Wert
Transfer own IP Address over ISDN	Hier wählen Sie aus, ob für den IPSec-Callback die IP-Adresse des eigenen Gateways über ISDN übertragen werden soll. Mögliche Werte: ■ *yes* - Die IP-Adresse wird gemäß den Einstellungen in den folgenden Feldern übertragen. ■ *no* - (Defaultwert) Die IP-Adresse wird nicht übertragen.

Feld	Wert
Mode	Nur sichtbar, wenn ***TRANSFER OWN IP ADDRESS OVER ISDN*** = *yes*. Hier wählen Sie aus, in welchem Modus das Gateway versucht, seine IP-Adresse an den Peer zu übertragen. Mögliche Werte: ■ *autodetect best possible mode (D or B channel)* - (Defaultwert) Das Gateway bestimmt automatisch den günstigsten Modus. Dabei werden zunächst alle D-Kanal-Modi versucht, bevor der B-Kanal verwendet wird (die Verwendung des B-Kanals verursacht Kosten). ■ *autodetect best possible mode (D channel only)* - Das Gateway bestimmt automatisch den günstigsten D-Kanal-Modus. Der B-Kanal ist von der Verwendung ausgeschlossen. ■ *use specific D channel mode* - Das Gateway versucht, die IP-Adresse in dem im Feld ***D-CHANNEL MODE*** eingestellten Modus zu übertragen. ■ *try specific D channel mode, fall back on B* - Das Gateway versucht, die IP-Adresse in dem im Feld ***D-CHANNEL MODE*** eingestellten Modus zu übertragen. Gelingt das nicht, wird die IP-Adresse im B-Kanal übetragen (dies verursacht Kosten). ■ *use B channel* - Das Gateway überträgt die IP-Adresse im B-Kanal. Dies verursacht Kosten.

Feld	Wert
D-Channel Mode	Nur sichtbar, wenn ***MODE*** = *use specific D channel mode* oder *try specific D channel mode, fall back on B*. Hier wählen Sie aus, in welchem D-Kanal-Modus das Gateway versucht, die IP-Adresse zu übertragen. Mögliche Werte: ■ *LLC* - (Defaultwert) Die IP-Adresse wird in den LLC Information Elements des D-Kanals übertragen. ■ *SUBADDR* - Die IP-Adresse wird in den Subaddress Information Elements des D-Kanals übertragen. ■ *LLC-and-SUBADDR* - Die IP-Adresse wird sowohl in den LLC- als auch in den Subaddress Information Elements übertragen.

Tabelle 3-4: ***IPSEC ➜ CONFIGURE PEERS ➜ APPEND/EDIT ➜ IPSEC CALLBACK***

3.2 Untermenü *PEER SPECIFIC SETTINGS*

Das Menü ***CONFIGURE PEERS*** ➜ ***APPEND/EDIT*** ➜ ***PEER SPECIFIC SETTINGS*** enthält die Optionen zur Anpassung der IKE- und IPSec-Einstellungen für den Peer:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[IPSEC][PEERS][EDIT][SPECIAL]: IPSec Peer Special Settings   MyGateway

 Special settings for p1

     IKE (Phase 1) Profile:   default                  edit >

     IPsec (Phase 2) Profile: default                  edit >

     Select Different Traffic List >

                           SAVE                          CANCEL
```

Dieses Menü erlaubt die Auswahl von zuvor definierten Profilen für Phase 1 und Phase 2. Der Wert *default* steht dabei für das im IPSec-Hauptmenü, Feld ***IKE (PHASE 1)/IPSEC (PHASE 2) DEFAULTS*** eingestellte Profil.

Das Menü ***SELECT DIFFERENT TRAFFIC LIST*** ist nur dann zugänglich, wenn ein Peer mit Traffic Lists angelegt wird.

3.2.1 Untermenü *IKE (PHASE 1) PROFILE*

Das Menü zur Konfiguration eines Phase-1-Profils ist bei der Peer-Konfiguration über das Menü ***CONFIGURE PEERS*** ➜ ***APPEND/EDIT*** ➜ ***PEER SPECIFIC SETTINGS*** ➜ ***IKE (PHASE 1) PROFILE: EDIT*** ➜ ***ADD/EDIT*** zugänglich:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[IPSEC] [PEERS] [ADD] [SPECIAL] [PHASE1] [ADD]                    MyGateway

 Description (Idx 0) :
   Proposal              :  none/default
   Lifetime              :  use default
   Group                 :  default
   Authentication Method :  default
   Mode                  :  default
   Heartbeats            :  default
   Block Time            :  -1
   Local ID              :
   Local Certificate     :  none
   CA Certificates       :

   View Proposals >
   Edit Lifetimes >

                         SAVE                          CANCEL
```

Das Menü enthält folgende Felder:

Feld	Wert
Description	Informationen zu diesen Parametern: Siehe “Proposal, Lifetime, Group...” auf Seite 26.
Proposal	
Lifetime	
Group	
Authentication Method	
Mode	

Feld	Wert
Heartbeats	Hier wählen Sie, ob und in welcher Weise IPSec Heartbeats verwendet werden. Um feststellen zu können, ob eine Security Association (SA) noch gültig ist oder nicht, hat Bintec einen IPSec-Heartbeat implementiert. Dieser sendet bzw. empfängt je nach Konfiguration Signale, bei deren Ausbleiben die SA als ungültig verworfen wird. Zur Verfügung stehen: ■ *default* - Das Gateway verwendet die Einstellung des Default-Profils. ■ *none* - Das Gateway sendet und erwartet keinen Heartbeat. ■ *expect* - Das Gateway erwartet einen Heartbeat vom Peer, sendet selbst aber keinen. ■ *send* - Das Gateway erwartet keinen Heartbeat vom Peer, sendet aber einen. ■ *both* - Das Gateway erwartet einen Heartbeat vom Peer und sendet selbst einen. Für Geräte der **VPN Access Linie** werden Heartbeats für Phase 1 und Phase 2 getrennt konfiguriert. Wenn Interoperabilität mit älterer Software zu gewährleisten ist, müssen für Phase 1 und Phase 2 die gleichen Werte konfiguriert werden.

Feld	Wert
Block Time	Hier legen Sie fest, wie lange ein Peer für Tunnelaufbauten blockiert wird, nachdem ein Phase-1-Tunnelaufbau fehlgeschlagen ist. Dies betrifft nur lokal initiierte Aufbauversuche. Zur Verfügung stehen Werte von *-1* bis *86400* (Sekunden), der Wert *-1* (Defaultwert) bedeutet die Übernahme des Wertes im Defaultprofil, der Wert *0*, dass der Peer in keinem Fall blockiert wird.
Local ID	Informationen zu diesen Parametern siehe "Proposal, Lifetime, Group..." auf Seite 26
Local Certificate	
CA Certificates	

Tabelle 3-5: ***IPSEC ➜ CONFIGURE PEERS ➜ APPEND/EDIT ➜ PEER SPECIFIC SETTINGS ➜ IKE (PHASE 1) PROFILE: EDIT ➜ ADD/EDIT***

3.2.2 Proposal, Lifetime, Group...

Die im Folgenden beschriebenen Felder des Menüs *IKE (PHASE 1) PROFILE: EDIT ➜ ADD/EDIT* bedürfen näherer Erläuterung.

Phase 1: Proposal

In diesem Feld können Sie auf Ihrem Gateway jede Kombination aus Verschlüsselungs- und Message-Hash-Algorithmen für IKE Phase 1 auswählen. Die Kombination von sechs Verschlüsselungsalgorithmen und vier Message Hash-Algorithmen ergibt 24 mögliche Werte in diesem Feld. Darüber hinaus können Sie den Wert *none/default* wählen, der dem Peer das im IPSec-Hauptmenü ausgewählte Default-Proposal zuweist.

In den folgenden beiden Tabellen sind die verfügbaren Verschlüsselungs- und Message Hash-Algorithmen aufgelistet:

Algorithmus	Beschreibung
Blowfish	➤➤ **Blowfish** ist ein sehr sicherer und zugleich schneller Algorithmus. Twofish kann als Nachfolger von Blowfish angesehen werden.
3DES	➤➤ **3DES** ist eine Erweiterung des DES Algorithmus mit einer effektiven Schlüssellänge von 112 Bit, was als sicher eingestuft wird. Es ist der langsamste Algorithmus, der derzeit unterstützt wird.
DES	➤➤ **DES** ist ein älterer Verschlüsselungsalgorithmus, der aufgrund seiner kleinen effektiven Länge von 56 Bit als schwach eingestuft wird.
CAST	➤➤ **CAST** ist ebenfalls ein sehr sicherer Algorithmus, etwas langsamer als Blowfish, aber schneller als 3DES.
Twofish	➤➤ **Twofish** war ein finaler Kandidat für den AES (Advanced Encryption Standard). Er wird als genauso sicher eingestuft wie Rijndael (AES), ist aber langsamer.
Rijndael	Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt

Tabelle 3-6: Verschlüsselungsalgorithmen

Im folgenden sind die verfügbaren ➤➤ **Hash**-Algorithmen aufgeführt:

Algorithmus	Beschreibung
MD5 (Message Digest #5)	➤➤ **MD5** ist ein älterer Hash Algorithmus. Wird mit 96 Bit Digest Length für IPSec verwendet.

Algorithmus	Beschreibung
SHA1 (Secure Hash Algorithm #1)	➤➤ **SHA1** ist ein Hash Algorithmus, der von der NSA (United States National Security Association) entwickelt wurde. Er wird als sicher eingestuft, ist aber langsamer als MD5. Wird mit 96 Bit Digest Length für IPSec verwendet.
RipeMD 160	➤➤ **RipeMD** 160 ist ein kryptographischer 160 Bit Hash-Algorithmus. Er wird als sicherer Ersatz für MD5 und RipeMD angewandt.
Tiger 192	➤➤ **Tiger 192** ist ein relativ neuer und sehr schneller Algorithmus.

Tabelle 3-7: Message Hash-Algorithmen

Hinweis

Beachten Sie, dass die Beschreibung der Verschlüsselung und Authentifizierung oder der Hash-Algorithmen auf dem Kenntnissstand und der Meinung des Autors zum Zeitpunkt der Erstellung dieses Handbuchs basiert. Die Qualität der Algorithmen im besonderen unterliegt relativen Gesichtpunkten und kann sich aufgrund von mathematischen oder kryptographischen Weiterentwicklungen ändern.

VIEW PROPOSALS Im Untermenü ***VIEW PROPOSALS*** erhalten Sie eine Übersicht über die Proposals, die vom IPSec-Wizard erstellt wurden:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[IPSEC][IKE PROPOSALS]: IKE Proposal                              MyGateway

    Description         Protocol                        Lifetime
    Blowfish/MD5        default  blowfish md5           900s/0KB (def)  =
    DES3/MD5            default  des3     md5           900s/0KB (def)  |
    CAST/MD5            default  cast12   md5           900s/0KB (def)  |
    DES/MD5             default  des      md5           900s/0KB (def)  |
    Blowfish/SHA1       default  blowfish sha1          900s/0KB (def)  |
    DES3/SHA1           default  des3     sha1          900s/0KB (def)  |
    CAST/SHA1           default  cast128  sha1          900s/0KB (def)  |
    DES/SHA1            default  des      sha1          900s/0KB (def)  |
    DES/Tiger192        default  des      tiger192      900s/0KB (def)  |
    DES/Ripemd160       default  des      ripemd160     900s/0KB (def)  |
    DES3/Tiger192       default  des3     tiger192      900s/0KB (def)  |
    DES3/Ripemd160      default  des3     ripemd160     900s/0KB (def)  |
    Blowfish/Tiger192   default  blowfish tiger192      900s/0KB (def)  |
    Blowfish/Ripemd160  default  blowfish ripemd160     900s/0KB (def)  v

    DELETE              EXIT
```

Dieses Menü dient lediglich der Information. Eine Konfiguration ist nicht möglich.

Phase 1: Lifetime

Dieses Feld zeigt die Lebensdauer (Lifetime) an, die ablaufen darf, bevor Phase-1-Schlüssel durch eine weitere Diffie-Hellman-Schlüsselberechnung erneuert werden müssen. Sie kann entweder als Wert in Sekunden, als verarbeitete Datenmenge (in Kb) oder als Kombination aus beiden konfiguriert werden. Der Defaultwert beträgt *900 sec/11000 Kb,* das bedeutet, dass die Schlüssel erneuert werden, wenn entweder 900 Sekunden abgelaufen sind oder 11000 Kb Daten verarbeitet wurden, je nachdem, welches Ereignis zuerst eintritt. Falls Sie zusätzliche Lebensdauerwerte konfiguriert haben, können Sie unter diesen hier auswählen.

Falls Sie sich entschließen, zusätzliche Lebensdauerwerte zu konfigurieren, können Sie dies im Menü ***EDIT LIFETIMES*** durchführen. Die Menümaske sieht folgendermaßen aus:

```
VPN Access Setup Tool                    Bintec Access Networks GmbH
[IPSEC][LIFETIME]: IPsec Configuration - Life Times          MyGateway

     Edit Lifetime Values

          Lifetime Restriction Based On: Time and Traffic

               900         Seconds

               11000       Kb

          Matching Policy:              Loose


                    SAVE                                  Exit
```

Das Menü umfasst folgende Felder:

Feld	Wert
Lifetime Restriction Based On	Wählen Sie das Kriterium für das Ende der Schlüssellebensdauer, mögliche Werte sind: ■ *Time* and *Traffic* ■ *Time* ■ *Traffic* Abhängig von Ihrer Wahl wird Ihnen eines der folgenden Felder oder beide angezeigt.
Seconds	Geben Sie die Lebensdauer für Phase-1-Schlüssel in Sekunden ein. Der Wert darf jeder ganzzahlige Wert bis zu einer Länge von 32 Bit sein.

Feld	Wert
Kb	Geben Sie die Lebensdauer für Phase-1-Schlüssel als Menge der verarbeiteten Daten in Kb ein. Der Wert darf jeder ganzzahlige Wert bis zu einer Länge von 32 Bit sein.
Matching Policy	Hier können Sie auswählen, wie strikt das Gateway die konfigurierte Lifetime einhält. Zur Verfügung stehen: ■ *loose* - Das Gateway akzeptiert und übernimmt jede Lifetime, die bei der Aushandlung vorgeschlagen wird (Defaultwert). ■ *strict* - Das Gateway akzeptiert und verwendet nur die konfigurierte Lifetime. Bei Abweichung scheitert die Phase-1-Aushandlung. ■ *notify* - Das Gateway akzeptiert alle vorgeschlagenen Werte, die größer sind, als der konfigurierte, verwendet selbst aber den eigenen, kleineren Wert und informiert den Peer darüber.

TABELLE 3-8: LIFETIME

Phase 1: Group

Die Gruppe (Group) definiert den Parametersatz, der für die Diffie-Hellman-Schlüsselberechnung während der Phase 1 zugrunde gelegt wird. "MODP", wie es von Bintec-Gateway unterstützt wird, steht für "modular exponentiation". Es können drei verschiedene Vorgaben ausgewählt werden, wobei 768, 1024 oder 1536 Bit genutzt werden.

Das Feld kann folgende Werte annehmen:

Wert	Bedeutung
1 (768 bit MODP)	Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 768 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.
2 (1024 bit MODP)	Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1024 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.
5 (1536 bit MODP)	Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1536 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.
none	Das Gateway verwendet nach dem Ablauf der Lifetime keine bestimmte Exponentiation, sondern verfährt wie beim initialen Tunnelaufbau.
default	Das Gateway verwendet die Einstellung des Default-Profils.

Tabelle 3-9: ***PHASE 1: GROUP***

Phase 1: Authentication Method

Dieses Feld zeigt die Authentifizierungsmethode an, die Sie während der Konfiguration mit dem IPSec-Wizard gewählt haben und ermöglicht Ihnen, diese zu ändern:

Wert	Bedeutung
Pre Shared Keys	Falls Sie für die Authentifizierung keine Zertifikate verwenden, können Sie *Pre Shared Keys* wählen. Diese werden bei der Peerkonfiguration im Menü ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***APPEND/EDIT*** konfiguriert.

Wert	Bedeutung
DSA Signatures	Phase-1-Schlüsselberechnungen werden unter Nutzung des ➤➤ **DSA**-Algorithmus authentifiziert.
RSA Signatures	Phase-1-Schlüsselberechnungen werden unter Nutzung des ➤➤ **RSA**-Algorithmus authentifiziert.
RSA Encryption	Mit RSA-Verschlüsselung werden als erweiterte Sicherheit zusätzlich die ID-Nutzdaten verschlüsselt.
default	Dieser Wert wird angezeigt, falls Sie den Peer so konfiguriert haben, dass er die globalen Defaults nutzt.

Tabelle 3-10: ***AUTHENTICATION METHOD***

Phase 1: Mode

Das Mode-Feld zeigt den momentan konfigurierten Phase-1-Modus an und ermöglicht Ihnen, die Einstellungen zu verändern:

Wert	Bedeutung
id_protect	Dieser Modus (auch als Main Mode bezeichnet) erfordert sechs Meldungen für eine Diffie-Hellman-Schlüsselberechnung und damit für die Einrichtung eines sicheren Kanals, über den die IPSec SAs ausgehandelt werden. Er setzt voraus, dass beide Peers statische IP-Adressen haben, falls für die Authentifizierung Preshared Keys genutzt werden. Bei der Verwendung des IPSec-Callbacks entfällt diese Einschränkung. Siehe “Untermenü IPSEC CALLBACK” auf Seite 14.

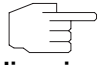
Wert	Bedeutung
aggressive	Der Aggressive Mode ist erforderlich, falls einer der Peers keine statische IP-Adresse hat und Preshared Keys für die Authentifizierung genutzt werden; er erfordert nur drei Meldungen für die Einrichtung eines sicheren Kanals.
default	Dem Peer wird kein spezifischer Modus zugewiesen, die globale Default-Einstellung wird verwendet.
id-protect-only	Das Gateway akzeptiert bei der Aushandlung ausschließlich den ID Protect Mode. Schlägt der Peer einen anderen Modus vor, scheitert die Aushandlung.
aggressive-only	Das Gateway akzeptiert bei der Aushandlung ausschließlich den Aggressive Mode. Schlägt der Peer einen anderen Modus vor, scheitert die Aushandlung.

TABELLE 3-11: MODUS

Phase 1: Local ID

Das ist die ID, die Sie Ihrem Gateway zuweisen. Falls Sie dieses Feld leer lassen, wählt das Gateway die Defaultwerte. Diese sind:

- Bei Authentifizierung mit Preshared Keys: die lokale IP-Adresse wie im *IPSECPEERLOCALADDRESS*-Feld in der *IPSECPEERTABLE* angegeben.
- Bei Authentifizierung mit ➤➤ **Zertifikat**: der erste im Zertifikat angegebene Subjekt-Alternativname oder, falls keiner angegeben ist, der Subjektname des Zertifikats.



Hinweis

Falls Sie Zertifikate für die Authentifizierung nutzen und Ihr Zertifikat Subjekt-Alternativnamen enthält (siehe "Zertifikatanforderung" auf Seite 73), müssen Sie hier achtgeben, da das Gateway per Default den ersten Subjekt-Alternativnamen wählt. Stellen Sie sicher, dass Sie und Ihr Peer beide den gleichen Namen nutzen, d.h. dass Ihre lokale ID und die Peer-ID, die Ihr Partner für Sie konfiguriert, identisch sind.

Phase 1: Local Certificate

Dieses Feld ermöglicht Ihnen, eines Ihrer eigenen Zertifikate für die Authentifizierung zu wählen. Es zeigt die Indexnummer dieses Zertifikats und den Namen an, unter dem es gespeichert ist. Dieses Feld wird nur bei Authentifizierungseinstellungen auf Zertifikatbasis angezeigt und weist darauf hin, dass ein Zertifikat zwingend erforderlich ist.

CA Certificates

Hier können Sie eine Liste zusätzlicher ➤➤ **CA**-Zertifikate eingeben, die für dieses Profil akzeptiert werden sollen. Einträge werden mit Kommata getrennt. Dadurch wird es z. B. möglich, auch für selbstsignierte Zertifikate ein CA-Zertifikat zu übermitteln.

Falls das CA-Zertifikat keine Zertifikat-Rückrufliste (Certificate Revocation List, CRL) oder keine CRL-Verteilstelle enthält und auf dem Gateway kein Zertifikatserver konfiguriert ist, wird die Variable ***NoCRLs*** auf "True" gesetzt. Zertifikate von dieser CA werden nicht auf ihre Gültigkeit überprüft.

3.2.3 Untermenü *IPSEC (PHASE 2) PROFILE*

Ebenso wie für die Phase 1 können Sie Profile für die Phase 2 des Tunnelaufbaus definieren.

Die Konfiguration erfolgt im Menü ***CONFIGURE PEERS ➜ APPEND/EDIT ➜ PEER SPECIFIC SETTINGS ➜ IPSEC (PHASE 2) PROFILE: EDIT ➜ ADD/EDIT***:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[IPSEC][PEERS][ADD][SPECIAL][PHASE2][ADD]                        MyGateway

   Description (Idx 0) :

   Proposal              :  default
   Lifetime              :  use default
   Use PFS               :  default
   Heartbeats            :  default
   Propagate PMTU        :  default


   View Proposals >
   Edit Lifetimes >


                         SAVE                              CANCEL
```

Das Menü enthält die folgenden Felder:

Feld	Wert
Proposal	Informationen zu diesen Parametern finden Sie bei "Proposal, Lifetime, Use PFS..." auf Seite 38
Lifetime	
Use PFS	

Feld	Wert
Heartbeats	Hier wählen Sie, ob und in welcher Weise IPSec Heartbeats verwendet werden. Um feststellen zu können, ob eine Security Association (SA) noch gültig ist oder nicht, hat Bintec einen IPSec-Heartbeat implementiert. Dieser sendet bzw. empfängt je nach Konfiguration Signale, bei deren Ausbleiben die SA als ungültig verworfen wird. Zur Verfügung stehen: ■ *default* - Das Gateway verwendet die Einstellung des Default-Profils. ■ *none* - Das Gateway sendet und erwartet keinen Heartbeat. ■ *expect* - Das Gateway erwartet einen Heartbeat vom Peer, sendet selbst aber keinen. ■ *send* - Das Gateway erwartet keinen Heartbeat vom Peer, sendet aber einen. ■ *both* - Das Gateway erwartet einen Heartbeat vom Peer und sendet selbst einen. Für Geräte der **VPN Access Line** werden Heartbeats für Phase 1 und Phase 2 getrennt konfiguriert. Wenn Interoperabilität mit älterer Software zu gewährleisten ist, müssen für Phase 1 und Phase 2 die gleichen Werte konfiguriert werden.

Feld	Wert
Propagate PMTU	Hier wählen Sie aus, ob während der Phase 2 die PMTU (Path Maximum Transfer Unit) propagiert werden soll oder nicht. Zur Verfügung stehen: ■ *default* - Das Gateway verwendet die Einstellung des Default-Profils. ■ *no* - Die Path Maximum Transfer Unit wird nicht übermittelt (Defaultwert). ■ *yes* - Die Path Maximum Transfer Unit wird übermittelt.

Tabelle 3-12: ***IPSEC ➜ CONFIGURE PEERS ➜ APPEND/EDIT ➜ PEER SPECIFIC SETTINGS ➜ IPSEC (PHASE 2) PROFILE: EDIT ➜ ADD/EDIT***

Das Menü ***VIEW PROPOSALS*** dient wie bei den Phase-1-Proposals lediglich der Auflistung der zur Verfügung stehenden Proposals. Das Menü ***EDIT LIFETIMES*** unterscheiden sich nicht von dem "Phase 1: Lifetime" auf Seite 29 in beschriebenen.

3.2.4 Proposal, Lifetime, Use PFS...

Die im Folgenden beschriebenen Felder des Menüs *IPSEC (PHASE 2) PROFILE: EDIT ➜ ADD/EDIT* bedürfen näherer Erläuterung.

Phase 2: Proposal

Dieses Feld ermöglicht Ihnen, jede Kombination aus IPSec-Protokoll, ➤➤ **Verschlüsselung**salgorithmus und/oder Message-Hash-Algorithmus zu wählen. In den folgenden Tabellen sind die Elemente dieser potentiellen Kombinationen aufgeführt:

IPSec-Protokoll	Beschreibung
ESP (Encapsulated Security Payload)	➤➤ **ESP** bietet Nutzdatenverschlüsselung sowie Authentifizierung.

IPSec-Protokoll	Beschreibung
AH (Authentication Header)	➤➤ **AH** bietet nur Authentifizierung, aber keine Nutzdatenverschlüsselung. Falls Sie eine Kombination wählen, bei der das AH-Protokoll benutzt wird, wird als Verschlüsselungsalgorithmus *none* angezeigt, z. B. *(AH (none, MD5)).*

Tabelle 3-13: IPSec-Protokolle

Zusätzlich zur Verschlüsselung und Authentifizierung unterstützt Bintec's IPSec-Implementierung die ➤➤ **Kompression** von IP-Nutzdaten durch ➤➤ **IPComP** (IP Payload Compression Protocol). IP-Nutzdatenkompression ist ein Protokoll zur Verkleinerung von IP-Datagrammen. Dieses Protokoll vergrößert die Gesamt-Kommunikationsperformance zwischen einem Paar miteinander kommunizierender Hosts/Gateways ("Knoten"). Es komprimiert die Datagramme, vorausgesetzt, die Knoten verfügen über ausreichende Rechenleistung, entweder durch die Leistung der CPU oder durch einen Kompressions-Koprozessor, und die Kommunikation erfolgt über langsame oder gestörte Verbindungen.

Die IP-Nutzdatenkompression ist besonders nützlich, wenn ➤➤ **IP**-Datagramme verschlüsselt werden. Die Verschlüsselung von IP-Datagrammen sorgt dafür, dass die Daten eine Zufallsnatur erhalten, wodurch eine Kompression auf niedrigeren Protokollebenen (z. B. PPP Compression Control Protocol [RFC1962]) unwirksam ist. Falls sowohl Kompression als auch Verschlüsselung gefordert sind, muss die Kompression vor der Verschlüsselung durchgeführt werden.

Bei allen IPSec-Proposals, bei denen keine bestimmte Einstellung für IPComP festgelegt ist, ist IPComP freigegeben. Das bedeutet, dass das Gateway während der SA-Aushandlung alle Proposals akzeptiert, unabhängig davon, ob diese die Nutzung von IPComP vorschlagen oder nicht. Falls der lokale Rechner die Aushandlung initiiert, schlägt er die Nutzung von IPComP als Vorzugs-Proposal vor, erlaubt jedoch dem antwortenden Rechner, einen Proposal ohne IPComP zu wählen.

Sie können dieses Verhalten ändern, indem Sie ein IPSec Proposal wählen, der eine der folgenden Einstellungen für ➤➤ **IPComP** festlegt:

IPComp-Option	Beschreibung
no Comp	Ihr Gateway akzeptiert keine SAs, die die Nutzung von IPComp festlegen. Falls der Peer so konfiguriert wurde, dass sein oder ihr Gateway IPComP vorschlägt, dann schlägt die IPSec SA-Aushandlung fehl und es wird keine Verbindung hergestellt.
force Comp	Ihr Gateway fordert, dass bei der IPSec SA-Aushandlung IPComP vereinbart werden kann. Falls der Peer dies nicht akzeptiert, wird keine Verbindung hergestellt.

Tabelle 3-14: IPComP-Optionen bei IPSec-Proposals

Da die wichtigsten Verschlüsselungs- und Hash-Algorithmen bereits beschrieben wurden, werden sie hier nur noch aufgelistet. Nur der NULL-Algorithmus steht in Phase 1 nicht zur Verfügung:

Algorithmen	Beschreibung
Blowfish	Beschreibungen der Verschlüsselungsalgorithmen finden Sie in Tabelle “Verschlüsselungsalgorithmen” auf Seite 27.
3DES	
DES	
CAST	
Twofish	
Rijndael	
NULL	Der NULL-"Algorithmus" nimmt keine Verschlüsselung der IP-Pakete vor, ist jedoch notwendig, falls IP-Pakete eine Authentifizierung durch das ESP-Protokoll ohne Verschlüsselung benötigen.

Tabelle 3-15: Phase-2-Verschlüsselungsalgorithmen

Dies sind die verfügbaren Hash-Algorithmen:

Algorithmen	Beschreibung
MD5	Beschreibungen der Message-Hash-Algorithmen finden Sie in Tabelle “Message Hash-Algorithmen” auf Seite 28.
SHA1	
NULL	Falls der NULL-"Algorithmus" für die Authentifizierung angewandt wird, wird unter ESP kein Message Hash erzeugt und die Nutzdaten werden nur verschlüsselt.

Tabelle 3-16: Message-Hash-Algorithmen in Phase 2

Hinweis

Beachten Sie, dass der NULL-Algorithmus in einem einzelnen Proposal entweder nur für die Verschlüsselung oder nur für die Authentifizierung festgelegt werden kann, aber nicht für beides.

Beachten Sie, dass RipeMD 160 und Tiger 192 für Message Hashing in Phase 2 nicht zur Verfügung stehen.

Ein Phase-2-Proposal würde somit beispielsweise folgendermaßen aussehen:

Beispielwerte	Bedeutung
1 (ESP(Blowfish, MD5))	IP-Pakete werden unter Anwendung des ➤➤ **ESP**-Protokolls, der Blowfish-Verschlüsselung und des MD5 Message Hash verarbeitet.
10 (ESP(NULL, SHA1))	IP-Pakete werden unter Anwendung des ESP-Protokolls verarbeitet; die NULL-Verschlüsselung und SHA 1 werden zur Erzeugung des Message Hash genutzt.
16 (AH(none, MD5))	IP-Pakete werden unter Anwendung des AH-Protokolls, ohne Verschlüsselung und mit MD5 als Message Hash-Algorithmus verarbeitet.

Tabelle 3-17: Beispiele für ***PHASE 2: PROPOSALS***

Phase 2: Lifetime

Informationen über die Lebensdauer des Proposals finden Sie unter "Phase 1: Lifetime" auf Seite 29. Falls Sie eine bestimmte IPSec-SA-Lebensdauer für diesen Peer festlegen möchten, können Sie dies im Menü ***EDIT LIFETIME*** vornehmen.

Use PFS

Da PFS (Perfect Forward Secrecy) eine weitere Diffie-Hellman-Schlüsselberechnung erfordert, um neues Verschlüsselungsmaterial zu erzeugen, müssen Sie die Exponentiations-Merkmale wählen. Wenn Sie PFS aktivieren, sind die Optionen die gleichen, wie bei der Konfiguration in ***PHASE 1: GROUP*** ("Phase 1: Group" auf Seite 31). PFS wird genutzt, um die Schlüssel einer umgeschlüsselten Phase-2-SA zu schützen, auch wenn die Schlüssel der Phase-1-SA bekannt geworden sind.

3.2.5 Untermenü *SELECT DIFFERENT TRAFFIC LIST*

Dieses Menü steht nur dann zur Verfügung, wenn Sie einen Peer konfigurieren, der auf Traffic Lists beruht und nicht auf einem virtuellen Interface.

In diesem Menü werden die für diesen Peer konfigurierten Traffic Lists angezeigt. Falls Sie mehr als eine Traffic List konfiguriert haben, können Sie wählen, welche aktiviert werden soll. Eine Liste aller verfügbaren Traffic Lists wird angezeigt und Sie können daraus wählen, wie es in der Hilfefunktion des Menüfensters beschrieben ist.

3.3 Untermenü *TRAFFIC LIST SETTINGS*

In diesem Menü erstellen Sie die Regeln, gemäß denen der Datenverkehr zum Peer behandelt wird. Sie können einen Traffic-List-Eintrag erstellen oder abändern.

Das Menüfenster, welches sich öffnet, sieht in beiden Fällen folgendermaßen aus (falls Sie einen vorhandenen Eintrag ändern, werden die Werte für diesen Eintrag angezeigt):

```
VPN Access Setup Tool                          Bintec Communications AG
[IPSEC][PEERS][EDIT][TRAFFIC][ADD]: Edit Traffic Entry       MyGateway

Description:


     Protocol:      dont-verify

     Local:
          Type: net   Ip:                / 0

     Remote:
          Type: net   Ip:                / 0


     Action:        pass

     Profile          default              edit >


                    SAVE                                  CANCEL
```

In den Feldern dieses Menüs sind folgende Werte möglich:

Feld	Wert
Description	Geben Sie eine Beschreibung ein, aus der hervorgeht, welche Art einer Regel (Rule) von Ihnen definiert wurde.
Protocol	Hier können Sie festlegen, ob der für diese Regel vorgesehene Datenverkehr nur auf die Pakete eines bestimmten Protokolls angewandt wird. Sie haben die Wahl zwischen der Festlegung eines Protokolls und der Option *dont-verify*, letzteres bedeutet, dass das Protokoll nicht als Filterkriterium herangezogen wird.

Feld	Wert
Local: Type	Geben Sie die lokalen Adresseinstellungen ein. Einzelheiten dazu finden Sie in der Tabelle “LOCAL/REMOTE: TYPE” auf Seite 46 unten.
Remote: Type	Geben Sie die Adresseinstellungen der fernen Gegenstelle ein. Die Optionen sind weitgehend identisch mit den Optionen im Feld ***LOCAL: TYPE***, mit einer Ausnahme: Die Option *own* gibt es nicht, stattdessen wird die Option *peer* angeboten. Dies ist jedoch nur bei Peer-Konfiguration relevant.
Action	Hier können Sie zwischen drei Optionen wählen: ■ *pass* ■ *drop* ■ *protect* Einzelheiten dazu finden Sie in Tabelle “ACTION” auf Seite 46 unten.
Profile	Nur für ***ACTION*** = *protect*. Hier wählen Sie ein IPSec-Profil aus, dass für die Verschlüsselung des Datenverkehrs verwendet werden soll. Die Einstellungsmöglichkeiten entsprechen denen des in “Untermenü IPSEC (PHASE 2) PROFILE” auf Seite 35 beschriebenen Menüs.

Tabelle 3-18: ***IPSEC ➜ CONFIGURE PEERS ➜ APPEND/EDIT ➜ TRAFFIC LIST SETTINGS***

Local/Remote: Type

Im Feld ***LOCAL/REMOTE: TYPE*** gibt es folgende Optionen:

Wert	Bedeutung
host	Geben Sie die ➤➤ **IP-Adresse** eines einzelnen Rechners ein, der unter diese Regel (Rule) fallen soll. Falls Sie bestimmte Protokolle gewählt haben, um den betreffenden Datenverkehr einzugrenzen, können Sie aufgefordert werden, eine ➤➤ ***PORT***-Nummer anzugeben. Dies gilt jedoch nur für UDP und TCP.
net	Geben Sie die IP-Adresse eines Netzes und die dazugehörige ➤➤ Netzmaske ein, die unter diese Regel fallen sollen. Die Eingabeaufforderung für die Netzmaske erscheint automatisch, wenn Sie *net* wählen. Sie wird von der Eingabeaufforderung für die IP-Adresse durch das Zeichen "/" getrennt. Auch hier können Sie aufgefordert werden, eine ***PORT***-Nummer anzugeben.
range	Geben Sie einen IP-Adressenbereich ein, der unter diese Regel fallen soll. Die Eingabeaufforderung ändert sich automatisch so, dass Sie zwei IP-Adressen eingeben können, die durch ein "-" voneinander getrennt sind. Auch hier können Sie aufgefordert werden, eine ***PORT***-Nummer anzugeben.
dhcp	Nur für ***REMOTE: TYPE***. Das entfernte Gateway bezieht seine IP-Konfiguration per ➤➤ **DHCP**.

Wert	Bedeutung
own/peer	Falls Sie diese Option wählen, wird automatisch angenommen, dass die dynamische IP-Adresse des Gateways (sofern anwendbar) unter diese Regel fällt. In diesem Fall sind keine weiteren Einstellungen notwendig.

Tabelle 3-19: ***LOCAL/REMOTE: TYPE***

Action Im Feld ***ACTION*** gibt es folgende Optionen:

Wert	Bedeutung
pass	Diese Option ermöglicht es, bestimmte IPSec Pakete unverändert passieren zu lassen.
drop	Diese Option verwirft alle Pakete, die den konfigurierten Filtern entsprechen.
protect	Der Datenverkehr wird gemäß des ausgewählten Profils verschlüsselt und/oder authentifiziert.

Tabelle 3-20: ***ACTION***

3.4 Untermenü *INTERFACE IP SETTINGS*

Dieses Menü wird sichtbar, wenn Sie im Menü *IPSEC* ➜ *CONFIGURE PEERS* ➜ *APPEN/EDIT* für das Feld *VIRTUAL INTERFACE* *yes* ausgewählt haben. Es ermöglicht die Konfiguration der IP-Parameter des virtuellen Interfaces.

Die Einstellungen für das virtuelle IPSec-Interface werden in den Menüs ***BASIC IP-SETTINGS***, ***MORE ROUTING*** und ***ADVANCED SETTINGS*** vorgenommen. Diese entsprechen den im Kapitel **WAN Partner** beschriebenen IP-Menüs. Das Menü ***MORE ROUTING*** ist nur dann sichtbar, wenn die grundlegenden Einstellungen im Menü Advanced Settings vorgenommen worden sind.

4 Untermenü *POST IPSEC RULES*

Im folgenden wird das Untermenü *POST IPSEC RULES* beschrieben.

Genauso, wie Sie Pre IPSec Rules konfigurieren müssen, die für den gesamten Datenverkehr gelten, bevor IPSec-SAs angewandt werden, müssen Sie Post IPSec Rules konfigurieren, die angewandt werden, nachdem ein Paket die Peer Traffic Lists passiert hat, d.h. falls keine Einträge in der Traffic List zu dem Paket gepasst haben.

Wenn Ihre Konfiguration optimal aufgebaut ist, müssen Sie möglicherweise nur eine einzige Post IPSec Rule konfigurieren, da alle Pakete, die verworfen oder im Klartext durchgelassen werden müssen, gemäß der Pre IPSec Rules behandelt werden, und alle Pakete, die geschützt werden müssen, gemäß den Peer Traffic Lists behandelt werden. Die einzige Entscheidung, die Sie somit hier fällen müssen, ist die, ob Sie alle "übrig gebliebenen" Pakete verwerfen oder passieren lassen möchten. Diese Entscheidung wird durch Auswahl eines Wertes für das Feld ***WHAT TO DO WITH ANYTHING THAT DIDN'T MATCH*** vorgenommen, welches Sie im ersten Fenster des Menüs ***IPSEC*** ➜ ***POST IPSEC RULES*** finden.

Dieses Feld kann folgende Werte annehmen:

Wert	Bedeutung
drop it	Alle Pakete, die nicht eine der IPSec Rules erfüllen, werden verworfen, nachdem IPSec angewandt wurde.
let pass	Alternativ kann allen Paketen, die nicht durch die IPSec Rules abgedeckt werden, erlaubt werden, zu passieren.

Tabelle 4-1: ***WHAT TO DO WITH ANYTHING THAT DIDN'T MATCH***

4.1 Untermenü *APPEND/EDIT*

Post IPSec Rules werden im Menü ***IPSEC*** ➜ ***POST IPSEC RULES*** ➜ ***APPEND/EDIT*** entweder bearbeitet oder hinzugefügt. In beiden Fällen sieht

das Menüfenster, welches sich öffnet, folgendermaßen aus (falls Sie einen vorhandenen Eintrag bearbeiten, werden die Werte für diesen Eintrag angezeigt):

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[IPSEC][POST IPSEC TRAFFIC][ADD]: Edit Traffic Entry          MyGateway

Description:


     Protocol:      dont-verify

     Local:
          Type: net   Ip:                / 0

     Remote:
          Type: net   Ip:                / 0


     Action:        pass


                    SAVE                                   CANCEL
```

Die Felder in diesem Menü können folgende Werte einnehmen:

Feld	Wert
Description	Geben Sie eine Beschreibung ein, aus der hervorgeht, welche Art Rule von Ihnen definiert wurde.
Protocol	Hier können Sie festlegen, ob der für diese Rule vorgesehene Datenverkehr nur auf die Pakete eines bestimmten Protokolls angewandt werden soll. Sie haben die Wahl zwischen der Festlegung eines Protokolls und der Option *dont-verify*; letzteres bedeutet, dass das Protokoll nicht als Filterkriterium benutzt wird.
Local: Type	Geben Sie die lokalen Adresseinstellungen ein. Einzelheiten dazu finden Sie in Tabelle “LOCAL/REMOTE: TYPE” auf Seite 50 unten.

Feld	Wert
Remote: Type	Geben Sie die Adresseinstellungen der fernen Gegenstelle ein. Die Optionen sind weitgehend identisch mit den Optionen im Feld ***LOCAL: TYPE***, mit einer Ausnahme: Die Option *own* gibt es nicht, stattdessen wird die Option *peer* angeboten. Dies ist jedoch nur bei Peer-Konfiguration relevant.
Action	Hier können Sie zwischen zwei Optionen wählen: ■ *pass*: Diese Option ermöglicht es, bestimmte Pakete IPSec unverändert passieren zu lassen. ■ *drop*: Diese Option verwirft alle Pakete, die den konfigurierten Filtern entsprechen.

Tabelle 4-2: ***IPSEC ➜ POST IPSEC RULES ➜ APPEND/EDIT***

LOCAL/REMOTE: TYPE Im Feld ***LOCAL/REMOTE: TYPE*** gibt es folgende Optionen:

Wert	Bedeutung
host	Geben Sie die IP-Adresse eines einzelnen Rechners ein, der unter diese Regel (Rule) fallen soll. Falls Sie bestimmte ➤➤ **Protokolle** gewählt haben, um den betreffenden Datenverkehr einzugrenzen, können Sie aufgefordert werden, eine ***PORT***-Nummer anzugeben. Dies gilt jedoch nur für ➤➤ **UDP** und ➤➤ **TCP**.

Wert	Bedeutung
net	Geben Sie die ➤➤ **IP-Adresse** eines Netzes und die dazugehörige Netzmaske ein, die unter diese Regel fallen sollen. Die Eingabeaufforderung für die ➤➤ **Netzmaske** erscheint automatisch, wenn Sie *net* wählen. Sie wird von der Eingabeaufforderung für die IP-Adresse durch das Zeichen "/" getrennt. Auch hier können Sie aufgefordert werden, eine ***PORT***-Nummer anzugeben.
range	Geben Sie einen IP-Adressenbereich ein, der unter diese Regel fallen soll. Die Eingabeaufforderung ändert sich automatisch so, dass Sie zwei IP-Adressen eingeben können, die durch ein "-" voneinander getrennt sind. Auch hier können Sie aufgefordert werden, eine ***PORT***-Nummer anzugeben.
dhcp	Nur für ***REMOTE: TYPE***. Das entfernte Gateway bezieht seine IP-Konfiguration per ➤➤ **DHCP**.
own/peer	Falls Sie diese Option wählen, wird automatisch angenommen, dass die dynamische IP-Adresse des Gateways (sofern anwendbar) unter diese Regel fällt. In diesem Fall sind keine weiteren Einstellungen notwendig. Obwohl dieser Eintrag hier gewählt werden kann, hat er für die Post IPSec Rules keine Funktion. Er ist für Peer-Konfigurationen von Bedeutung (siehe "Untermenü TRAFFIC LIST SETTINGS" auf Seite 42).

TABELLE 4-3: LOCAL/REMOTE: TYPE

5 Untermenü *IKE (PHASE 1) DEFAULTS*

Im folgenden wird das Untermenü *IKE (PHASE 1) DEFAULTS: EDIT* beschrieben.

Das Menü zur Konfiguration eines globalen Phase-1-Profils ist über das Menü ***IPSEC*** ➜ **APPEND/EDIT** ➜ ***IKE (PHASE 1) DEFAULTS: EDIT*** ➜ ***ADD/EDIT*** zugänglich:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[IPSEC][PHASE1][ADD]                                              MyGateway

 Description (Idx 0) :
   Proposal                :  none/default
   Lifetime                :  use default
   Group                   :  default
   Authentication Method   :  default
   Mode                    :  default
   Heartbeats              :  default
   Block Time              :  -1
   Local ID                :
   Local Certificate       :  none
   CA Certificates         :

   View Proposals >
   Edit Lifetimes >

                          SAVE                              CANCEL
```

Das Menü enthält folgende Felder:

Feld	Wert
Description	Informationen zu diesen Parametern: Siehe “Proposal, Lifetime, Group...” auf Seite 53.
Proposal	
Lifetime	
Group	
Authentication Method	
Mode	

Feld	Wert
Heartbeats	Hier wählen Sie, ob und in welcher Weise IPSec Heartbeats verwendet werden. Um feststellen zu können, ob eine Security Association (SA) noch gültig ist oder nicht, hat Bintec einen IPSec-Heartbeat implementiert. Dieser sendet bzw. empfängt je nach Konfiguration Signale, bei deren Ausbleiben die SA als ungültig verworfen wird. Zur Verfügung stehen: ■ *default* - Das Gateway verwendet die Einstellung des vom IPSecWizard erstellten Profils. ■ *none* - Das Gateway sendet und erwartet keinen Heartbeat. ■ *expect* - Das Gateway erwartet einen Heartbeat vom Peer, sendet selbst aber keinen. ■ *send* - Das Gateway erwartet keinen Heartbeat vom Peer, sendet aber einen. ■ *both* - Das Gateway erwartet einen Heartbeat vom Peer und sendet selbst einen. Für Geräte der **VPN Access Linie** werden Heartbeats für Phase 1 und Phase 2 getrennt konfiguriert. Wenn Interoperabilität mit älterer Software zu gewährleisten ist, müssen für Phase 1 und Phase 2 die gleichen Werte konfiguriert werden.

Feld	Wert
Block Time	Hier legen Sie fest, wie lange ein Peer für Tunnelaufbauten blockiert wird, nachdem ein Phase-1-Tunnelaufbau fehlgeschlagen ist. Dies betrifft nur lokal initiierte Aufbauversuche. Zur Verfügung stehen Werte von *-1* bis *86400* (Sekunden), der Wert *-1* (Defaultwert) bedeutet die Übernahme des Wertes im Defaultprofil, der Wert *0*, dass der Peer in keinem Fall blockiert wird.
Local ID	Informationen zu diesen Parametern siehe "Proposal, Lifetime, Group..." auf Seite 53
Local Certificate	
CA Certificates	

Tabelle 5-1: ***IPSec ➜ IKE (Phase 1) Profile: edit ➜ ADD/EDIT***

5.1 Proposal, Lifetime, Group...

Die im Folgenden beschriebenen Felder des Menüs *IKE (Phase 1) Profile: edit ➜ ADD/EDIT* bedürfen näherer Erläuterung.

Phase 1: Proposal

In diesem Feld können Sie auf Ihrem Gateway jede Kombination aus ➤➤ **Verschlüsselungs-** und Message Hash-Algorithmen für IKE Phase 1 auswählen. Die Kombination von sechs Verschlüsselungsalgorithmen und vier Message Hash-Algorithmen ergibt 24 mögliche Werte in diesem Feld.

In den folgenden beiden Tabellen sind die verfügbaren Verschlüsselungs- und Message Hash-Algorithmen aufgelistet:

Algorithmus	Beschreibung
Blowfish	➤➤ **Blowfish** ist ein sehr sicherer und zugleich schneller Algorithmus. Twofish kann als Nachfolger von Blowfish angesehen werden.

Algorithmus	Beschreibung
3DES	➤➤ **3DES** ist eine Erweiterung des DES Algorithmus mit einer effektiven Schlüssellänge von 112 Bit, was als sicher eingestuft wird. Es ist der langsamste Algorithmus, der derzeit unterstützt wird.
DES	➤➤ **DES** ist ein älterer Verschlüsselungsalgorithmus, der aufgrund seiner kleinen effektiven Länge von 56 Bit als schwach eingestuft wird.
CAST	➤➤ **CAST** ist ebenfalls ein sehr sicherer Algorithmus, etwas langsamer als Blowfish, aber schneller als 3DES.
Twofish	➤➤ **Twofish** war ein finaler Kandidat für den AES (Advanced Encryption Standard). Er wird als genauso sicher eingestuft wie Rijndael (AES), ist aber langsamer.
Rijndael	Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt.

Tabelle 5-2: Verschlüsselungsalgorithmen

Im folgenden sind die verfügbaren ➤➤ **Hash**-Algorithmen aufgeführt:

Algorithmus	Beschreibung
MD5 (Message Digest #5)	➤➤ **MD5** ist ein älterer Hash Algorithmus. Wird mit 96 Bit Digest Length für IPSec verwendet.
SHA1 (Secure Hash Algorithm #1)	➤➤ **SHA1** ist ein Hash Algorithmus, der von der NSA (United States National Security Association) entwickelt wurde. Er wird als sicher eingestuft, ist aber langsamer als MD5. Wird mit 96 Bit Digest Length für IPSec verwendet.

Algorithmus	Beschreibung
RipeMD 160	➤➤ **RipeMD 160** ist ein kryptographischer 160 Bit Hash-Algorithmus. Er wird als sicherer Ersatz für MD5 und RipeMD angewandt.
Tiger 192	➤➤ **Tiger 192** ist ein relativ neuer und sehr schneller Algorithmus.

Tabelle 5-3: Message Hash-Algorithmen

Hinweis

Beachten Sie, dass die Beschreibung der Verschlüsselung und Authentifizierung oder der Hash-Algorithmen auf dem Kenntnissstand und der Meinung des Autors zum Zeitpunkt der Erstellung dieses Handbuchs basiert. Die Qualität der Algorithmen im besonderen unterliegt relativen Gesichtpunkten und kann sich aufgrund von mathematischen oder kryptographischen Weiterentwicklungen ändern.

VIEW PROPOSALS

Im Untermenü ***VIEW PROPOSALS*** erhalten Sie eine Übersicht über die Proposals, die vom IPSec-Wizard erstellt wurden:

```
VPN Access Setup Tool                        Bintec Access Networks GmbH
[IPSEC][IKE PROPOSALS]: IKE Proposal                              MyGateway

    Description        Protocol                      Lifetime
    Blowfish/MD5       default  blowfish md5         900s/0KB (def)   =
    DES3/MD5           default  des3     md5         900s/0KB (def)   |
    CAST/MD5           default  cast12   md5         900s/0KB (def)   |
    DES/MD5            default  des      md5         900s/0KB (def)   |
    Blowfish/SHA1      default  blowfish sha1        900s/0KB (def)   |
    DES3/SHA1          default  des3     sha1        900s/0KB (def)   |
    CAST/SHA1          default  cast128  sha1        900s/0KB (def)   |
    DES/SHA1           default  des      sha1        900s/0KB (def)   |
    DES/Tiger192       default  des      tiger192    900s/0KB (def)   |
    DES/Ripemd160      default  des      ripemd160   900s/0KB (def)   |
    DES3/Tiger192      default  des3     tiger192    900s/0KB (def)   |
    DES3/Ripemd160     default  des3     ripemd160   900s/0KB (def)   |
    Blowfish/Tiger192  default  blowfish tiger192    900s/0KB (def)   |
    Blowfish/Ripemd160 default  blowfish ripemd160   900s/0KB (def)   v

    DELETE             EXIT
```

Dieses Menü dient lediglich der Information. Eine Konfiguration ist nicht möglich.

Phase 1: Lifetime

Dieses Feld zeigt die Lebensdauer (Lifetime) an, die ablaufen darf, bevor Phase-1-Schlüssel durch eine weitere Diffie-Hellman-Schlüsselberechnung erneuert werden müssen. Sie kann entweder als Wert in Sekunden, als verarbeitete Datenmenge (in Kb) oder als Kombination aus beiden konfiguriert werden. Der Defaultwert beträgt *900 sec/11000 Kb,* das bedeutet, dass die Schlüssel erneuert werden, wenn entweder 900 Sekunden abgelaufen sind oder 11000 Kb Daten verarbeitet wurden, je nachdem, welches Ereignis zuerst eintritt. Falls Sie zusätzliche Lebensdauerwerte konfiguriert haben, können Sie unter diesen hier auswählen.

Falls Sie sich entschließen, zusätzliche Lebensdauerwerte zu konfigurieren, können Sie dies im Menü ***EDIT LIFETIMES*** durchführen. Die Menümaske sieht folgendermaßen aus:

```
VPN Access Setup Tool                    Bintec Access Networks GmbH
[IPSEC][LIFETIME]: IPsec Configuration - Life Times          MyGateway


     Edit Lifetime Values


          Lifetime Restriction Based On: Time and Traffic

               900         Seconds

               11000       Kb

          Matching Policy:              Loose


                    SAVE                                  Exit
```

Das Menü umfasst folgende Felder:

Feld	Wert
Lifetime Restriction Based On	Wählen Sie das Kriterium für das Ende der Schlüssellebensdauer, mögliche Werte sind: ■ *Time* and *Traffic* ■ *Time* ■ *Traffic* Abhängig von Ihrer Wahl wird Ihnen eines der folgenden Felder oder beide angezeigt.
Seconds	Geben Sie die Lebensdauer für Phase-1-Schlüssel in Sekunden ein. Der Wert darf jeder ganzzahlige Wert bis zu einer Länge von 32 Bit sein.
Kb	Geben Sie die Lebensdauer für Phase-1-Schlüssel als Menge der verarbeiteten Daten in Kb ein. Der Wert darf jeder ganzzahlige Wert bis zu einer Länge von 32 Bit sein.

Feld	Wert
Matching Policy	Hier können Sie auswählen, wie strikt das Gateway die konfigurierte Lifetime einhält. Zur Verfügung stehen: ■ *loose* - Das Gateway akzeptiert und übernimmt jede Lifetime, die bei der Aushandlung vorgschlagen wird (Defaultwert). ■ *strict* - Das Gateway akzeptiert und verwendet nur die konfigurierte Lifetime. Bei Abweichung scheitert die Phase-1-Aushandlung. ■ *notify* - Das Gateway akzeptiert alle vorgschlagenen Werte, die größer sind, als der konfigurierte, verwendet selbst aber den eigenen, kleineren Wert und informiert den Peer darüber.

TABELLE 5-4: LIFETIME

Phase 1: Group

Die Gruppe (Group) definiert den Parametersatz, der für die Diffie-Hellman-Schlüsselberechnung während der Phase 1 zugrunde gelegt wird. "MODP", wie es von Bintec-Gateways unterstützt wird, steht für "modular exponentiation". Es können drei verschiedene Vorgaben ausgewählt werden, wobei 768, 1024 oder 1536 Bit genutzt werden.

Das Feld kann folgende Werte annehmen:

Wert	Bedeutung
1 (768 bit MODP)	Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 768 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.

Wert	Bedeutung
2 (1024 bit MODP)	Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1024 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.
5 (1536 bit MODP)	Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1536 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.
none	Das Gateway verwendet nach dem Ablauf der Lifetime keine bestimmte Exponentiation, sondern verfährt wie beim initialen Tunnelaufbau.
default	Das Gateway verwendet die Einstellung des vom IPSecWizard erstellten Profils.

Tabelle 5-5: ***PHASE 1: GROUP***

Phase 1: Authentication Method

Dieses Feld ermöglicht Ihnen, die Authentisierungs-Methode für das globale Profil zu ändern:

Wert	Bedeutung
Pre Shared Keys	Falls Sie für die Authentifizierung keine Zertifikate verwenden, können Sie *Pre Shared Keys* wählen. Diese werden bei der Peerkonfiguration im Menü ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***APPEND/EDIT*** konfiguriert.
DSA Signatures	Phase-1-Schlüsselberechnungen werden unter Nutzung des ➤➤ **DSA**-Algorithmus authentifiziert.
RSA Signatures	Phase-1-Schlüsselberechnungen werden unter Nutzung des ➤➤ **RSA**-Algorithmus authentifiziert.

Wert	Bedeutung
RSA Encryption	Mit RSA-Verschlüsselung werden als erweiterte Sicherheit zusätzlich die ID-Nutzdaten verschlüsselt.
default	Das Gateway verwendet die Einstellung des vom IPSecWizard erstellten Profils.

Tabelle 5-6: ***AUTHENTICATION METHOD***

Phase 1: Mode

Das Mode-Feld zeigt den momentan konfigurierten Phase-1-Modus an und ermöglicht Ihnen, die Einstellungen zu verändern:

Wert	Bedeutung
id_protect	Dieser Modus (auch als Main Mode bezeichnet) erfordert sechs Meldungen für eine Diffie-Hellman-Schlüsselberechnung und damit für die Einrichtung eines sicheren Kanals, über den die IPSec SAs ausgehandelt werden. Er setzt voraus, dass beide Peers statische IP-Adressen haben, falls für die Authentifizierung Preshared Keys genutzt werden. Bei der Verwendung des IPSec-Callbacks entfällt diese Einschränkung. Siehe "Untermenü IPSEC CALLBACK" auf Seite 14.
aggressive	Der Aggressive Mode ist erforderlich, falls einer der Peers keine statische IP-Adresse hat und Preshared Keys für die Authentifizierung genutzt werden; er erfordert nur drei Meldungen für die Einrichtung eines sicheren Kanals.
default	Das Gateway verwendet die Einstellung des vom IPSecWizard erstellten Profils.

Wert	Bedeutung
id-protect-only	Das Gateway akzeptiert bei der Aushandlung ausschließlich den ID Protect Mode. Schlägt der Peer einen anderen Modus vor, scheitert die Aushandlung.
aggressive-only	Das Gateway akzeptiert bei der Aushandlung ausschließlich den Aggressive Mode. Schlägt der Peer einen anderen Modus vor, scheitert die Aushandlung.

TABELLE 5-7: MODE

Phase 1: Local ID

Das ist die ID, die Sie Ihrem Gateway zuweisen. Falls Sie dieses Feld leer lassen, wählt das Gateway die Defaultwerte. Diese sind:

- Bei Authentifizierung mit Preshared Keys: die lokale IP-Adresse wie im *IPSECPEERLOCALADDRESS*-Feld in der *IPSECPEERTABLE* angegeben.
- Bei Authentifizierung mit ➤➤ **Zertifikat**: der erste im Zertifikat angegebene Subjekt-Alternativname oder, falls keiner angegeben ist, der Subjektname des Zertifikats.

Hinweis

Falls Sie Zertifikate für die Authentifizierung nutzen und Ihr Zertifikat Subjekt-Alternativnamen enthält (siehe "Zertifikatanforderung" auf Seite 73), müssen Sie hier achtgeben, da das Gateway per Default den ersten Subjekt-Alternativnamen wählt. Stellen Sie sicher, dass Sie und Ihr Peer beide den gleichen Namen nutzen, d.h. dass Ihre lokale ID und die Peer-ID, die Ihr Partner für Sie konfiguriert, identisch sind.

Phase 1: Local Certificate

Dieses Feld ermöglicht Ihnen, eines Ihrer eigenen Zertifikate für die Authentifizierung zu wählen. Es zeigt die Indexnummer dieses Zertifikats und den Namen an, unter dem es gespeichert ist. Dieses Feld wird nur bei Authentifizierungeinstellungen auf Zertifikatbasis angezeigt und weist darauf hin, dass ein Zertifikat zwingend erforderlich ist.

CA Certificates

Hier können Sie eine Liste zusätzlicher ➤➤ **CA**-Zertifikate eingeben, die für dieses Profil akzeptiert werden sollen. Einträge werden mit Kommata getrennt. Dadurch wird es z. B. möglich, auch für selbstsignierte Zertifikate ein CA-Zertifikat zu übermitteln.

Falls das CA-Zertifikat keine Zertifikat-Rückrufliste (Certificate Revocation List, CRL) oder keine CRL-Verteilstelle enthält und auf dem Gateway kein Zertifikatserver konfiguriert ist, wird die Variable ***NoCRLs*** auf "True" gesetzt. Zertifikate von dieser CA werden nicht auf ihre Gültigkeit überprüft.

6 Untermenü *IPSec (Phase 2) Defaults*

Im folgenden wird das Untermenü *IKPSec (Phase 2) Defaults* beschrieben.

Ebenso wie für die Phase 1 können Sie Profile für die Phase 2 des Tunnelaufbaus definieren.

Die Konfiguration erfolgt im Menü ***IPSec*** ➜ ***IPSec (Phase 2) Defaults: edit*** ➜ ***ADD/EDIT***:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[IPSEC][PHASE2][ADD]: IPsec Configuration - Phase 2 Profiles MyGateway

   Description (Idx 0) :

   Proposal              :  default
   Lifetime              :  use default
   Use PFS               :  default
   Heartbeats            :  default
   Propagate PMTU        :  default


   View Proposals >
   Edit Lifetimes >


                         SAVE                              CANCEL
```

Das Menü enthält die folgenden Felder:

Feld	Wert
Proposal	Informationen zu diesen Parametern finden Sie bei “Proposal, Lifetime, Use PFS...” auf Seite 65
Lifetime	
Use PFS	

Feld	Wert
Heartbeats	Hier wählen Sie, ob und in welcher Weise IPSec Heartbeats verwendet werden. Um feststellen zu können, ob eine Security Association (SA) noch gültig ist oder nicht, hat Bintec einen IPSec-Heartbeat implementiert. Dieser sendet bzw. empfängt je nach Konfiguration Signale, bei deren Ausbleiben die SA als ungültig verworfen wird. Zur Verfügung stehen: ■ *default* - Das Gateway verwendet die Einstellung des Default-Profils. ■ *none* - Das Gateway sendet und erwartet keinen Heartbeat. ■ *expect* - Das Gateway erwartet einen Heartbeat vom Peer, sendet selbst aber keinen. ■ *send* - Das Gateway erwartet keinen Heartbeat vom Peer, sendet aber einen. ■ *both* - Das Gateway erwartet einen Heartbeat vom Peer und sendet selbst einen. Für Geräte der **VPN Access Linie** werden Heartbeats für Phase 1 und Phase 2 getrennt konfiguriert. Wenn Interoperabilität mit älterer Software zu gewährleisten ist, müssen für Phase 1 und Phase 2 die gleichen Werte konfiguriert werden.

Feld	Wert
Propagate PMTU	Hier wählen Sie aus, ob während der Phase 2 die PMTU (Path Maximum Transfer Unit) propagiert werden soll oder nicht. Zur Verfügung stehen: ■ *default* - Das Gateway verwendet die Einstellung des Default-Profils. ■ *no* - Die Path Maximum Transfer Unit wird nicht übermittelt (Defaultwert). ■ *yes* - Die Path Maximum Transfer Unit wird übermittelt.

Tabelle 6-1: ***IPSec ➜ IPSec (Phase 2) Profile: edit ➜ ADD/EDIT***

Das Menü ***View Proposals*** dient wie bei den Phase-1-Proposals lediglich der Auflistung der zur Verfügung stehenden Proposals. Das Menü ***Edit Lifetimes*** unterscheiden sich nicht von dem in "Phase 1: Lifetime" auf Seite 56 beschriebenen.

6.1 Proposal, Lifetime, Use PFS...

Die im Folgenden beschriebenen Felder des Menüs *IPSec (Phase 2) Profile: edit ➜ ADD/EDIT* bedürfen näherer Erläuterung.

Phase 2: Proposal

Dieses Feld ermöglicht Ihnen, jede Kombination aus IPSec-Protokoll, ➤➤ **Verschlüsselungsalgorithmus** und/oder Message-Hash-Algorithmus zu wählen. In den folgenden Tabellen sind die Elemente dieser potentiellen Kombinationen aufgeführt:

IPSec-Protokoll	Beschreibung
ESP (Encapsulated Security Payload)	➤➤ **ESP** bietet Nutzdatenverschlüsselung sowie Authentifizierung.

IPSec-Protokoll	Beschreibung
AH (Authentication Header)	➤➤ **AH** bietet nur Authentifizierung, aber keine Nutzdatenverschlüsselung. Falls Sie eine Kombination wählen, bei der das AH-Protokoll benutzt wird, wird als Verschlüsselungsalgorithmus *none* angezeigt, z.B. *(AH (none, MD5))*.

Tabelle 6-2: IPSec-Protokolle

Zusätzlich zur Verschlüsselung und Authentifizierung unterstützt Bintec's IPSec-Implementierung die ➤➤ **Kompression** von IP-Nutzdaten durch ➤➤ **IPComP** (IP Payload Compression Protocol). IP-Nutzdatenkompression ist ein Protokoll zur Verkleinerung von IP-Datagrammen. Dieses Protokoll vergrößert die Gesamt-Kommunikationsperformance zwischen einem Paar miteinander kommunizierender Hosts/Gateways ("Knoten"). Es komprimiert die Datagramme, vorausgesetzt, die Knoten verfügen über ausreichende Rechenleistung, entweder durch die Leistung der CPU oder durch einen Kompressions-Koprozessor, und die Kommunikation erfolgt über langsame oder gestörte Verbindungen.

Die IP-Nutzdatenkompression ist besonders nützlich, wenn IP-Datagramme verschlüsselt werden. Die Verschlüsselung von IP-Datagrammen sorgt dafür, dass die Daten eine Zufallsnatur erhalten, wodurch eine Kompression auf niedrigeren Protokollebenen (z. B. PPP Compression Control Protocol [RFC1962]) unwirksam ist. Falls sowohl Kompression als auch ➤➤ **Verschlüsselung** gefordert sind, muss die Kompression vor der Verschlüsselung durchgeführt werden.

Bei allen IPSec-Proposals, bei denen keine bestimmte Einstellung für IPComP festgelegt ist, ist IPComP freigegeben. Das bedeutet, dass das Gateway während der SA-Aushandlung alle Proposals akzeptiert, unabhängig davon, ob diese die Nutzung von IPComP vorschlagen oder nicht. Falls der lokale Rechner die Aushandlung initiiert, schlägt er die Nutzung von IPComP als Vorzugs-Proposal vor, erlaubt jedoch dem antwortenden Rechner, einen Proposal ohne IPComP zu wählen.

Sie können dieses Verhalten ändern, indem Sie ein IPSec Proposal wählen, der eine der folgenden Einstellungen für ➤➤ **IPComP** festlegt:

IPComP-Option	Beschreibung
no Comp	Ihr Gateway akzeptiert keine SAs, die die Nutzung von IPComP festlegen. Falls der Peer so konfiguriert wurde, dass sein oder ihr Gateway IPComP vorschlägt, dann schlägt die IPSec SA-Aushandlung fehl und es wird keine Verbindung hergestellt.
force Comp	Ihr Gateway fordert, dass bei der IPSec SA-Aushandlung IPComP vereinbart werden kann. Falls der Peer dies nicht akzeptiert, wird keine Verbindung hergestellt.

Tabelle 6-3: IPComP-Optionen bei IPSec-Proposals

Da die wichtigsten Verschlüsselungs- und Hash-Algorithmen bereits beschrieben wurden, werden sie hier nur noch aufgelistet. Nur der NULL-Algorithmus steht in Phase 1 nicht zur Verfügung:

Algorithmen	Beschreibung
Blowfish	Beschreibungen der Verschlüsselungsalgorithmen finden Sie in der Tabelle “Verschlüsselungsalgorithmen” auf Seite 54.
3DES	
DES	
CAST	
Twofish	
Rijndael	
NULL	Der NULL-"Algorithmus" nimmt keine Verschlüsselung der IP-Pakete vor, ist jedoch notwendig, falls IP-Pakete eine Authentifizierung durch das ESP-Protokoll ohne Verschlüsselung benötigen.

Tabelle 6-4: Phase-2-Verschlüsselungsalgorithmen

Dies sind die verfügbaren Hash-Algorithmen:

Algorithmen	Beschreibung
MD5	Beschreibungen der Message-Hash-Algorithmen finden Sie in der Tabelle “Message Hash-Algorithmen” auf Seite 55.
SHA1	
NULL	Falls der NULL-"Algorithmus" für die Authentifizierung angewandt wird, wird unter ESP kein Message Hash erzeugt und die Nutzdaten werden nur verschlüsselt.

Tabelle 6-5: Message-Hash-Algorithmen in Phase 2

Hinweis

Beachten Sie, dass der NULL-Algorithmus in einem einzelnen Proposal entweder nur für die Verschlüsselung oder nur für die Authentifizierung festgelegt werden kann, aber nicht für beides.

Beachten Sie, dass RipeMD 160 und Tiger 192 für Message Hashing in Phase 2 nicht zur Verfügung stehen.

Ein Phase-2-Proposal würde somit beispielsweise folgendermaßen aussehen:

Beispielwerte	Bedeutung
1 (ESP(Blowfish, MD5))	IP-Pakete werden unter Anwendung des ESP-Protokolls, der Blowfish-Verschlüsselung und des MD5 Message Hash verarbeitet.
10 (ESP(NULL, SHA1))	IP-Pakete werden unter Anwendung des ESP-Protokolls verarbeitet; die NULL-Verschlüsselung und SHA 1 werden zur Erzeugung des Message Hash genutzt.
16 (AH(none, MD5))	IP-Pakete werden unter Anwendung des AH-Protokolls, ohne Verschlüsselung und mit MD5 als Message Hash-Algorithmus verarbeitet.

Tabelle 6-6: Beispiele für ***Phase 2: proposals***

Phase 2: Lifetime

Informationen über die Lebensdauer des Proposals finden Sie unter “Phase 1: Lifetime” auf Seite 56. Falls Sie eine bestimmte IPSec-SA-Lebensdauer für diesen Peer festlegen möchten, können Sie dies im Menü ***EDIT LIFETIME*** vornehmen.

Use PFS

Da PFS (Perfect Forward Secrecy) eine weitere Diffie-Hellman-Schlüsselberechnung erfordert, um neues Verschlüsselungsmaterial zu erzeugen, müssen Sie die Exponentiations-Merkmale wählen. Wenn Sie PFS aktivieren, sind die Optionen die gleichen, wie bei der Konfiguration in ***PHASE 1: GROUP*** (“Phase 1: Group” auf Seite 58). PFS wird genutzt, um die Schlüssel einer umgeschlüsselten Phase-2-SA zu schützen, auch wenn die Schlüssel der Phase-1-SA bekannt geworden sind.

7 Untermenü *CERTIFICATE AND KEY MANAGEMENT*

Im folgenden wird das Untermenü ***CERTIFICATE AND KEY MANAGEMENT*** beschrieben.

Im Menü ***CERTIFICATE AND KEY MANAGEMENT*** gelangt man in folgende Untermenüs:

- ***KEY MANAGEMENT***
- ***OWN CERTIFICATES***
- ***CERTIFICATE AUTHORITY CERTIFICATES***
- ***PEER CERTIFICATES***
- ***CERTIFICATE REVOCATION LISTS***
- ***CERTIFICATE SERVERS***

7.1 Untermenü *KEY MANAGEMENT*

Das erste Menüfenster von ***CERTIFICATE AND KEY MANAGEMENT*** ➜ ***KEY MANAGEMENT*** zeigt Informationen über die auf Ihrem Gateway gespeicherten Schlüssel an:

```
VPN Access Setup Tool                        Bintec Access Networks GmbH
[IPSEC][CERTMGMT][KEYS]: IPSec Configuration -
                         Configure Keys                          MyGateway

Highlight an entry and type 'e' to generate a pkcs#10 certificate
request

  Description                                    Algorithm    Key Length
  automatic key RSA 1024 (e 65537)                rsa         001024


     CREATE              DELETE        REQUEST CERT        EXIT
```

Diese Liste enthält eine Beschreibung des/der Schlüssel(s), und informiert Sie über den benutzten Algorithmus und die Schlüssellänge. Darüber hinaus können Sie neue Schlüssel erzeugen oder Zertifikate für existierende Schlüssel anfordern.

7.1.1 Schlüsselerzeugung

Wenn Sie einen neuen Schlüssel erzeugen möchten, können Sie dies im Menü ***CERTIFICATE AND KEY MANAGEMENT*** ➜ ***KEY MANAGEMENT*** ➜ ***CREATE*** vornehmen

```
VPN Access Setup Tool                        Bintec Access Networks GmbH
[IPSEC][CERTMGMT][KEYS][CREATE]: IPSec Configuration -
                                   Create Keys                MyGateway

     Description:
     Algorithm:              rsa
     Key Size (Bits):        1024
     RSA Public Exponent:    65537




                Create                                  Exit
```

Das Menü ermöglicht Ihnen, folgende Parameter zu konfigurieren:

Feld	Wert
Description	Hier können Sie einen beliebigen Namen für den Schlüssel eingeben, den Sie gerade erzeugen.
Algorithm	Hier können Sie einen der verfügbaren Algorithmen auswählen. Zur Verfügung stehen ➤➤ **RSA** und ➤➤**DSA**.

Feld	Wert
Key Size (Bits)	Hier können Sie die Länge des zu erzeugenden Schlüssels auswählen. Der verfügbare Wertebereich geht von *512* bis *4096* Bit. Beachten Sie, dass ein Schlüssel mit der Länge *512* Bit als unsicher eingestuft werden könnte, während ein Schlüssel mit *4096* Bit nicht nur viel Zeit zur Erzeugung erfordert, sondern während der IPSec-Verarbeitung einen wesentlichen Teil der Ressourcen belegt. Ein Wert von *768* oder mehr wird jedoch empfohlen, als Defaultwert ist *1024 Bit vorgegeben*.
RSA Public Exponent	(Dieses Feld wird nur dann angezeigt, wenn Sie den RSA-Algorithmus benutzen.) Der Public Exponent ist Teil des Public Key (öffentlicher Schlüssel), der für RSA-Signaturen und RSA-Verschlüsselung erzeugt wurde. Falls Sie von Ihrer Zertifizierungsstelle (CA) keine besondere Empfehlung erhalten, können Sie den Defaultwert unverändert übernehmen.

Tabelle 7-1: ***IPSEC → CERTIFICATE AND KEY MANAGEMENT → KEY MANAGEMENT → CREATE***

7.1.2 Zertifikatanforderung

Nachdem Sie einen Schlüssel erzeugt haben, können Sie für diesen Schlüssel ein Zertifikat anfordern, indem Sie den entsprechenden Schlüssel hervorheben und dann die "e"-Taste auf Ihrer Tastatur drücken. Alternativ können Sie ***REQUEST CERT*** aufrufen und den Schlüssel, den Sie zertifiziert haben möchten, im Menü ***CERTIFICATE AND KEY MANAGEMENT → KEY MANAGEMENT → REQUEST CERT*** auswählen**.**

Falls Sie ein Zertifikat anfordern möchten, öffnet sich folgendes Untermenü:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[IPSEC][CERTMGMT]..[ENROLL]: IPSec Configuration -
                             Certificate Enrollment          MyGateway

  Key to enroll:              1 ()

  Method:       SCEP          CA-Certificate: (download)
  Autosave:     on            CA-Domain:
  Password:
  Subject Name:

  Subject Alternative Names (optional):
    Type   Value
    IP     172.16.98.181
    DNS    x2200
    NONE

  State of Last Enrollment:   none
  Server:
  Certname:

             Start                                Exit
```

Dieses Menü enthält folgende Felder:

Feld	Wert
Key to enroll	Wählen Sie den Schlüssel, den Sie zertifiziert haben möchten.

Feld	Wert
Method	Hier wählen Sie aus, auf welche Art Sie das Zertifikat beantragen wollen. Zur Verfügung stehen: ■ *SCEP* - Der Schlüssel wird mittels des Simple Certificate Enrollment Protocols bei einer CA beantragt. ■ *Upload* - Das Gateway erzeugt für den Schlüssel eine PKCS#10-Anfrage, die an einen Server der CA gesendet wird. das Zertifikat muss nach der Ausstellung noch in das Gateway importiert werden. ■ *Show* - Das Gateway erzeugt eine PKCS#10-Anfrage und zeigt das Ergebnis in einem Menüfenster an.
CA-Certificate	Nur für ***METHOD*** = *SCEP*. Wählen Sie das CA-Zertifikat der Zertifizierungsstelle (CA), von der Sie das Zertifikat anfordern möchten. Falls keine CA-Zertifikate zur Verfügung stehen, wird das Gateway zuerst das CA-Zertifikat der fraglichen CA herunterladen. Er fährt dann mit dem Registrierungsprozess fort, sofern keine wesentlichen Parameter mehr fehlen. In diesem Fall kehrt es in das Menü ***REQUEST CERT*** zurück. Falls das CA-Zertifikat keine Zertifikat-Rückrufliste (Certificate Revocation List, CRL) oder eine CRL-Verteilstelle enthält und auf dem Gateway kein Zertifikatserver konfiguriert ist, wird die Variable ***NoCRLs*** auf "True" gesetzt. Zertifikate von diesem CA werden nicht auf ihre Gültigkeit überprüft.

Feld	Wert
Autosave	Nur für ***METHOD*** = *SCEP*. Falls Sie diese Option aktivieren, speichert das Gateway automatisch die verschiedenen Schritte des Registrierungsprozesses. Dies ist dann von Nutzen, wenn die Registrierung nicht sofort abgeschlossen werden kann oder wenn das Gateway neu gebootet werden muss. Falls der Status nicht gespeichert wurde, kann die Registrierung nicht abgeschlossen werden. Sobald die Registrierung abgeschlossen ist und das Zertifikat vom CA-Server heruntergeladen wurde, wird es automatisch in der Konfiguration des Gateways gespeichert. Als Wahlmöglichkeiten gibt es *on* und *off*.
CA-Domain	Nur für ***METHOD*** = *SCEP*. Geben Sie den ➤➤ **Domain**namen des CA-Servers ein, an den die Registrierung gesandt wird, z.B. **enroll.ca.com**.
Password	Nur für ***METHOD*** = *SCEP*. Um Zertifikate für Ihre Schlüssel zu erhalten, benötigen Sie möglicherweise ein Passwort von der Zertifizierungsstelle. Tragen Sie das Passwort, welches Sie von Ihrer Zertifizierungsstelle erhalten haben, hier ein.
Subject Name	Geben Sie einen Subjektnamen für das Zertifikat, welches Sie anfordern, ein. Der Name, den Sie hier eingeben, muss der Syntax für subjektunterschiedene Namen gemäß X.509 entsprechen.

Feld	Wert
Subject Alternative Names (optional)	Hier können Sie zusätzliche Informationen eingeben, die als Subjektname benutzt werden können. Eine Liste der Optionen finden Sie in der Tabelle “Subjekt-Alternativnamen” auf Seite 78 unten.
State of Last Enrollment	Nur für ***METHOD*** = *SCEP*. Hier wird das Ergebnis des letzten Zertifikat-Antrags an die CA angezeigt. Das Feld kann nicht editiert werden.
Signing algorithm to use	Nur für ***METHOD*** = *Upload*. Hier wählen Sie aus, mit welchem Algorithmus die Zertifikat-Anfrage authentifiziert werden soll. Zur Verfügung stehen: ■ *md5WithRSAEncryption* ■ *sha1WithRSAEncryption*.
Server	Nicht für ***METHOD*** = *Show*. Hier tragen Sie den ➤➤ **TFTP**-Server ein, an den die Zertifikatanforderung gesandt wird. Sie können entweder einen auflösbaren Host-Namen oder eine IP-Adresse eingeben. Beachten Sie bitte, dass Sie vor der Serveradresse kein Protokoll (wie TFTP oder HTTP) eingeben dürfen.
Certname/Filename	Nicht für ***METHOD*** = *Show*. Geben Sie für das resultierende Zertifikat einen Namen ein. Für ***METHOD*** = *Upload* können Sie auswählen, ob die Anfrage im Format *base64* oder *binary* gesendet werden soll.

Tabelle 7-2: ***IPSEC ➜ CERT. AND KEY MNGMNT. ➜ KEY MNGMNT. ➜ REQUEST CERT***

Unten finden Sie die Auswahloptionen für das Feld ***SUBJECT ALTERNATIVE NAMES***. Im Feld ***SUBJECT ALTERNATIVE NAMES – TYPE*** können Sie aus verschiedenen Informationstypen auswählen, die als Subjekt-Alternativname benutzt werden können. Im Feld ***SUBJECT ALTERNATIVE NAMES – VALUE*** können Sie die spezifischen Informationen eintragen, die Sie liefern möchten. Hier stehen drei Instanzen zur Verfügung, die Defaulteinstellungen für die ersten beiden Instanzen sind die erste IP-Adresse Ihres Gateways und dessen ➤➤ **DNS**-Name.

Die Optionen für ***TYPE*** sind:

Wert	Bedeutung
IP	Die ➤➤ **IP**-Adresse Ihres Gateways wird als ein Subjekt-Alternativname benutzt.
DNS	Ein DNS-Name wird als Subjekt-Alternativname benutzt (z.B.: MyGateway).
Email	Eine E-Mail-Adresse wird als Subjekt-Alternativname benutzt.
URI	Ein Uniform Resource Identifier wird als Subjekt-Alternativname benutzt. URI ist die Adressierungstechnik, aus der die URLs abgeleitet werden. Technisch betrachtet sind URLs wie beispielsweise HTTP:// und FTP:// spezifische Unterkennungen von URIs.
DN	Ein DN (Distinguished Name) wird als Subjekt-Alternativname benutzt.
RID	Eine RID (Registered Identity) wird als Subjekt-Alternativname benutzt.

Tabelle 7-3: **Subjekt-Alternativnamen**

7.2 Zertifikat-Untermenüs

In den Zertifikat-Untermenüs ***OWN CERTIFICATES***, ***CERTIFICATE AUTHORITY CERTIFICATES*** und ***PEER CERTIFICATES*** können Sie die Zertifikate managen, die

Sie für Authentifizierungsmethoden benötigen, die auf ➤➤ **Zertifikaten** aufbauen (z. B. DSA-, RSA- und RSA-Verschlüsselung).

Hinweis

Im allgemeinen müssen Sie ein Peer-Zertifikat nur in seltenen Fällen herunterladen:

- Falls Sie die RSA-Verschlüsselung als Authentifizierungsmethode konfiguriert haben, aber weder einen CRL-Server angegeben, noch eine CRL statisch auf Ihrem Gateway gespeichert haben.
  Beachten Sie, dass es eine wesentliche Sicherheitslücke darstellt, wenn Sie keinen Zertifikatserver angeben und über keine statisch konfigurierten CRLs verfügen, da in diesem Fall Zertifikate, die gesperrt wurden, nicht automatisch erkannt werden können.
- Falls Sie das Peer-Zertifikat nicht während der IKE-Aushandlung empfangen. Dies ist dann der Fall, wenn beim Peer das Absenden von Zertifikaten gesperrt ist oder vom lokalen Rechner keine "Get Certificate Requests" (Zertifikatanforderungen) ausgesandt werden. Beide Optionen können im Menü ***IPSec*** ➜ ***Advanced Settings*** eingestellt werden, indem entweder ***Ignore Cert Request Payloads*** oder ***Do not send Cert Request Payloads*** auf *yes* gesetzt werden.

Das erste Menüfenster aller Zertifikat-Untermenüs sieht fast identisch aus:

```
VPN Access Setup Tool                        Bintec Access Networks GmbH
[IPSEC][CERTMGMT][OWN]: IPSec Configuration -
                        Certificate Management                MyGateway

Flags:  'O'= own cert, 'CA'= CA cert, 'N'= no CRLs, 'T'= cert forced
trusted

  Description     Flags   SerialNo       Subject Names
  own.cer         O       1013591521 ,   CN=myro



     DOWNLOAD             DELETE               EXIT
```

Das Menü zeigt die ***Description*** (Beschreibung), alle möglicherweise gesetzten ***Flags***, die ***Serial No*** (Seriennummer) des fraglichen Zertifikats und die Daten zu den ***Subject Names*** an.

Wenn Sie einen Eintrag hervorheben und mit ***ENTER*** bestätigen, können Sie ein Fenster aufrufen, welches das Zertifikat anzeigt und zusätzliche Informationen darüber liefert:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH

Change Certificate Attributes
 Description:   own.cer
 Type of certificate: Own Certificate      Uses Key: automatic key RSA

Certificate Contents:
 Certificate =                                                          =
   SerialNumber = 1013591521                                            |
   SubjectName = <CN=mafr>                                              |
   IssuerName = <CN=Test CA 1, OU=Web test, O=SSH Communications        |
     Security, C=FI>                                                    |
   Validity =                                                           |
     NotBefore = 2002 Feb 13th, 00:00:00 GMT                            |
     NotAfter  = 2002 Apr  1st, 00:00:00 GMT                            |
   PublicKeyInfo =                                                      v

                    SAVE                                  Exit
```

Sie können zwar den Inhalt des Zertifikats nicht verändern, jedoch an folgenden Daten Änderungen vornehmen:

Feld	Wert
Description	Hier wird die Beschreibung angezeigt, die Sie beim Import des Zertifikats eingegeben haben. Jetzt können Sie diese ändern.
Type of Certificate	Hier können Sie zwischen drei Arten von Zertifikaten auswählen: ■ *Own Certificate (eigenes Zertifikat)* ■ *Certificate Authority (Zertifizierungsstelle)* ■ *Peer Certificate (Peer-Zertifikat)* Falls Sie hier *Certificate Authority* wählen, müssen Sie zusätzlich angeben, ob die Zertifizierungsstelle Zertifikat-Rückruflisten (CRLs) ausgibt oder nicht.

Tabelle 7-4: ***IPSecFlags ➜ Certificate and Key Management ➜ Own Certificates ➜ EDIT***

7.2.1 Zertifikatimport

Ein weiteres Untermenü, in das Sie vom ersten Zertifikatmenü aus gelangen können (***Certificate and Key Management ➜ Own***, ***CA*** oder ***Peer Certificates***), ist das ***DOWNLOAD-***Menü, über das Sie entweder ein Zertifikat von einem ➤➤ **TFTP**-Server herunterladen oder durch direktes Einfügen des Zertifikatinhalts in das Setup-Tool importieren können.

Es sieht folgendermaßen aus:

```
VPN Access Setup Tool                        Bintec Access Networks GmbH
[IPSEC][CERTMGMT][GETCERT]: IPSec Configuration -
                            Get Certificate                   MyGateway

    Import a Certificate/CRL using:  TFTP

      Type of certificate: Own Certificate



     Server:
     Name:                                                  auto

              START                                 EXIT
```

Dieses Menü enthält folgende Felder:

Feld	Wert
Import a Certificate/CRL using:	Geben Sie an, auf welche Weise Sie die Zertifikatdaten eingeben möchten: ■ *TFTP* ■ *Direct Input (direkte Eingabe)*
Type of Certificate	Dieses Feld zeigt einen der folgenden Einträge an: *Certificate Authority, Own Certificate oder Peer Certificate*. Sie können diesen Eintrag nicht ändern.
Please enter certificate data	Hier können Sie den Inhalt des Zertifikats, welches Sie von der Zertifizierungsstelle (CA) empfangen oder von Ihrem Systemadministrator erhalten haben, in die dafür vorgesehene Zeile unterhalb dieses Felds durch Kopieren/Einfügen eintragen. Die Zeile für die Eingabe der Zertifikatdaten steht nur dann zur Verfügung, wenn Sie zuvor *Direct Input* ausgewählt hatten.

Feld	Wert
Server	Geben Sie den TFTP-Server an, von dem das Zertifikat heruntergeladen werden kann. Sie können entweder eine IP-Adresse oder einen auflösbaren Host-Namen eingeben. Diese Eingabeaufforderung erscheint nur dann, wenn Sie zuvor *TFTP* ausgewählt hatten.
Name	Geben Sie den Namen des Zertifikats ein, welches heruntergeladen werden soll (falls Sie *TFTP-D*ownload gewählt haben) oder welches Sie eingetragen haben (falls Sie *Direct Input* gewählt haben). Falls Sie das Zertifikat über TFTP heruntergeladen haben, wird dieser Name auch als Dateiname benutzt.
auto/base64/binary	Wählen Sie die Art der Codierung, so dass das Gateway das Zertifikat decodieren kann. *auto* aktiviert die automatische Codiererkennung. Falls der Zertifikat-Download im *auto*-Modus fehlschlägt, versuchen Sie es mit einer bestimmten Codierung.

Tabelle 7-5: ***IPSEC ➜ CERTIFICATE AND KEY MANAGEMENT ➜ OWN CERTIFICATES ➜ DOWNLOAD***

Darüber hinaus können Sie bei Peer-Zertifikaten die Option ***FORCE TRUSTED*** aktivieren. Wenn ***FORCE TRUSTED*** aktiviert ist, macht Ihr Bintec-Gateway keine Rückfrage bei der Zertifizierungsstelle, ob das Zertifikat gültig ist oder nicht.

7.3 Untermenü *CERTIFICATE REVOCATION LISTS*

Nach Aufruf des Zertifikat-Rückruflisten-Menüs wird Ihnen eine Liste der gespeicherten CRLs (Certificate Revocation Lists) angezeigt. Das erste Menüfenster enthält wichtige Informationen über die CRLs:

- die Beschreibung, die Sie beim Download der CRL eingegeben haben
- den Herausgeber der CRL (normalerweise Ihre Zertifizierungsstelle)
- die Seriennummer der CRL
- die NumC (das ist die Zahl der zurückgerufenen Zertifikate, die in der CRL enthalten sind).

Das Menü sieht folgendermaßen aus:

```
VPN Access Setup Tool                        Bintec Access Networks GmbH
[IPSEC][CERTMGMT][CRLS]: IPSec Configuration
                         - CRL Management                    MyGateway

Description   Issuer                                      SerialNo  NumC
ca1.crl.pem    CN=Test CA 1, OU=Web test, O=SSH Comm. S [none]    0059


DOWNLOAD         DELETE              EXIT
```

Wenn Sie einen Eintrag hervorheben und mit ***ENTER*** bestätigen, können Sie ein Menüfenster aufrufen, welches Einzelheiten über die CRL enthält und Ihnen

ermöglicht, die Beschreibung der fraglichen CRL zu verändern. Es sieht z.B. so aus:

```
VPN Access Setup Tool                        Bintec Access Networks GmbH
[IPSEC][CERTMGMT][CRLS][EDIT]: IPSec Configuration -
                               CRL Management                MyGateway

     Change Certificate Revocation List Attributes
     Description:   ca1.crl.pem

     CRL Contents:
     CRL =                                                              =
       IssuerName = <CN=Test CA 1, OU=Web test, O=SSH Comm              |
         Security, C=FI>                                                |
       ThisUpdate = 2002 Feb 19th, 11:54:01 GMT                         |
       NextUpdate = 2002 Feb 19th, 13:00:00 GMT                         |
       Extensions =                                                     |
          Available = (not available)                                   |
       RevokedCertList =                                                |
         Entry 1                                                        |
          SerialNumber = 1000471081                                     |
         RevocationDate = 2001 Sep 14th, 12:38:01 GMT                   v

              SAVE                                  EXIT
```

Ausgehend vom ersten ***CERTIFICATE REVOCATION LISTS***-Menüfenster können Sie auch das CRL-***DOWNLOAD***-Menü aufrufen. Hier können Sie CRLs entweder über TFTP oder durch direkte Eingabe importieren. Dieser Prozess funktioniert auf gleiche Weise, wie ein Zertifikatimport. Weitere Einzelheiten finden Sie unter "Zertifikatimport" auf Seite 81.

7.3.1 Untermenü *CERTIFICATE SERVERS*

Wenn Sie Zertifikatserver eingegeben haben, werden diese im ersten Menüfenster des ***CERTIFICATE SERVERS***-Menüs aufgeführt.

Folgende Informationen werden angezeigt:

- die Beschreibung, die Sie für einen Zertifikatserver eingegeben haben
- die URL des Servers
- die Präferenz, die dem fraglichen Server zugeteilt wurde.

Wenn Sie entweder einen Eintrag hervorheben und mit ***ENTER*** bestätigen oder die Option ***ADD*** wählen, gelangen Sie in das Menü ***ADD/EDIT***. Hier können Sie entweder einen neuen Zertifikatserver eintragen, oder die Einstellungen von bereits vorhandenen verändern. Neben der Eingabe einer Beschreibung (***DESCRIPTION)*** und der ***URL*** des Servers können Sie dem Server eine Präferenz (***PREFERENCE)*** zuweisen. Das Gateway fragt die Zertifikatserver in der Reihenfolge der ihnen zugewiesenen Präferenzen ab, beginnend mit *0*.

8 Untermenü *ADVANCED SETTINGS*

Im folgenden wird das Untermenü *ADVANCED SETTINGS* beschrieben.

Im Menü ***IPSEC*** ➜ ***ADVANCED SETTINGS*** können Sie bestimmte Funktionen und Merkmale an die besonderen Erfordernisse Ihrer Umgebung anpassen, d.h. größtenteils werden Interoperabilitäts-Flags gesetzt. Die Defaultwerte ermöglichen es, dass Ihr System einwandfrei mit anderen Bintec-Gateways zusammenarbeitet, so dass Sie diese Werte nur ändern müssen, wenn Ihnen bekannt ist, dass Sie besondere Einstellungen benötigen. Dies kann beispielsweise notwendig sein, wenn die entfernte Seite mit älteren IPSec-Implementierungen arbeitet.

Das Menü ***ADVANCED SETTINGS*** sieht folgendermaßen aus:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[IPSEC][ADVANCED]: IPSec Configuration - Advanced Settings   MyGateway


  Ignore Cert Req Payloads :  no
  Dont send Cert Req Payl. :  no
  Dont Send Cert Chains    :  no
  Dont send CRLs           :  yes

  Dont send Key Hash Payl. :  no
  Trust ICMP Messages      :  no
  Dont Send Initial Contact:  no
  Sync SAs With Local Ifc  :  no
  Max. Symmetric Key Length:  1024
  Use Zero Cookies         :  yes
  Cookies Size             :  32
  RADIUS Authentication    :  disabled

               SAVE                              CANCEL

Use <Space> to select
```

Die Felder und ihre Bedeutung sind wie folgt:

Feld	Wert
Ignore Cert Req Payloads	Gibt an, ob ➤➤ **Zertifikat**anforderungen, die während des IKE von der entfernten Seite empfangen wurden, ignoriert werden sollen oder nicht. Mögliche Werte sind *yes* oder *no* (Defaultwert).
Dont send Cert Req Payl.	Gibt an, ob während des IKE Zertifikatanforderungen gesandt werden sollen oder nicht. Mögliche Werte sind *yes* oder *no* (Defaultwert).
Dont Send Cert Chains	Gibt an, ob während des IKE komplette Zertifikatketten gesandt werden sollen oder nicht. Mögliche Werte sind *yes* oder *no* (Defaultwert). Wählen Sie hier *yes,* falls Sie nicht die Zertifikate aller Stufen von Ihrem bis zu dem der CA an den Peer senden möchten.
Dont send CRLs	Gibt an, ob während des IKE CRLs gesandt werden sollen oder nicht. Mögliche Werte sind *yes* (Defaultwert) oder *no*.
Dont send Key Hash Payl.	Gibt an, ob während des IKE Schlüssel-Hash-Nutzdaten gesandt werden oder nicht. Als Default wird der Hash des Public Key (öffentlichen Schlüssels) der entfernten Seite zusammen mit den anderen Authentifizierungsdaten gesandt. Gilt nur für ➤➤ **RSA**-Verschlüsselung; wählen Sie *yes*, um dieses Verhalten zu unterdrücken. Mögliche Werte sind *yes* oder *no* (Defaultwert).

Feld	Wert
Trust ICMP Messages	Gibt an, ob beim IKE auf die ➤➤ **ICMP**-Meldungen "Port Unreachable" und "Host Unreachable" vertraut werden soll oder nicht. Auf die ICMP-Meldungen "Port Unreachable" und "Host Unreachable" wird nur dann vertraut, falls während dieser Aushandlung keine Datagramme vom entfernten Host empfangen wurden. Das bedeutet, falls die lokale Seite als erste Antwort auf das erste Paket einer neuen Phase-1-Aushandlung die ICMP-Meldung "Port Unreachable" oder "Host Unreachable" empfängt, bricht sie die Aushandlung sofort ab. Mögliche Werte sind *yes* oder *no* (Defaultwert).
Dont Send Initial Contact	Gibt an, ob bei IKE-Aushandlungen IKE Initial Contact-Meldungen auch dann gesandt werden sollen, wenn keine SAs mit einem Peer bestehen, oder nicht. Mögliche Werte sind *yes* oder *no* (Defaultwert).
Sync SAs With Local Ifc	Stellt sicher, dass alle SAs gelöscht werden, deren Datenverkehr über eine Schnittstelle geroutet wurde, deren Status von *up* auf *down*, *dormant* oder *blocked* gewechselt hat. Mögliche Werte sind *yes* oder *no* (Defaultwert).
Max. Symmetric Key Length	Gibt die maximale Länge eines Chiffrierschlüssels (in Bits) an, die von der entfernten Stelle akzeptiert wird. Diese Grenze verhindert "denial-of-service"-Angriffe, bei denen der Angreifer nach einem riesigen Schlüssel für einen Verschlüsselungsalgorithmus fragt, der variable Schlüssellängen zuläßt. Der Defaultwert ist *1024*.

Feld	Wert
Use Zero Cookies	Gibt an, ob zeroed (auf Null gesetzte) ISAKMP-Cookies gesandt werden sollen oder nicht. Diese sind dem SPI (Security Parameter Index) in IKE-Proposals äquivalent; da sie redundant sind, werden sie normalerweise auf den Wert der laufenden Aushandlung gesetzt. Alternativ kann das Gateway Nullen für alle Werte des Cookies nutzen. Wählen Sie *yes* für diese Option. Mögliche Werte sind *yes* (Defaultwert) oder *no*.
Cookies Size	Gibt die Länge der in IKE-Proposals benutzten zeroed SPI in Bytes an. Dieses Feld wird nur dann wirksam, wenn ***USE ZERO ISAKMP COOKIES*** auf *yes* gesetzt ist. Der Defaulwert ist *32*.
RADIUS Authentication	Hier können Sie die RADIUS-Authentisierung über IPSec aktivieren. Mögliche Werte sind *enabled* und *disabed* (Defaultwert).

Tabelle 8-1: ***IPSEC ➜ ADVANCED SETTINGS***

9 Untermenü *WIZARD*

Im folgenden wird das Untermenü *WIZARD* beschrieben.

Im Menü Wizard können Sie den IPSec Wizard des Setup Tools erneut starten, den Sie bereits zu Beginn der IPSec-Konfiguration einmal durchlaufen haben. Zwar erzwingt das Setup Tool seine Verwendung nicht, aber ohne zumindest den nicht-interaktiven Teil des Wizards durchlaufen zu haben, stehen die erforderlichen Profile für Phase 1 und Phase 2 nicht zur Verfügung.

Wenn Sie das IPSec-Menü aus dem Hauptmenü zum ersten Mal auswählen, startet automatisch der IPSec Wizard. Wenn Sie die Abfrage, ob der Wizard ausgeführt werden soll, bestätigen, öffnet sich folgendes Fenster:

```
VPN Access Setup Tool                        Bintec Access Networks GmbH
[IPSEC] [WIZARD]: IPsec Configuration - Wizard Menu            MyGateway

   IPsec 1st step configurations wizard

   Configuration History:



   What to do?                                              start wizard
                                                    (<Space>  to choose)
                                                    (<Return> to select)
                                 Exit
```

Wenn Sie sich zum ersten Mal im Wizard-Menü befinden, stehen Ihnen nur zwei Optionen zur Verfügung: Sie können den Wizard mit ***START WIZARD*** starten oder das Wizard-Menü mit ***EXIT*** verlassen. Wenn Sie den IPSec Wizard starten,

werden Ihnen Informationen zu den Konfigurationsschritten im Fensterbereich unter der Überschrift Configuration History angezeigt:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[IPSEC] [WIZARD]: IPsec Configuration - Wizard Menu              MyGateway

IPsec 1st step configurations wizard

Configuration History:
   - for ESP:  NULL Rijndael Twofish Blowfish CAST DES DES3
               MD5 SHA1 NOMAC
   - for AH:   SHA1 MD5
+ Check default IKE profile ...
  already configured (default setings)
+ Check default IPSec profile ...
  already configured (default setings)
+ Check IPSEC Default Authentication Method ...
  Currently set to "Pre Shared Keys"

Use which Default IPSEC Authentication Method ?          current: PSK
                                                  (<Space>  to choose)
                                                  (<Return> to select)
                                        Exit
```

Nach Beginn der Konfiguration mittels des IPSec Wizards stehen Ihnen für das Feld ***WHAT TO DO?*** folgende Optionen zur Verfügung:

Wert	Bedeutung
clear config	Diese Einstellung macht alle Einstellungen rückgängig, die während der Konfiguration vorgenommen worden sind. Nachdem die Konfiguration gelöscht worden ist, sollten Sie den Wizard erneut starten. Sollten sich bereits Schlüsselpaare (Public Key Pairs) auf dem Gateway befinden, so werden diese nicht gelöscht, um die Gültigkeit vorhandener ➤➤ **Zertifikate** nicht zu zerstören.

Wert	Bedeutung
dump messages	Das Gateway sichert die Nachrichten, die währen der Konfiguration ausgegeben worden sind, entweder lokal oder auf einem konfigurierten Syslog-Host.
skip	Mit dieser Option können Sie einen Konfigurationsschritt überspringen, wenn dieser nicht notwendig ist (zum Beispiel das Anfordern eines Zertifikates, wenn bereits eines vorhanden ist).
abort	Diese Option steht zur Verfügung, um einen notwendigen Konfigurationsschritt zu umgehen. Die Option beendet den IPSec Wizard ebenso wie ***EXIT***, allerdings bleiben Sie im Wizard-Menü und können den Wizard ggf. direkt wieder aufrufen.
start (wizard)	Diese Option ruft entweder einen spezifischen Vorgang auf, der bisher nicht ausgeführt wurde oder startet den Wizard von vorn. Sie steht nur zur Verfügung, wenn die Wizard-Konfiguration noch unvollständig ist.

Tabelle 9-1: ***WHAT TO DO?***

Der IPSec- Wizard Schritt für Schritt

Der IPSec Wizard ist kein Menü im eigentlichen Sinn, sondern eine Abfolge automatisierter Abläufe. Der Wizard führt Sie dabei durch die zur Konfiguration notwendigen Menüs. Diese unterscheiden sich nicht von den Menüs, die auch vom ***IPSEC*** Hauptmenü zugänglich sind. Sie können eine mit dem Wizard erstellte Konfiguration daher jederzeit Ihren Bedürfnissen anpassen.

Der Wizard durchläuft folgende Schritte:

Schritt 1 (NAT-Einstellungen)

Der Wizard überprüft, ob auf Ihrem Gateway ➤➤ **NAT** aktiviert ist, und passt die Einstellungen ggf. so an, dass eine funktionsfähige IPSec-Konfiguration sichergestellt ist und keine Datenpakete unnötigerweise verworfen werden. Wenn der Wizard Änderungen an der NAT-Konfiguration vornimmt, werden diese in der Configuration History angezeigt.

Schritt 2 (Erstellung der Proposals)

Der Wizard stellt ➤➤ **Verschlüsselungs** -und Message-Hash-Algorithmen zu sogenannten Proposals zusammen. In diesem Schritt werden keine Konfigurationseinstellungen vorgenommen, Sie können die zu verwendenden Proposals später im IPSec-Hauptmenü oder bei der Peer-Konfiguration bestimmen. Während der Wizard-Konfiguration wird eine Default-Kombination ausgewählt.

Schritt 3 (Authentisierungsart festlegen)

Der Wizard fragt ab, welche Authentisierungsart (Authentication Method) verwendet werden soll. Wenn Sie Pre Shared Keys verwenden, fahren Sie mit Schritt 8 fort und erstellen einen Peer mit dem notwendigen Passwort (dem Preshared Key).

Wenn Sie eine auf ➤➤ **Zertifikaten** basierende Methode auswählen, erstellt der Wizard zunächst ein entsprechendes Schlüsselpaar und fährt mit den Schritten 4 bis 7 fort.

Schritt 4 (Zertifikat beantragen)

Der Wizard überprüft, ob auf dem Gateway bereits eigene Zertifikate für die vorhandenen Schlüsseln installiert sind. Wenn der Wizard ein Schlüsselpaar erstellt hat, werden Sie aufgefordert, ein Zertifikat für diesen Schlüssel zu beantragen.

Wenn Sie ein Zertifikat beantragen wollen (Sie müssen dafür bestimmte Informationen zur Verfügung haben), springt der Wizard in das entsprechende Menü (“Zertifikatanforderung” auf Seite 73). Nach Eingabe der notwendigen Daten gelangen Sie zurück in das Wizard-Menü.

Schritt 5 (Eigenes Zertifikat)

Wenn Sie entweder ein Zertifikat beantragt haben oder den entsprechenden Wizard-Schritt übersprungen haben, fragt der Wizard, ob Sie ein eigenes Zertifikat (Own Certificate) importieren wollen. Wenn Sie Ihr Zertifikat noch nicht erhalten haben, können Sie den Wizard nun beenden und später mit der Konfiguration fortfahren. Wenn Sie Ihr Zertifikat mittels SCEP beantragt haben, wird es automatisch vom Gateway gespeichert, sobald die Certificate Authority das Zertifikat ausgestellt hat. In diesem Fall können Sie diesen Schritt überspringen.

Haben Sie das Zertifikat manuell beantragt, so bestätigen Sie, und der Wizard wechselt in das Menü zum Zertifikat-Import. Siehe “Zertifikat-Untermenüs” auf Seite 78. Nach Eingabe der notwenigen Daten gelangen Sie in das Wizard-Menü zurück.

Schritt 6 (CA-Zertifikat) Sobald Ihr Zertifikat auf dem Gateway installiert ist, fordert der Wizard Sie zum Download eines ➤➤ **CA**-Zertifikats (Certificate Authority Certificate) auf. Dieses ist das Zertifikat, mit dem sich die CA, die Ihr Zertifikat ausgestellt hat, ihrerseits authentisiert. Der Wizard wechselt in das entsprechende Menü. Siehe “Zertifikat-Untermenüs” auf Seite 78. Nach Eingabe der notwenigen Daten gelangen Sie in das Wizard-Menü zurück.

Schritt 7 (CRL Server / Peer Certificate) Wenn sowohl Ihr Zertifikat als auch das der CA auf dem Gateway installiert sind, fordert der Wizard Sie auf, einen Server anzugeben, von dem Certificate Revocation Lists (CRLs) heruntergeladen werden können. Dies ist dann notwendig, wenn im CA-Zertifikat kein CRL Distribution Point angegeben ist, Sie aber ➤➤ **RSA** Encryption als Authentication Method ausgewählt haben.

Wenn Sie einen CRL-Server angeben wollen, wechselt der Wizard in das entsprechende Menü. Siehe “Untermenü CERTIFICATE SERVERS” auf Seite 85. Nach Eingabe der notwenigen Daten gelangen Sie in das Wizard-Menü zurück.

Wenn SIe keinen CRL-Server angeben und kein CRL Distribution Point im CA-Zertifikat angegeben ist, Sie aber dennoch RSA Encryption als Authentication Method gewählt haben, fordert der Wizard Sie zum Download eines Peer-Zertifikates auf. Er wechselt in das entsprechende Menü. Siehe “Zertifikat-Untermenüs” auf Seite 78. Nach Eingabe der notwenigen Daten gelangen Sie in das Wizard-Menü zurück.

Schritt 8 (Peer) Im nächsten Schritt werden Sie aufgefordert, einen IPSec-Peer zu konfigurieren. Der Wizard wechselt in das entsprechende Menü. Siehe “Untermenü CONFIGURE PEERS” auf Seite 11. Nach Eingabe der notwenigen Daten gelangen Sie in das Wizard-Menü zurück.

Schritt 9 (Peer Traffic / Peer Interface) Wenn Sie einen Peer angelegt haben, fordert der Wizard Sie auf, den zu sichernden Datenverkehr zu spezifizieren.

Wenn Sie den Peer mit einem virtuellen Interface angelegt haben, wechselt der Wizard in das Menü zur Eingabe der Peer IP Settings. Siehe “Untermenü INTERFACE IP SETTINGS” auf Seite 46. Nach Eingabe der notwenigen Daten gelangen Sie in das Wizard-Menü zurück.

Wenn Sie den Peer mit Traffic-Listen angelegt haben, wechselt der Wizard in das Menü zur Definition eines Traffic-Listen-Eintrags. Siehe “Untermenü

TRAFFIC LIST SETTINGS" auf Seite 42. Nach Eingabe der notwenigen Daten gelangen Sie in das Wizard-Menü zurück.

Schritt 9 beendet die IPSec-Wizard-Konfiguration. Das Gateway verfügt nun über eine funktionsfähige IPSec-Konfiguration.

10 Untermenü *MONITORING*

Im folgenden wird das Untermenü *MONITORING* beschrieben.

Im Menü ***IPSEC*** ➜ ***MONITORING*** gelangt man in folgende Untermenüs:

- ***GLOBAL SETTINGS***
- ***IKE SECURITY ASSOCIATIONS***
- ***IPSEC SA BUNDLES***

Das letzte Menü aus dem IPSec-Kontext ist ***IPSEC*** ➜ ***MONITORING***. Hier können Sie sich den Status der globalen Statistiken, IKE Security Associations und IPSec Security Associations anzeigen lassen. Dementsprechend enthält es drei Untermenüs, die in den folgenden Kapiteln beschrieben werden.

10.1 Untermenü *GLOBAL STATISTICS*

Alle Felder im Menü ***IPSEC*** ➜ ***MONITORING*** ➜ ***GLOBAL STATISTICS*** können nur gelesen werden, d. h. Sie können sich hier die Einstellungen und Statistiken anzeigen lassen, können jedoch keine Änderungen an der Konfiguration vornehmen.

Es sieht folgendermaßen aus (die hier aufgeführten Werte sind nur Beispiele):

```
VPN Access Setup Tool                          Bintec Communications AG
[IPSEC][MONITORING][STATS]: IPSec Monitoring -
                            Global Statistics                  MyGateway

 Peers    Up     :  10    /16      Dormant: 6         Blocked: 0

 SAs      Phase 1:  10    /0      Phase 2: 10    /0

 Packets            In           Out

          Total  :  850          600
          Passed :  50           50
          Dropped:  30           40
          Protect:  770          510
          Errors :  0            0

                                EXIT
```

Die Felder und die Bedeutung der angezeigten Werte sind folgende:

Feld	Wert
Peers Up	Zeigt die Anzahl der aktiven Peers (***OPERSTATUS*** = *up*) von der Anzahl der konfigurierten Peers.
Peers Dormant	Zeigt die Anzahl der inaktiven Peers (***OPERSTATUS*** = *dormant*).
Peers Blocked	Zeigt die Anzahl der blockierten Peers (***OPERSTATUS*** = *blocked*).
SAs Phase 1	Zeigt die Anzahl der aktiven Phase-1-SAs (State = established) zur Gesamtzahl der Phase-1-SAs an.
SAs Phase 2	Zeigt die Anzahl der aktiven Phase-2-SAs (***STATE*** = *established*) zur Gesamtzahl der Phase-2-SAs an.

Feld	Wert
Packets In/Out	Hier wird die Anzahl der Pakete angezeigt, die auf eine bestimme Art und Weise behandelt worden sind: ■ *Total*: Die Anzahl aller bearbeiteten Pakete. ■ *Passed*: Die Anzahl der Pakete, die im Klartext weitergeleitet wurden. ■ *Dropped*: Die Anzahl der verworfenen Pakete. ■ *Protect*: Die Anzahl der durch IPSec geschützten Pakete. ■ *Error*: Die Anzahl der Pakete, bei deren Behandlung es zu Fehlern gekommen ist.

Tabelle 10-1: ***IPSEC ➜ MONITORING ➜ GLOBAL STATISTICS***

10.2 Untermenü *IKE SECURITY ASSOCIATIONS*

Das nächste Überwachungs-Untermenü (***IPSEC*** ➜ ***MONITORING*** ➜ ***IKE SECURITY ASSOCIATIONS***) zeigt Statistiken über die IKE-SAs an. Es sieht folgendermaßen aus (die aufgeführten Werte sind nur Beispiele):

```
VPN Access Setup Tool                          Bintec Communications AG
[IPSEC][MONITORING][IKE SAS]: IPSec Monitoring -
                                IKE SAs                          MyGateway

T: xch.-Type: B=Base      I=Id-prot.  O=auth-Only A=Aggressive
A: Auth-Meth: P=P-S-Key   D=DSA-sign. S=RSA-sign. E=RSA-encryption
R: Role     : I=Initiator R=Responder
S: State    : N=Negotiate E=Establ.   D=Delete W=Waiting-for-remove
E: Enc.-Alg : d=DES D=3ES B=Blowfish  C=Cast R=Rijndael T=Twofish
H: Hash-Alg : M=MD5       S=SHA1      T=Tiger      R=Ripemd160
type 'h' to toggle this help

Remote ID               Remote IP       Local ID        TARSEH

remote                  192.168.1.1     local           IPIEBM




     DELETE              EXIT
```

Die Bedeutung der Zeichen in der Spalte ***TARSEH*** (das ist die letzte Spalte rechts unterhalb des Hilfebereichs des Menüfensters) wird im oberen Teil des Menüfensters erläutert; somit ist das oben dargestellte Beispiel folgendermaßen zu verstehen:

Feld	Wert
Remote ID	Zeigt die ID des entfernen Peers an. Im Beispiel erfolgt die Authentifizierung mit Zertifikaten; damit besteht die entfernte ID aus Quotes aus dem Zertifikat des Peers.
Remote IP	Zeigt die IP-Adresse des entfernten Peers an.

Feld	Wert
Local ID	Zeigt die lokale ID an. Auch hier besteht die ID aus Quotes aus dem Zertifikat welches für die Authentifizierung benutzt wurde.
TARSEH	Zeigt die Kombination der im Hilfebereich des Menüfensters erläuterten Parameter an. Das Beispiel ISREBM bedeutet somit: ■ Austauschtyp: id_protect (*I*) ■ Authentifizierungsmethode: RSA-Signatur (*S*) ■ Rolle: Antwortender (Responder, *R*) ■ Status: Eingerichtet (Established, *E*) ■ Verschlüsselungsalgorithmus: Blowfish (*B*) ■ Hash-Algorithmus: MD5 (*M*)

Tabelle 10-2: ***IPSEC ➜ MONITORING ➜ IKE SECURITY ASSOCIATIONS***

10.3 Untermenü *IPSEC SA BUNDLES*

Das nächste Untermenü (***IPSEC*** ➜ ***MONITORING*** ➜ ***IPSEC SA BUNDLES***) zeigt die IPSec-Security Associations an, die in IKE Phase 2 ausgehandelt wurden. Das Menü sieht folgendermaßen aus:

```
VPN Access Setup Tool                          Bintec Communications AG
[IPSEC][MONITORING][IPSEC BUNDLES]: IPsec Monitoring -
                                    IPsec SA Bundles          MyGateway

 Local            LPort Pto  Remote              RPort CEA   In    Out

 192.168.1.2/32     0    all  192.168.1.1/32      0     -E-   888   1232









   DELETE              EXIT
```

Die Bedeutung der Abkürzung in der Spalte **SEA** wird wieder im Hilfebereich des Menüfensters erläutert. Die Felder haben folgende Bedeutung:

Feld	Wert
Local	Zeigt die lokale ➤➤ **IP-Adresse**, den Adressenbereich oder das Netz an, welches von dieser SA geschützt wird.
LPort	Zeigt die lokale ➤➤**Port**nummer oder den Portnummernbereich an, die/der von dieser SA geschützt wird.
Pto	Zeigt das Schicht-4-Protokoll des durch diese SA geschützten Datenverkehrs an (*0* = jedes).
Remote	Zeigt die entfernte IP-Adresse, den Adressenbereich oder das Netz an, welches von dieser SA geschützt wird.

Feld	Wert
RPort	Zeigt die entfernte Portnummer oder den Portnummernbereich an, die/der von dieser SA geschützt wird.
CEA	Zeigt an, welche IPSec-Protokolle für die SA verwendet werden: ■ *C* = IPComP ■ *E* = ESP ■ *A* = AH.
In	Zeigt die Anzahl der über diese SA empfangenen Bytes an.
Out	Zeigt die Anzahl der über diese SA gesendeten Bytes an.

Tabelle 10-3: ***IPSEC ➜ MONITORING ➜ IPSEC SECURITY ASSOCIATIONS***

Index: IPSec

Numerics

A

B

C