IPSec

Version 0.9

Purpose

This document is part of the user's guide to the installation and configuration of Bintec gateways running software release 7.1.4 or later. For up-to-the-minute information and instructions concerning the latest software release, you should always read our **Release Notes**, especially when carrying out a software update to a later release level. The latest **Release Notes** can be found at www.bintec.net.

Liability

While every effort has been made to ensure the accuracy of all information in this manual, Bintec Access Networks GmbH cannot assume liability to any party for any loss or damage caused by errors or omissions or by statements of any kind in this document and is only liable within the scope of its terms of sale and delivery.

The information in this manual is subject to change without notice. Additional information, changes and **Release Notes** for Bintec gateways can be found at www.bintec.net.

As multiprotocol gateways, Bintec gateways set up WAN connections in accordance with the system configuration. To prevent unintentional charges accumulating, the operation of the product should be carefully monitored. Bintec Access Networks GmbH accepts no liability for loss of data, unintentional connection costs and damages resulting from unsupervised operation of the product.

Trademarks

Bintec and the Bintec logo are registered trademarks of Bintec Access Networks GmbH.

Other product names and trademarks mentioned are usually the property of the respective companies and manufacturers.

Copyright

Guidelines and standards

Bintec gateways comply with the following guidelines and standards:

R&TTE Directive 1999/5/EG

CE marking for all EU countries and Switzerland

You will find detailed information in the Declarations of Conformity at www.bintec.net.

How to reach Bintec

Bintec Access Networks GmbH Suedwestpark 94 D-90449 Nuremberg Germany Telephone: +49 180 300 9191 0 Fax: +49 180 300 9193 0 Internet: www.bintec.net	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 IPSec Menu

The fields of the *IPSEC* menu are described below.

When you configure IPSec for the first time, a ➤➤ **Setup Tool** Wizard is started that guides you through a partly automatic configuration of various initial settings. (The configuration with the Setup Tool Wizard is described in "Submenu Wizard" on page 89.)

The IPSec Main menu opens on exiting the IPSec Wizard. The menu is as follows:

```
VPN Access 25 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
```

Note

You must follow the IPSec Wizard at least until the first command prompt. If you wish, you can cancel the IPSec Wizard at the first command prompt and continue the configuration in the IPSec menus, but we recommend creating the first peer completely with the IPSec Wizard.

If the IPSec Wizard cannot make the necessary ➤➤ **NAT** settings and create the IKE and IPSec proposals, further configuration steps are necessary. Some of these are only possible in the ➤➤ **SNMP shell**, but are essential for IPSec configuration.

Only the ***ENABLE IPSEC*** field in the ***IPSEC*** Main Menu offers you the choice of two options.

ENABLE IPSEC This field contains the following values:

Description	Meaning
no (default value)	IPSec is not activated regardless of the configuration. If IPSec is currently activated, it is deactivated as soon as you press **SAVE**.
yes	IPSec is activated as soon as you press **SAVE**. If you do not have a valid IPSec license, all IP packets are denied until you deactivate IPSec again. All devices in the **VPN Access** line possess an IPSec license as standard.

Table 1-1: Fields of the ***ENABLE IPSEC*** submenu

For the ***IKE (PHASE 1) DEFAULTS*** and ***IPSEC (PHASE 2) DEFAULTS*** fields, you can also choose between the profiles configured in the ***EDIT*** menu.

2 Submenu Pre IPSec Rules

The *PRE IPSEC RULES* submenu is described below.

If you configure IPSec on your gateway, you must create rules for handling the data traffic before the IPSec SAs are used. For example, you must allow specific packets to pass in plain language to fulfill certain basic functions.

All the rules already created are listed in the first window of the ***PRE IPSEC*** menu:

```
VPN Access 25 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   192.168.13.1    M32   80    PA  default
own Address         -   tcp   192.168.13.1    M32   21    DR  default




     APPEND              DELETE              EXIT
```

These values are read only and depend on the settings made in ***IPSEC*** ➜ ***PRE IPSEC RULES*** ➜ **APPEND/EDIT**. More information about the settings can be found in the next chapter (see “Submenu APPEND/EDIT” on page 7).

The following entries are included:

Field	Description
Local Address	Shows the local ➤➤ **IP address** of the rule.

Field	Description
M/R	Shows the length of the ➤➤ **netmask** (if the rule has been defined for a network) or the number of consecutive IP addresses if the rule has been created for an IP address range. *M32* therefore stands for a 32-bit netmask (255.255.255.255, i.e. an individual host) and *R10* for a series of 10 IP addresses including the specified address.
Port	Shows the local or remote ➤➤ **port** number used for filtering the packets; applies only to UDP and TCP ports (*0* = all).
Proto	Shows the protocol used for filtering the packets using this rule.
Remote Address	Shows the remote IP address of this rule.
A	Shows the action initiated by this rule. The filtered packets are either denied (*DR*) or can pass unchanged (*PA*).
Proposal	Shows the IPSec proposals used. This has no function for pre IPSec rules, as no SAs (Security Associations) are used.

Table 2-1: ***IPSec ➜ Pre IPSec Rules***

You can only configure one setting in this menu: You can define which of the traffic list entries is to be the first active rule in the rule chain. You can also shift the rules up or down within the list to arrange the pre IPSec rules to suit your needs. Every rule before the rule defined as "active traffic list" is ignored. How the active traffic list is selected is described in the help section of the menu window.

2.1 Submenu APPEND/EDIT

Pre IPSec rules are edited or added in the ***IPSec*** ➜ ***Pre IPSec Rules*** ➜ ***APPEND/EDIT*** menu. The following menu window opens in both cases (if you edit an existing entry, the existing values of this entry are shown):

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[Pre IPSEC TRAFFIC][ADD]: Edit Traffic Entry                  MyGateway

Description:

     Protocol:      don't-verify

     Local:
          Type: net   Ip:                / 0

     Remote:
          Type: net   Ip:                / 0

     Action:        pass

                    SAVE                                  CANCEL
```

The menu consists of the following fields:

Field	Description
Description	Enter a description that enables the type of rule to be clearly identified.
Protocol	Here you can define whether the applicable data traffic for this rule is only to apply to packets with a certain protocol. You can choose between specific protocols and the option *don't-verify* (default value), which means that the protocol is not used as filter criterion.
Local: Type	Enter the local address data. For possible values, see table "Local/Remote: Type," on page 9.

Field	Description
Remote: Type	Enter the remote address data. The options are largely the same as the options in the ***LOCAL: TYPE*** field, with one exception: The *own* option is not available and is replaced by *peer*. This is only relevant for peer configuration.
Action	You can choose between two options: ■ *pass* (default value)*:* This option allows IPSec packets to pass unchanged. ■ *drop:* This option denies all packets that match the filter set.

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

LOCAL/REMOTE: TYPE The ***LOCAL/REMOTE: TYPE*** field has the following options:

Description	Meaning
host	Define the IP address of an individual machine to which this rule is to be applied. If you have selected certain protocols to restrict the data traffic, you may be requested to enter a ***PORT*** number. This only applies to UDP and TCP.
net (default value)	Define the IP address of the network and the corresponding netmask to which this rule is to be applied. The command prompt for the netmask appears automatically if you select *net*. It is separated from the IP address by "/". You are requested to enter a ***PORT*** number again.

Description	Meaning
range	Define an IP address range to which this rule is to be applied. The command prompt automatically allows two IP addresses to be entered. These are separated by "-". You are requested to enter a ***PORT*** number again.
dhcp	Only for ***REMOTE: TYPE***. The remote gateway obtains its IP configuration via ➤➤ **DHCP**.
own/peer	If you select this option, the IP address of the gateway (if usable) is automatically rated as affected by the rule. No other settings are necessary. Although this entry can be selected here, it cannot be used on pre IPSec rules. It is used for peer configuration (see "Submenu Traffic List Settings" on page 40).

Table 2-3: ***LOCAL/REMOTE: TYPE***

Note

Make sure the pre IPSec rules have been carefully configured. This is decisive for proper functioning of all data traffic that is not to be protected by IPSec procedures.

It is particularly important that IKE traffic in plain language is allowed to pass. This can be achieved by configuring a pre IPSec rule with the following specifications:

- ***PROTOCOL***= *udp*
- ***LOCAL TYPE***: *net* (the IP address and netmask fields remain empty)
- ***LOCAL PORT***: *500*
- ***REMOTE TYPE***: *net* (the IP address and netmask fields also remain empty)
- ***REMOTE PORT***: *500*
- ***ACTION***: *pass*

The IPSec Wizard modifies the settings if necessary.

3 Submenu Configure Peers

The *CONFIGURE PEERS* submenu is described below.

The menu (***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***APPEND***) for creating a peer (of any type) has the following structure:

```
VPN Access 25 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
```

It contains the following fields:

Field	Description
Description	Here you enter the desired description of the peer. The maximum length of the entry is 255 characters.

Field	Description
Admin Status	Here you select the status to which you wish to set the peer after saving the configuration. The setting applies to any type of peer. Possible settings: ■ *up* (default value) - The peer is available for setting up a tunnel immediately after saving the configuration. ■ *down* - The peer is initially not available after saving the configuration. ■ *dialup* - A tunnel is set up once after saving. All the possible types of connection (including callback) are covered. ■ *callback* - A tunnel is set up to the peer after saving. This is done as if an initial callback has already been received.
Oper Status	Shows the present status of the peer. This field cannot be edited.
Peer Address	Here you enter the official ➤➤ **IP address** of the peer or its resolvable ➤➤ **host name**. This entry is not necessary in certain configurations.
Peer IDs	Here you enter the ID of the peer. This entry is not necessary in certain configurations. On the peer gateway, this ID corresponds to the ***Local ID*** (***Configure Peers*** ➜ ***APPEND/EDIT*** ➜ ***Peer specific Settings*** ➜ ***IKE (Phase 1) Defaults: edit*** ➜ ***ADD/EDIT***).

Field	Description
Pre Shared Key	Only for authentication via preshared keys. Here you enter the pass phrase agreed with the peer. The ***AUTHENTICATION METHOD*** for the peer can be modified in the ***CONFIGURE PEERS*** ➜ **APPEND/EDIT** ➜ ***PEER SPECIFIC SETTINGS*** ➜ ***IKE (PHASE 1) DEFAULTS: EDIT*** menu.
Virtual Interface	Here you define if the peer is listed with a traffic list or as a virtual interface. Possible settings: ■ *no* - Connections to the peer are controlled via a traffic list. ■ *yes* - The peer is created as a virtual interface. The data traffic routed over this interface is fully encrypted. The default setting is *no*.

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

The peer is modified in the following menus:

- ***IPSEC CALLBACK*** (information on configuration of the IPSec callback - see “Submenu IPSec Callback” on page 14),
- ***PEER SPECIFIC SETTINGS*** (see “Submenu Peer specific Settings” on page 22),
- ***TRAFFIC LIST SETTINGS*** (for ***VIRTUAL INTERFACE*** = *no*, for information on the configuration of traffic lists see “Submenu Traffic List Settings” on page 40),
- ***INTERFACE IP SETTINGS*** (for ***VIRTUAL INTERFACE*** = *yes*, see “Submenu Interface IP Settings” on page 44).

3.1 Submenu IPSec Callback

To enable hosts without fixed IP addresses to obtain a secure connection over the ➤➤ **Internet**, Bintec has supported the DynDNS service since Release 6.2.2. This service enables a peer to be identified using a host name that can be resolved by DNS. It is not necessary to configure the IP address of the peer.

The DynDNS service does not signal whether a peer is actually online and cannot cause a peer to set up an Internet connection to enable an IPSec tunnel over the Internet. This possibility is created with the IPSec callback: A direct ➤➤ **ISDN** call to a peer signals that you are online and waiting for the peer to set up an IPSec tunnel over the Internet. If the called peer currently has no connection to the Internet, the ISDN call causes a connection to be set up. This ISDN call costs nothing (depending on country), as it does not have to be accepted by the gateway. The identification of the caller from his ISDN number is sufficient information to initiate setting up a tunnel.

Before you can configure this service, you must first configure a number for IPSec callback in the ***ISDN0*** ➜ ***INCOMING CALL ANSWERING*** menu. The value *IPSec* is available for this purpose in the ***ITEM*** field. This entry ensures that incoming calls for this number are routed to the IPSec service.

The rest of the configuration is carried out in the ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***APPEND/EDIT*** menu. This menu contains the ***ISDN CALLBACK*** submenu:

```
VPN Access 25 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
```

The menu contains the following fields:

Field	Description
ISDN Callback	Here you select the Callback Mode. See table “ISDN Callback,” on page 16 for the available options.
Incoming ISDN Number	Only for ***ISDN CALLBACK*** = *passive* or *both*. Here you enter the ISDN number from which the remote gateway calls the local gateway (calling party number).
Outgoing ISDN Number	Only for ***ISDN CALLBACK*** = *active* or *both*. Here you enter the ISDN number with which the local gateway calls the remote gateway (calling party number).
Transfer own IP Address over ISDN	Here you can activate the function for transferring the IP address of the local gateway to the remote gateway. (Default value is *no*.) See “Transfer of IP Address over ISDN” on page 17 for information about this function.

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

Note

Make sure the number of the remote gateway is always entered in the ***INCOMING ISDN NUMBER*** and ***OUTGOING ISDN NUMBER*** fields. The two numbers are generally identical with the exception of the prefix "0". This must not be entered with the number for the ***IN*** field.

Under certain circumstances (e.g. when operating the gateway on a PABX with Calling Line Identification Restriction), it may be necessary to enter different numbers. Ask the system administrator for the numbers to be configured.

The ***ISDN CALLBACK*** field can have the following values:

Description	Meaning
disabled (default value)	ISDN callback is deactivated. The local gateway neither reacts to incoming ISDN calls nor initiates ISDN calls to the remote gateway.

Description	Meaning
passive	The local gateway reacts only to incoming ISDN calls and, if necessary, initiates setting up an IPSec tunnel to the peer. No ISDN calls are sent to the remote gateway to cause this to set up an IPSec tunnel.
active	The local gateway sends an ISDN call to the remote gateway to cause this to set up an IPSec tunnel. The gateway does not react to incoming ISDN calls.
both	The gateway can react to incoming ISDN calls and send ISDN calls to the remote gateway. The setting up of an IPSec tunnel is executed (after an incoming ISDN call) and initiated (by an outgoing ISDN call).

TABLE 3-3: ISDN CALLBACK

If you have configured callback for a peer, this will always be executed. If callback is active, the peer is therefore caused to initiate setting up an IPSec tunnel by an ISDN call as soon as this tunnel is required. If callback is set to passive, setting up a tunnel to the peer is always initiated if an ISDN call is received on the relevant number. This ensures that both peers are reachable and that the connection can be set up over the Internet. The only case in which callback is not executed is if SAs (Security Associations) already exist, i.e. the tunnel to the peer already exists.

Note

If a tunnel is to be set up to a peer, the interface over which the tunnel is to be implemented is activated first by the IPSec Daemon. If DynIPSec is configured on the local gateway, the IP address is propagated first and then the ISDN call is sent to the remote gateway. This ensures that the remote gateway can actually reach the local gateway if it initiates the tunnel setup.

3.1.1 Transfer of IP Address over ISDN

Transferring the IP address of a gateway over ISDN (in the D-channel and/or B-channel) opens up new possibilities for the configuration of IPSec VPNs. This enables restrictions that occur in IPSec configuration with dynamic IP addresses to be avoided.

Before System Software Release 7.1.4, IPSec ISDN callback only supported tunnel setup if the current IP address of the initiator could be determined by indirect means (e.g. via DynDNS). However, DynDNS has serious disadvantages, such as the latency until the IP address is actually updated in the database. This can mean that the IP address propagated via DynDNS is not correct. This problem is avoided by transferring the IP address over ISDN. This type of transfer of dynamic IP addresses also enables the more secure ID Protect mode to be used for tunnel setup.

Method of operation

Various modes are available for transferring your own IP address to the peer: The address can be transferred free in the ➤➤ **D-channel** or in the ➤➤ **B-channel**, but here the call must be accepted by the remote station and therefore incurs costs.

If a peer whose IP address has been assigned dynamically wants to arrange for another peer to set up an IPSec tunnel, it can transfer its own IP address as per the settings described in “Configuration” on page 18. Not all transfer modes are supported by all telephone companies. If you are not sure, automatic selection by the gateway can be used to ensure that all the available possibilities can be used.

Note

The callback configuration on the two gateways should be identical so that the gateway of the called peer can identify the IP address information.

The IP address transfer and the start of IKE phase 1 negotiation take place in the following steps:

1. Peer A (the callback initiator) sets up a connection to the Internet in order to be assigned a dynamic IP address and be reachable for peer B over the Internet.

2. The gateway creates a token with a limited validity and saves it together with the current IP address in the ➤➤ **MIB** entry belonging to peer B.
3. The gateway sends the initial call to peer B, which transfers the IP address of peer A and the token as per the callback configuration.
4. Peer B extracts the IP address of peer A and the token from the ISDN call and assigns them to peer A based on the ➤➤ **calling party number** configured (the ISDN number used by peer A to send the initial call to peer B).
5. The IPSec Daemon at peer B's gateway can use the transferred IP address to initiate phase 1 negotiation with peer A. Here the token is returned to peer A in part of the payload in IKE negotiation.
6. Peer A is now able to compare the token returned by peer B with the entries in the MIB and so identify the peer without knowing its IP address.

As peer A and peer B can now mutually identify each other, negotiations can also be conducted in the ID Protect mode using preshared keys.

Configuration

The configuration is carried out in the context of IPSec callback configuration in the ***IPSec*** ➜ ***Configure Peers*** ➜ ***APPEND/EDIT*** ➜ ***IPSec Callback*** menu. If the ***Transfer own IP Address over ISDN*** field is set to *yes*, the menu changes as follows (the screenshot contains example values):

```
VPN Access 25 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
```

It now contains the following fields:

Field	Description
Transfer own IP Address over ISDN	Here you select whether the IP address of your own gateway is to be transferred over ISDN for IPSec callback. Possible values: ■ *yes* - The IP address is transferred according to the settings in the following fields. ■ *no* - (Default value) The IP address is not transferred.

Field	Description
Mode	Only visible if ***TRANSFER OWN IP ADDRESS OVER ISDN*** = *yes*. Here you select the mode in which the gateway tries to transfer its IP address to the peer. Possible values: ■ *autodetect best possible mode (D or B channel)* - (Default value) The gateway determines the best mode automatically. All D-channel modes are tried first before the B-channel is used (using the B-channel incurs costs). ■ *autodetect best possible mode (D channel only)* - The gateway determines the best D-channel mode automatically. The use of the B-channel is excluded. ■ *use specific D channel mode* - The gateway tries to transfer the IP address in the mode set in the ***D-CHANNEL MODE*** field. ■ *try specific D channel mode, fall back on B* - The gateway tries to transfer the IP address in the mode set in the ***D-CHANNEL MODE*** field. If this does not succeed, the IP address is transferred in the B-channel (this incurs costs). ■ *use B channel* - The gateway transfers the IP address in the B-channel. This incurs costs.

Field	Description
D-Channel Mode	Only visible if ***MODE*** = *use specific D channel mode* or *try specific D channel mode, fall back on B*. Here you select the D-channel mode in which the gateway tries to transfer the IP address. Possible values: ■ *LLC* - (Default value) The IP address is transferred in the LLC information elements of the D-channel. ■ *SUBADDR* - The IP address is transferred in the subaddress information elements of the D-channel. ■ *LLC-and-SUBADDR* - The IP address is transferred in both the LLC and subaddress information elements.

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

3.2 Submenu Peer specific Settings

The menu ***CONFIGURE PEERS*** ➜ ***APPEND/EDIT*** ➜ ***PEER SPECIFIC SETTINGS*** contains the options for modifying the IKE and IPSec settings for the peer:

```
VPN Access 25 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
```

This menu allows the selection of previously defined profiles for phase 1 and phase 2. The value *default* represents the profile set in the ***IKE (PHASE 1)/IPSEC (PHASE 2) DEFAULTS*** field of the IPSec main menu.

The ***SELECT DIFFERENT TRAFFIC LIST*** menu is only accessible if a peer with traffic lists is configured.

3.2.1 Submenu IKE (Phase 1) Profile

The menu for configuration of a phase 1 profile is accessible for peer configuration via the ***CONFIGURE PEERS*** ➜ ***APPEND/EDIT*** ➜ ***PEER SPECIFIC SETTINGS*** ➜ ***IKE (PHASE 1) PROFILE: EDIT*** ➜ ***ADD/EDIT*** menu:

```
VPN Access 25 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        :
   Nat-Traversal          :  enabled

   View Proposals >
   Edit Lifetimes >

                         SAVE                              CANCEL
```

The menu contains the following fields:

Field	Description
Description (Idx 0)	Here you enter the desired description of the profile. The maximum length of the entry is 255 characters.
Proposal	Information on these parameters: see “Proposal, Lifetime, Group...” on page 25
Lifetime	
Group	
Authentication Method	
Mode	

Field	Description
Heartbeats	Here you select whether and in what way IPSec heartbeats are used. Bintec has implemented an IPSec heartbeat to determine whether or not a Security Association (SA) is still valid. This function sends and receives signals according to the configuration. If these signals are not received, the SA is discarded as invalid. Possible settings: ■ *default* (default value) - The gateway uses the setting of the default profile. ■ *none* - The gateway sends and expects no heartbeat. ■ *expect* - The gateway expects a heartbeat from the peer, but does not send one itself. ■ *send* - The gateway expects no heartbeat from the peer, but sends one itself. ■ *both* - The gateway expects a heartbeat from the peer and sends one itself. For devices from the **VPN Access** Line, heartbeats are configured separately for phase 1 and phase 2. If interoperability with older software is to be assured, the same values must be configured for phase 1 and phase 2.
Block Time	Here you define how long a peer is blocked for tunnel setups after a phase 1 tunnel setup has failed. This affects only locally initiated setup attempts. Possible values are *-1* to *86400* (seconds); *-1* (default) means the value in the default profile is used and *0* means that the peer is never blocked.

Field	Description
Local ID	For information on these parameters see "Proposal, Lifetime, Group..." on page 25
Local Certificate	
CA Certificates	
Nat-Traversal	

Table 3-5: ***IPSec ➜ Configure Peers ➜ APPEND/EDIT ➜ Peer specific Settings ➜ IKE (Phase 1) Profile: edit ➜ ADD/EDIT***

3.2.2 Proposal, Lifetime, Group...

The fields of the *IKE (Phase 1) Profile: edit* ➜ *ADD/EDIT* menu described below need a more detailed explanation.

Phase 1: Proposal

In this field you can select any combination of encryption and message hash algorithms for IKE phase 1 on your gateway. The combination of six encryption algorithms and four message hash algorithms gives 24 possible values in this field. You can also select the value *none/default*, which assigns the peer the default proposal selected in the IPSec main menu.

The available encryption and message hash algorithms are listed in the two tables below:

Algorithm	Description
Blowfish	➤➤ **Blowfish** is a very secure and fast algorithm. Twofish can be regarded as the successor to Blowfish.
3DES	➤➤ **3DES** is an extension of the DES algorithm with an effective key length of 112 bits, which is rated as secure. It is the slowest algorithm currently supported.

Algorithm	Description
DES	➤➤ **DES** is an older encryption algorithm, which is rated as weak due to its small effective length of 56 bits.
CAST	➤➤ **CAST** is also a very secure algorithm, a little slower than Blowfish, but faster than 3DES.
Twofish	➤➤ **Twofish** was a final candidate for the AES (Advanced Encryption Standard). It is rated as just as secure as Rijndael (AES), but is slower.
Rijndael	Rijndael has been nominated as AES due to its fast key set-up, low memory requirements, high level of security against attacks and general speed.

Table 3-6: Encryption algorithms

The available ➤➤ **hash** algorithms are listed below:

Algorithm	Description
MD5 (Message Digest #5)	➤➤ **MD5** is an older hash algorithm. It is used with 96 bits digest length for IPSec.
SHA1 (Secure Hash Algorithm #1)	➤➤ **SHA1** is a hash algorithm developed by the NSA (United States National Security Association). It is rated as secure, but is slower than MD5. It is used with 96 bits digest length for IPSec.
RipeMD 160	➤➤ **RipeMD** 160 is a cryptographic 160-bit hash algorithm. It is used as a secure replacement for MD5 and RipeMD.

Algorithm	Description
Tiger 192	➤➤ **Tiger 192** is a relatively new and very fast algorithm.

Table 3-7: Message hash algorithms

Note

Note that the description of the encryption and authentication or the hash algorithms is based on the author's knowledge and opinion at the time of creating this User's Guide. Particularly the quality of the algorithms is subject to relative aspects and may change due to mathematical or cryptographic developments.

VIEW PROPOSALS

The ***VIEW PROPOSALS*** submenu provides an overview of the proposals created by the IPSec Wizard:

```
VPN Access 25 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
```

This menu is for information purposes only. Configuration is not possible.

Phase 1: Lifetime

This field shows the lifetime that may expire before a phase 1 key must be renewed with another Diffie-Hellman key calculation. This can be configured either as a value in seconds, as a processed amount of data (in kB) or as a combination of both. The default value is *900 sec/11000 kB,* which means the

key is renewed when either 900 seconds have elapsed or 11000 kB of data have been processed, depending on which event occurs first. If you have configured additional lifetime values, you can select from these here.

If you decide to configure additional lifetime values, you can do this in the ***EDIT LIFETIMES*** menu. The following menu mask is offered:

```
VPN Access 25 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
```

The menu contains the following fields:

Field	Description
Lifetime Restriction Based On	Select the criterion for the end of the key lifetime, possible values are: ■ *Time* and *Traffic* ■ *Time* ■ *Traffic* One or both of the following fields are shown, depending on your selection.
Seconds	Enter the lifetime for phase 1 key in seconds. The value can be any whole number value up to a length of 32 bits.

Field	Description
Kb	Enter the lifetime for phase 1 key as amount of data processed in kB. The value can be any whole number value up to a length of 32 bits.
Matching Policy	Here you can select how strictly the gateway observes the configured lifetime. Possible settings: ■ *loose* - The gateway accepts and uses any lifetime proposed in the negotiation (default value). ■ *strict* - The gateway accepts and uses only the configured lifetime. The phase 1 negotiation fails in the event of deviation. ■ *notify* - The gateway accepts all proposed values that are larger than the configured value, but uses its own smaller value itself and notifies the peer accordingly.

TABLE 3-8: LIFETIME

Phase 1: Group

The group defines the parameter set used as the basis for the Diffie-Hellman key calculation during phase 1. "MODP" as supported by Bintec gateways stands for "modular exponentiation". Three different settings can be selected: 768, 1024 or 1536 bits.

The field can have the following values:

Description	Meaning
1 (768-bit MODP)	During the Diffie-Hellman key calculation, modular exponentiation at 768 bits is used to create the encryption material.

Description	Meaning
2 (1024-bit MODP)	During the Diffie-Hellman key calculation, modular exponentiation at 1024 bits is used to create the encryption material.
5 (1536-bit MODP)	During the Diffie-Hellman key calculation, modular exponentiation at 1536 bits is used to create the encryption material.
none	The gateway uses no particular exponentiation after the lifetime expires, but proceeds as for the initial tunnel setup.
default	The gateway uses the setting of the default profile.

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

Phase 1: Authentication method

This field shows the authentication method you selected during configuration with the IPSec Wizard and enables you to change this:

Description	Meaning
Preshared Keys	If you do not use certificates for the authentication, you can select *Preshared Keys*. These are configured in the peer configuration in the ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***APPEND/EDIT*** menu.
DSA Signatures	Phase 1 key calculations are authenticated using the ➤➤ **DSA** algorithm.
RSA Signatures	Phase 1 key calculations are authenticated using the ➤➤ **RSA** algorithm.
RSA Encryption	In RSA encryption the ID payload is also encrypted for additional security.

Description	Meaning
default	This value is shown if you have configured the peer to use the global defaults.

Table 3-10: *AUTHENTICATION METHOD*

Phase 1: Mode

The Mode field shows the currently configured phase 1 mode and enables you to change the settings:

Description	Meaning
id_protect	This mode (also designated Main Mode) requires six messages for a Diffie-Hellman key calculation and thus for configuring a secure channel, over which the IPSec SAs can be negotiated. A condition is that both peers have static IP addresses if preshared keys are used for authentication. This limitation does not apply if IPSec callbacks are used. see “Submenu IPSec Callback” on page 14
aggressive	The Aggressive Mode is necessary if one of the peers does not have a static IP address and preshared keys are used for authentication; it requires only three messages for configuring a secure channel.
default	The peer is not assigned any specific mode and the global default setting is used.
id-protect-only	The gateway accepts only the ID Protect Mode in the negotiation. If the peer suggests another mode, the negotiation fails.
aggressive-only	The gateway accepts only the Aggressive Mode in the negotiation. If the peer suggests another mode, the negotiation fails.

Table 3-11: *MODE*

Phase 1: Local ID

This is the ID you assign to your gateway. If you leave this field empty, the gateway selects the default values. These are:

- For authentication with preshared keys: the local IP address as shown in the ***IPSECPEERLOCALADDRESS*** field in the ***IPSECPEERTABLE***.
- For authentication with ➤➤ **certificate**: the first alternative subject name indicated in the certificate or, if none is shown, the subject name of the certificate.

Note

If you use certificates for authentication and your certificate contains alternative subject names (see "Request Certificate" on page 71), you must make sure the gateway selects the first alternative subject name by default. Make sure you and your peer both use the same name, i.e. that your local ID and the peer ID your partner configures for you are identical.

Phase 1: Local Certificate

This field enables you to select one of your own certificates for authentication. It shows the index number of this certificate and the name under which it is saved. This field is only shown for authentication settings based on certificates and indicates that a certificate is essential.

Phase 1: CA Certificates

Here you can enter a list of additional ➤➤ **CA** certificates that are to be accepted for this profile. Entries are separated by commas. This makes it possible, for example, to transfer a CA certificate even for self-signed certificates.

If the CA certificate contains no Certificate Revocation List (CRL) or no CRL distribution point and no certificate server is configured on the gateway, the variable ***NOCRLS*** is set to "True". Certificates from this CA are not checked for validity.

Phase 1: NAT Traversal

NAT Traversal (NAT-T) allows the creation of IPSec tunnels across one or more gateways that have Network Address Translation activated.

Without NAT-T there may be incompatibilities between IPSec and NAT (cf. RFC 3715, section 2). These especially constrict the creation of an IPSec tunnel from a host inside a LAN and behind a NAT gateway to another host or another gate-

way outside the LAN. NAT-T allows establishing such tunnels without any conflicts: the IPSec Daemon automatically detects active NAT and uses NAT-T.

The configuration of NAT-T is as simple as activating or deactivating it in the settings of Phase 1 profiles for the global profile (in ***IPSEC ➜ IKE (PHASE 1) DEFAULTS: EDIT***, see "Phase 1: NAT Traversal" on page 58) or peerspecific (in ***CONFIGURE PEERS ➜ ADD/EDIT ➜ PEER SPECIFIC SETTINGS ➜ IKE (PHASE 1) DEFAULTS: EDIT***).

In ***CONFIGURE PEERS ➜ ADD/EDIT ➜ PEER SPECIFIC SETTINGS ➜ IKE (PHASE 1) DEFAULTS: EDIT*** you can choose from three values for the field ***NAT-TRAVERSAL***:

- *default* - If you choose this value, the gateway uses the value chosen for the global default profile (see "Phase 1: NAT Traversal" on page 58).
- *enabled* - NAT-T is activated in this profile.
- *disabled* - NAT-T is deactivated in this profile.

When configuring an IPSec connection by means of the HTML Wizard or by means of the Setup Tool IPSec Wizard, NAT-T is activated (*enabled*). The Setup Tool IPSec Wizard, however, does not change the the NAT-T settings of an already existing default profile

Note

If you want to allow IPSec connections starting with the gateway as well as connections starting with a host inside the LAN, you must remove such entries pertaining to IKE traffic from the ***IPNATOUTTABLE***. Otherwise all IKE sessions will be directed to the same internal IP address, and only the session initiated last is really established.

Deleting the NAT entries, however, has the effect that you may experience difficulties with IPSec connections from the gateway to other hosts or gateways which do not support NAT-T, since the source port of the IKE connection is now changed by NAT.

3.2.3 Submenu IPSec (Phase 2) Profile

You can define profiles for phase 2 of the tunnel setup just as for phase 1.

The configuration is set in the ***CONFIGURE PEERS*** ➜ ***APPEND/EDIT*** ➜ ***PEER SPECIFIC SETTINGS*** ➜ ***IPSEC (PHASE 2) PROFILE: EDIT*** ➜ ***ADD/EDIT*** menu:

```
VPN Access 25 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
```

The menu contains the following fields:

Field	Description
Description (Idx 0)	Here you enter the desired description of the profile. The maximum length of the entry is 255 characters.
Proposal	Information on these parameters can be found in "Proposal, Lifetime, Use PFS..." on page 36
Lifetime	
Use PFS	

Field	Description
Heartbeats	Here you select whether and in what way IPSec heartbeats are used. Bintec has implemented an IPSec heartbeat to determine whether or not a Security Association (SA) is still valid. This function sends and receives signals according to the configuration. If these signals are not received, the SA is discarded as invalid. Possible settings: ■ *default* (default value) - The gateway uses the setting of the default profile. ■ *none* - The gateway sends and expects no heartbeat. ■ *expect* - The gateway expects a heartbeat from the peer, but does not send one itself. ■ *send* - The gateway expects no heartbeat from the peer, but sends one itself. ■ *both* - The gateway expects a heartbeat from the peer and sends one itself. For devices from the **VPN Access** line, heartbeats are configured separately for phase 1 and phase 2. If interoperability with older software is to be assured, the same values must be configured for phase 1 and phase 2.

Field	Description
Propagate PMTU	Here you select whether or not the PMTU (Path Maximum Transfer Unit) is to be propagated during phase 2. Possible settings: ■ *default* (default value) - The gateway uses the setting of the default profile. ■ *no* - The Path Maximum Transfer Unit is not transferred (default value). ■ *yes* - The Path Maximum Transfer Unit is transferred.

Table 3-12: ***IPSec ➜ Configure Peers ➜ APPEND/EDIT ➜ Peer specific Settings ➜ IPSec (Phase 2) Profile: edit ➜ ADD/EDIT***

The ***View Proposals*** menu is used only for listing the available proposals, as for phase 1 proposals. The ***Edit Lifetimes*** menu does not differ from that described in "Phase 1: Lifetime" on page 27.

3.2.4 Proposal, Lifetime, Use PFS...

The fields of the *IPSec (Phase 2) Profile: edit* ➜ *ADD/EDIT* menu described below need a more detailed explanation.

Phase 2: Proposal

This field enables you to select any combination of IPSec protocol, ➤➤ **encryption** algorithm and/or message hash algorithm. The elements of these potential combinations are listed in the tables below:

IPSec Protocol	Description
ESP (Encapsulated Security Payload)	➤➤ **ESP** offers payload encryption and authentication.

IPSec Protocol	Description
AH (Authentication Header)	➤➤ **AH** offers only authentication, no payload encryption. If you select a combination that uses the AH protocol, *none* is shown as encryption algorithm, e.g. *(AH (none, MD5)).*

Table 3-13: IPSec protocols

In addition to encryption and authentication, Bintec's IPSec implementation supports ➤➤ **compression** of the IP payload with ➤➤ **IPComP** (IP Payload Compression Protocol). IP Payload Compression is a protocol for reducing the size of IP datagrams. This protocol increases the overall communication performance between a pair of intercommunicating hosts/gateways ("nodes"). It compresses the datagrams, provided the nodes have sufficient computing power, by using either CPU power or a compression coprocessor, and communication takes place over slow or faulty connections.

The IP Payload Compression is especially useful if ➤➤ **IP** datagrams are encrypted. The encryption of IP datagrams ensures that the data are of a random nature, which means compression at lower protocol levels (e.g. PPP Compression Control Protocol [RFC1962]) has no effect. If both compression and encryption are required, compression must be carried out before encryption.

For all IPSec proposals in which no particular IPComP setting is defined, IPComP is enabled. This means that the gateway accepts all proposals during SA negotiation, regardless of whether or not these propose the use of IPComP. If the local PC initiates the negotiation, it proposes the use of IPComP as preferred proposal, but allows the answering PC to select a proposal without IPComP.

You can change this by selecting an IPSec proposal that defines one of the following settings for ➤➤ **IPComP**:

IPComp Option	Description
no Comp	Your gateway accepts no SAs that define the use of IPComp. If the peer is configured so that its or your gateway proposes IPComP, the IPSec SA negotiation fails and no connection is set up.
force Comp	Your gateway requests that IPComP can be agreed in IPSec SA negotiation. If the peer does not accept this, no connection is set up.

Table 3-14: IPComP options for IPSec proposals

As the major encryption and hash algorithms have already been described, they are only listed here. Only the NULL algorithm is not available in phase 1:

Algorithms	Description
Blowfish	Descriptions of the encryption algorithms can be found in table “Encryption algorithms,” on page 26.
3DES	
DES	
CAST	
Twofish	
Rijndael	
NULL	The NULL “algorithm” does not encrypt the IP packets, but is necessary in case IP packets need authentication by the ESP protocol without encryption.

Table 3-15: Phase 2 encryption algorithms

The following hash algorithms are available:

Algorithms	Description
MD5	Descriptions of the message hash algorithms can be found in table “Message hash algorithms,” on page 27.
SHA1	
NULL	If the NULL "algorithm" is used for authentication, ESP creates no message hash and the payload is only encrypted.

Table 3-16: Message hash algorithms in phase 2

Note

Note that the NULL algorithm in a single proposal can be defined either only for encryption or only for authentication, but not for both.

Note that RipeMD 160 and Tiger 192 are not available for message hashing in phase 2.

A phase 2 proposal, for example, would thus appear as follows:

Example values	Meaning
1 (ESP(Blowfish, MD5))	IP packets are processed using the ➤➤ **ESP** protocol, Blowfish encryption and MD5 message hash.
10 (ESP(NULL, SHA1))	IP packets are processed using the ESP protocol; the NULL encryption and SHA 1 are used to create the message hash.
16 (AH(none, MD5))	IP packets are processed using the AH protocol, without encryption and with MD5 as message hash algorithm.

Table 3-17: Examples of ***PHASE 2: PROPOSALS***

Phase 2: Lifetime

Information on the lifetime of the proposal can be found at “Phase 1: Lifetime” on page 27. If you would like to define a certain IPSec SA lifetime for this peer, you can do this in the ***EDIT LIFETIME*** menu.

Use PFS

As PFS (Perfect Forward Secrecy) requires another Diffie-Hellman key calculation to create new encryption material, you must select the exponentiation features. If you activate PFS, the options are the same as for the configuration in ***PHASE 1: GROUP*** ("Phase 1: Group" on page 29). PFS is used to protect the keys of a re-encrypted phase 2 SA, even if the keys of the phase 1 SA have become known.

3.2.5 Submenu Select Different Traffic List

This menu is only available if you configure a peer that is based on traffic lists and not on a virtual interface.

This menu shows the traffic lists configured for this peer. If you have configured more than one traffic list, you can select which list is to be activated. A list of all available traffic lists is shown and you can select from this as described in the help function of the menu window.

3.3 Submenu Traffic List Settings

This menu is for creating the rules for handling the data traffic to the peer. You can create or change a traffic list entry.

The menu window that opens has the following structure in both cases (if you change an existing entry, the values for this entry are shown):

```
VVPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IPSEC][PEERS][EDIT][TRAFFIC][ADD]: Edit Traffic Entry        MyGateway

Description:


     Protocol:      don't-verify

     Local:
          Type: net   Ip:                / 0

     Remote:
          Type: net   Ip:                / 0


     Action:        pass

     Profile          default              edit >


                SAVE                                  CANCEL
```

The following values are possible in the fields of this menu:

Field	Description
Description	Enter a description that indicates what kind of rule you have defined.
Protocol	Here you can define whether the data traffic planned for this rule is only applied to the packets of a certain protocol. You can choose between defining a protocol and the option *don't-verify*; the latter means that the protocol is not used as filter criterion.
Local: Type	Enter the local address settings. Details can be found below in table "Local/Remote: Type," on page 43.

Field	Description
Remote: Type	Enter the address settings for the remote station. The options are largely identical to the options in the ***LOCAL: TYPE*** field, with one exception: The *own* option is not available, but the *peer* option is offered instead. This is only relevant for peer configuration.
Action	Here you can select between three options. ■ *pass* ■ *drop* ■ *protect* Details can be found below in table “Action,” on page 44.
Profile	Only for ***ACTION*** = *protect*. Here you select an IPSec profile to be used for encryption of the data traffic. The possible settings are the same as those in the menu described in “Submenu IPSec (Phase 2) Profile” on page 33.

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

Local/Remote: Type

The following options are available in the ***LOCAL/REMOTE: TYPE*** field:

Description	Meaning
host	Enter the ➤➤ **IP address** of a single PC that is to be covered by this rule. If you have selected certain protocols to limit the data traffic concerned, you may be requested to enter a ➤➤ ***PORT*** number. This only applies to UDP and TCP.

Description	Meaning
net	Enter the IP address of a network and the associated ➤➤ netmask that are to be covered by this rule. The command prompt for the netmask appears automatically if you select *net*. It is separated from the command prompt for the IP address by the character "/". You may also be requested to enter a ***PORT*** number here.
range	Enter an IP address range that is to be covered by this rule. The command prompt changes automatically so that you can enter two IP addresses separated by a "-". You may also be requested to enter a ***PORT*** number here.
dhcp	Only for ***REMOTE: TYPE***. The remote gateway obtains its IP configuration via ➤➤ **DHCP**.
own/peer	If you select this option, it is assumed automatically that the dynamic IP address of the gateway (if applicable) is covered by this rule. In this case no further settings are necessary.

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

Action The ***ACTION*** field has the following options:

Description	Meaning
pass	This option enables certain IPSec packets to pass through unchanged.
drop	This option discards all packets that match the configured filters.

Description	Meaning
protect	The data traffic is encrypted and/or authenticated in accordance with the selected profile.

Table 3-20: ***ACTION***

3.4 Submenu Interface IP Settings

This menu is visible if you have selected *yes* **for the *VIRTUAL INTERFACE* field in the *IPSEC* ➜ *CONFIGURE PEERS* ➜ *APPEN/EDIT* menu. It permits configuration of the IP parameters of the virtual interface.**

The settings for the virtual IPSec interface are made in the ***BASIC IP SETTINGS***, ***MORE ROUTING*** and ***ADVANCED SETTINGS*** menus. These correspond to the IP menus described in the chapter **WAN Partner**. The ***MORE ROUTING*** menu is only visible if the basic settings have been made in the Advanced Settings menu.

4 Submenu Post IPSec Rules

The *POST IPSEC RULES* submenu is described below.

You must configure post IPSec rules in exactly the same way as you configure pre IPSec rules, which apply to the whole data traffic before IPSec SAs are used. Post IPSec rules are used after a packet has passed the peer traffic lists, i.e. in case no entries in the traffic list matched.

If your configuration is ideally set up, you may possibly only need to configure a single post IPSec rule, as all packets that must be discarded or allowed to pass in plain language are handled as per the pre IPSec rules and all packets that must be protected are handled as per the peer traffic lists. The only decision you therefore need to make here is whether you discard the "remaining" packets or allow them to pass. This decision is made by selecting a value for the ***WHAT TO DO WITH ANYTHING THAT DIDN'T MATCH*** field, which you will find in the first window of the ***IPSEC*** ➜ ***POST IPSEC RULES*** menu.

This field can have the following values:

Description	Meaning
drop it	All packets that do not match one of the IPSec rules are discarded after IPSec has been applied.
let pass	Alternatively, all packets that cannot be covered by the IPSec rules are allowed to pass.

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

4.1 Submenu APPEND/EDIT

Post IPSec rules are either edited or added in the ***IPSEC*** ➜ ***POST IPSEC RULES*** ➜ ***APPEND/EDIT*** menu. The menu window that opens has the following

structure in both cases (if you edit an existing entry, the values for this entry are shown):

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IPSEC][POST IPSEC TRAFFIC][ADD]: Edit Traffic Entry          MyGateway

Description:


     Protocol:      don't-verify

     Local:
          Type: net   Ip:                / 0

     Remote:
          Type: net   Ip:                / 0


     Action:        pass


                    SAVE                                  CANCEL
```

The fields in this menu can have the following values:

Field	Description
Description	Enter a description that indicates what kind of rule you have defined.
Protocol	Here you can define whether the data traffic planned for this rule is only to be applied to the packets of a certain protocol. You can choose between defining a protocol and the option *don't-verify*; the latter means that the protocol is not used as filter criterion.
Local: Type	Enter the local address settings. Details can be found below in table "Local/Remote: Type," on page 48.

Field	Description
Remote: Type	Enter the address settings for the remote station. The options are largely identical to the options in the ***LOCAL: TYPE*** field, with one exception: The *own* option is not available, but the *peer* option is offered instead. This is only relevant for peer configuration.
Action	Here you can select between two options: ■ *pass*: This option enables certain IPSec packets to pass through unchanged. ■ *drop*: This option discards all packets that match the configured filters.

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

LOCAL/REMOTE: TYPE The following options are available in the ***LOCAL/REMOTE: TYPE*** field:

Description	Meaning
host	Enter the IP address of a single PC that is to be covered by this rule. If you have selected certain ➤➤ **protocols** to limit the data traffic concerned, you may be requested to enter a ***PORT*** number. This applies only to ➤➤ **UDP** and ➤➤ **TCP**.
net	Enter the ➤➤ **IP address** of a network and the associated netmask that are to be covered by this rule. The command prompt for the ➤➤ **netmask** appears automatically if you select *net*. It is separated from the command prompt for the IP address by the character "/". You may also be requested to enter a ***PORT*** number here.

Description	Meaning
range	Enter an IP address range that is to be covered by this rule. The command prompt changes automatically so that you can enter two IP addresses separated by a "-". You may also be requested to enter a ***PORT*** number here.
dhcp	Only for ***REMOTE: TYPE***. The remote gateway obtains its IP configuration via ➤➤ **DHCP**.
own/peer	If you select this option, it is assumed automatically that the dynamic IP address of the gateway (if applicable) is covered by this rule. In this case no further settings are necessary. This entry can be selected here, but has no function for the post IPSec rules. It is necessary for peer configuration (see “Submenu Traffic List Settings” on page 40).

Table 4-3: ***LOCAL/REMOTE: TYPE***

5 Submenu IKE (Phase 1) Defaults

The *IKE (PHASE 1) DEFAULTS: EDIT* submenu is described below.

The menu for configuration of a global phase 1 profile is accessible via the ***IPSEC*** ➜ ***APPEND/EDIT*** ➜ ***IKE (PHASE 1) DEFAULTS: EDIT*** ➜ ***ADD/EDIT*** menu:

```
VPN Access 25 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       :
   Nat-Traversal         :  enabled

   View Proposals >
   Edit Lifetimes >

                         SAVE                          CANCEL
```

The menu contains the following fields:

Field	Description
Description	Here you enter the desired description of the profile. The maximum length of the entry is 255 characters.
Proposal	Information on these parameters: see “Proposal, Lifetime, Group...” on page 51
Lifetime	
Group	
Authentication Method	
Mode	

Field	Description
Heartbeats	Here you select whether and in what way IPSec heartbeats are used. Bintec has implemented an IPSec heartbeat to determine whether or not a Security Association (SA) is still valid. This function sends and receives signals according to the configuration. If these signals are not received, the SA is discarded as invalid. Possible settings: ■ *default* - The gateway uses the setting of the profile created by the IPSec Wizard. ■ *none* - The gateway sends and expects no heartbeat. ■ *expect* - The gateway expects a heartbeat from the peer, but does not send one itself. ■ *send* - The gateway expects no heartbeat from the peer, but sends one itself. ■ *both* - The gateway expects a heartbeat from the peer and sends one itself. For devices from the **VPN Access** line, heartbeats are configured separately for phase 1 and phase 2. If interoperability with older software is to be assured, the same values must be configured for phase 1 and phase 2.
Block Time	Here you define how long a peer is blocked for tunnel setups after a phase 1 tunnel setup has failed. This affects only locally initiated setup attempts. Possible values are *-1* to *86400* (seconds); *-1* (default) means the value in the default profile is used and *0* means that the peer is never blocked.

Field	Description
Local ID	For information on these parameters see "Proposal, Lifetime, Group..." on page 51
Local Certificate	
CA Certificates	
Nat-Traversal	

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

5.1 Proposal, Lifetime, Group...

The fields of the *IKE (Phase 1) Profile: edit* ➜ *ADD/EDIT* menu described below need a more detailed explanation.

Phase 1: Proposal

In this field you can select any combination of ➤➤ **encryption** and message hash algorithms for IKE phase 1 for your gateway. The combination of six encryption algorithms and four message hash algorithms gives 24 possible values in this field.

The available encryption and message hash algorithms are listed in the two tables below:

Algorithm	Description
Blowfish	➤➤ **Blowfish** is a very secure and fast algorithm. Twofish can be regarded as the successor to Blowfish.
3DES	➤➤ **3DES** is an extension of the DES algorithm with an effective key length of 112 bits, which is rated as secure. It is the slowest algorithm currently supported.
DES	➤➤ **DES** is an older encryption algorithm, which is rated as weak due to its small effective length of 56 bits.

Algorithm	Description
CAST	➤➤ **CAST** is also a very secure algorithm, a little slower than Blowfish, but faster than 3DES.
Twofish	➤➤ **Twofish** was a final candidate for the AES (Advanced Encryption Standard). It is rated as just as secure as Rijndael (AES), but is slower.
Rijndael	Rijndael has been nominated as AES due to its fast key set-up, low memory requirements, high level of security against attacks and general speed.

Table 5-2: Encryption algorithms

The available ➤➤ **hash** algorithms are listed below:

Algorithm	Description
MD5 (Message Digest #5)	➤➤ **MD5** is an older hash algorithm. It is used with 96 bits digest length for IPSec.
SHA1 (Secure Hash Algorithm #1)	➤➤ **SHA1** is a hash algorithm developed by the NSA (United States National Security Association). It is rated as secure, but is slower than MD5. It is used with 96 bits digest length for IPSec.
RipeMD 160	➤➤ **RipeMD 160** is a cryptographic 160-bit hash algorithm. It is used as a secure replacement for MD5 and RipeMD.
Tiger 192	➤➤ **Tiger 192** is a relatively new and very fast algorithm.

Table 5-3: Message hash algorithms

Note

Note that the description of the encryption and authentication or the hash algorithms is based on the author's knowledge and opinion at the time of creating this User's Guide. Particularly the quality of the algorithms is subject to relative aspects and may change due to mathematical or cryptographic developments.

VIEW PROPOSALS The ***VIEW PROPOSALS*** submenu provides an overview of the proposals created by the IPSec Wizard:

```
VPN Access 25 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
```

This menu is for information purposes only. Configuration is not possible.

Phase 1: Lifetime

This field shows the lifetime that may expire before a phase 1 key must be renewed with another Diffie-Hellman key calculation. This can be configured either as a value in seconds, as a processed amount of data (in kB) or as a combination of both. The default value is *900 sec/11000 kB,* which means the key is renewed when either 900 seconds have elapsed or 11000 kB of data have been processed, depending on which event occurs first. If you have configured additional lifetime values, you can select from these here.

If you decide to configure additional lifetime values, you can do this in the ***EDIT LIFETIMES*** menu. The following menu mask is offered:

```
VPN Access 25 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
```

The menu contains the following fields:

Field	Description
Lifetime Restriction Based On	Select the criterion for the end of the key lifetime, possible values are: ■ *Time* and *Traffic* ■ *Time* ■ *Traffic* One or both of the following fields are shown, depending on your selection.
Seconds	Enter the lifetime for phase 1 key in seconds. The value can be any whole number value up to a length of 32 bits.
Kb	Enter the lifetime for phase 1 key as amount of data processed in kB. The value can be any whole number value up to a length of 32 bits.

Field	Description
Matching Policy	Here you can select how strictly the gateway observes the configured lifetime. Possible settings: ■ *loose* - The gateway accepts and uses any lifetime suggested in the negotiation (default value). ■ *strict* - The gateway accepts and uses only the configured lifetime. The phase 1 negotiation fails in the event of deviation. ■ *notify* - The gateway accepts all proposed values that are larger than the configured value, but uses its own smaller value itself and notifies the peer accordingly.

Table 5-4: ***LIFETIME***

Phase 1: Group

The group defines the parameter set used as the basis for the Diffie-Hellman key calculation during phase 1. "MODP" as supported by Bintec gateways stands for "modular exponentiation". Three different settings can be selected: 768, 1024 or 1536 bits.

The field can have the following values:

Description	Meaning
1 (768-bit MODP)	During the Diffie-Hellman key calculation, modular exponentiation at 768 bits is used to create the encryption material.
2 (1024-bit MODP)	During the Diffie-Hellman key calculation, modular exponentiation at 1024 bits is used to create the encryption material.

Description	Meaning
5 (1536-bit MODP)	During the Diffie-Hellman key calculation, modular exponentiation at 1536 bits is used to create the encryption material.
none	The gateway uses no particular exponentiation after the lifetime expires, but proceeds as for the initial tunnel setup.
default	The gateway uses the setting of the profile created by the IPSec Wizard.

Table 5-5: ***PHASE 1: GROUP***

Phase 1: Authentication method

This field enables you to change the authentication method for the global profile:

Description	Meaning
Preshared Keys	If you do not use certificates for the authentication, you can select *Preshared Keys*. These are configured in the peer configuration in the ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***APPEND/EDIT*** menu.
DSA Signatures	Phase 1 key calculations are authenticated using the ➤➤ **DSA** algorithm.
RSA Signatures	Phase 1 key calculations are authenticated using the ➤➤ **RSA** algorithm.
RSA Encryption	In RSA encryption the ID payload is also encrypted for additional security.
default	The gateway uses the setting of the profile created by the IPSec Wizard.

Table 5-6: ***AUTHENTICATION METHOD***

Phase 1: Mode

The Mode field shows the currently configured phase 1 mode and enables you to change the settings:

Description	Meaning
id_protect	This mode (also designated Main Mode) requires six messages for a Diffie-Hellman key calculation and thus for configuring a secure channel, over which the IPSec SAs can be negotiated. A condition is that both peers have static IP addresses if preshared keys are used for authentication. This limitation does not apply if IPSec callbacks are used. see “Submenu IPSec Callback” on page 14
aggressive	The Aggressive Mode is necessary if one of the peers does not have a static IP address and preshared keys are used for authentication; it requires only three messages for configuring a secure channel.
default	The gateway uses the setting of the profile created by the IPSec Wizard.
id-protect-only	The gateway accepts only the ID Protect Mode in the negotiation. If the peer suggests another mode, the negotiation fails.
aggressive-only	The gateway accepts only the Aggressive Mode in the negotiation. If the peer suggests another mode, the negotiation fails.

Table 5-7: ***MODE***

Phase 1: Local ID

This is the ID you assign to your gateway. If you leave this field empty, the gateway selects the default values. These are:

- For authentication with preshared keys: the local IP address as shown in the ***IPSECPEERLOCALADDRESS*** field in the ***IPSECPEERTABLE***.

- For authentication with ➤➤ **certificate**: the first alternative subject name indicated in the certificate or, if none is shown, the subject name of the certificate.

Note

If you use certificates for authentication and your certificate contains alternative subject names (see "Request Certificate" on page 71), you must make sure the gateway selects the first alternative subject name by default. Make sure you and your peer both use the same name, i.e. that your local ID and the peer ID your partner configures for you are identical.

Phase 1: Local Certificate

This field enables you to select one of your own certificates for authentication. It shows the index number of this certificate and the name under which it is saved. This field is only shown for authentication settings based on certificates and indicates that a certificate is essential.

Phase 1: CA Certificates

Here you can enter a list of additional ➤➤ **CA** certificates that are to be accepted for this profile. Entries are separated by commas. This makes it possible, for example, to transfer a CA certificate even for self-signed certificates.

If the CA certificate contains no Certificate Revocation List (CRL) or no CRL distribution point and no certificate server is configured on the gateway, the variable ***NoCRLs*** is set to "True". Certificates from this CA are not checked for validity.

Phase 1: NAT Traversal

NAT Traversal (NAT-T) allows the creation of IPSec tunnels across one or more gateways that have Network Address Translation activated.

Without NAT-T there may be incompatibilities between IPSec and NAT (cf. RFC 3715, section 2). These especially constrict the creation of an IPSec tunnel from a host inside a LAN and behind a NAT gateway to another host or another gateway outside the LAN. NAT-T allows establishing such tunnels without any conflicts: the IPSec Daemon automatically detects active NAT and uses NAT-T.

The configuration of NAT-T is as simple as activating or deactivating it in the settings of Phase 1 profiles for the global profile (in ***IPSEC ➜ IKE (PHASE 1) DEFAULTS: EDIT***) or peerspecific (in ***CONFIGURE PEERS ➜ ADD/EDIT ➜ PEER***

SPECIFIC SETTINGS ➜ IKE (PHASE 1) DEFAULTS: EDIT, see "Phase 1: NAT Traversal" on page 32).

In ***IPSEC ➜ IKE (PHASE 1) DEFAULTS: EDIT*** you can choose from two values for the field ***NAT-TRAVERSAL***:

- *enabled* - NAT-T is activated in this profile.
- *disabled* - NAT-T is deactivated in this profile.

When configuring an IPSec connection by means of the HTML Wizard or by means of the Setup Tool IPSec Wizard, NAT-T is activated (*enabled*). The Setup Tool IPSec Wizard, however, does not change the the NAT-T settings of an already existing default profile.

Note

If you want to allow IPSec connections starting with the gateway as well as connections starting with a host inside the LAN, you must remove such entries pertaining to IKE traffic from the ***IPNATOUTTABLE***. Otherwise all IKE sessions will be directed to the same internal IP address, and only the session initiated last is really established.

Deleting the NAT entries, however, has the effect that you may experience difficulties with IPSec connections from the gateway to other hosts or gateways which do not support NAT-T, since the source port of the IKE connection is now changed by NAT.

6 Submenu IPSec (Phase 2) Defaults

The *IKPSEC (PHASE 2) DEFAULTS* submenu is described below.

You can define profiles for phase 2 of the tunnel setup just as for phase 1.

The configuration is set in the ***IPSEC*** ➜ ***IPSEC (PHASE 2) DEFAULTS: EDIT*** ➜ ***ADD/EDIT*** menu:

```
VPN Access 25 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
```

The menu contains the following fields:

Field	Description
Description (Idx 1)	Here you enter the desired description of the profile. The maximum length of the entry is 255 characters.
Proposal	Information on these parameters can be found in “Proposal, Lifetime, Use PFS...” on page 63
Lifetime	
Use PFS	

Field	Description
Heartbeats	Here you select whether and in what way IPSec heartbeats are used. Bintec has implemented an IPSec heartbeat to determine whether or not a Security Association (SA) is still valid. This function sends and receives signals according to the configuration. If these signals are not received, the SA is discarded as invalid. Possible settings: ■ *default* - The gateway uses the setting of the default profile. ■ *none* - The gateway sends and expects no heartbeat. ■ *expect* - The gateway expects a heartbeat from the peer, but does not send one itself. ■ *send* - The gateway expects no heartbeat from the peer, but sends one itself. ■ *both* - The gateway expects a heartbeat from the peer and sends one itself. For devices from the **VPN Access** line, heartbeats are configured separately for phase 1 and phase 2. If interoperability with older software is to be assured, the same values must be configured for phase 1 and phase 2.

Field	Description
Propagate PMTU	Here you select whether or not the PMTU (Path Maximum Transfer Unit) is to be propagated during phase 2. Possible settings: ■ *default* - The gateway uses the setting of the default profile. ■ *no* - The Path Maximum Transfer Unit is not transferred (default value). ■ *yes* - The Path Maximum Transfer Unit is transferred.

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

The ***View Proposals*** menu is used only for listing the available proposals, as for phase 1 proposals. The ***Edit Lifetimes*** menu does not differ from that described in "Phase 1: Lifetime" on page 53.

6.1 Proposal, Lifetime, Use PFS...

The fields of the *IPSec (Phase 2) Profile: edit* ➜ *ADD/EDIT* menu described below need a more detailed explanation.

Phase 2: Proposal

This field enables you to select any combination of IPSec protocol, ➤➤ **encryption algorithm** and/or message hash algorithm. The elements of these potential combinations are listed in the tables below:

IPSec Protocol	Description
ESP (Encapsulated Security Payload)	➤➤ **ESP** offers payload encryption and authentication.

IPSec Protocol	Description
AH (Authentication Header)	➤➤ **AH** offers only authentication, no payload encryption. If you select a combination that uses the AH protocol, *none* is shown as encryption algorithm, e.g. *(AH (none, MD5)).*

Table 6-2: IPSec protocols

In addition to encryption and authentication, Bintec's IPSec implementation supports ➤➤ **compression** of the IP payload with ➤➤ **IPComP** (IP Payload Compression Protocol). IP Payload Compression is a protocol for reducing the size of IP datagrams. This protocol increases the overall communication performance between a pair of intercommunicating hosts/gateways ("nodes"). It compresses the datagrams, provided the nodes have sufficient computing power, by using either CPU power or a compression coprocessor, and communication takes place over slow or faulty connections.

The IP Payload Compression is especially useful if IP datagrams are encrypted. The encryption of IP datagrams ensures that the data are of a random nature, which means compression at lower protocol levels (e.g. PPP Compression Control Protocol [RFC1962]) has no effect. If both compression and ➤➤ **encryption** are required, compression must be carried out before encryption.

For all IPSec proposals in which no particular IPComP setting is defined, IPComP is enabled. This means that the gateway accepts all proposals during SA negotiation, regardless of whether or not these propose the use of IPComP. If the local PC initiates the negotiation, it proposes the use of IPComP as preferred proposal, but allows the answering PC to select a proposal without IPComP.

You can change this by selecting an IPSec proposal that defines one of the following settings for ➤➤ **IPComP**:

IPComP Option	Description
no Comp	Your gateway accepts no SAs that define the use of IPComP. If the peer is configured so that its or your gateway proposes IPComP, the IPSec SA negotiation fails and no connection is set up.
force Comp	Your gateway requests that IPComP can be agreed in IPSec SA negotiation. If the peer does not accept this, no connection is set up.

Table 6-3: IPComP options for IPSec proposals

As the major encryption and hash algorithms have already been described, they are only listed here. Only the NULL algorithm is not available in phase 1:

Algorithms	Description
Blowfish	Descriptions of the encryption algorithms can be found in table “Encryption algorithms,” on page 52.
3DES	
DES	
CAST	
Twofish	
Rijndael	
NULL	The NULL “algorithm” does not encrypt the IP packets, but is necessary in case IP packets need authentication by the ESP protocol without encryption.

Table 6-4: Phase 2 encryption algorithms

The following hash algorithms are available:

Algorithms	Description
MD5	Descriptions of the message hash algorithms can be found in table “Message hash algorithms,” on page 52.
SHA1	
NULL	If the NULL "algorithm" is used for authentication, ESP creates no message hash and the payload is only encrypted.

Table 6-5: Message hash algorithms in phase 2

Note

Note that the NULL algorithm in a single proposal can be defined either only for encryption or only for authentication, but not for both.

Note that RipeMD 160 and Tiger 192 are not available for message hashing in phase 2.

A phase 2 proposal, for example, would thus appear as follows:

Example values	Meaning
1 (ESP(Blowfish, MD5))	IP packets are processed using the ESP protocol, Blowfish encryption and MD5 message hash.
10 (ESP(NULL, SHA1))	IP packets are processed using the ESP protocol; the NULL encryption and SHA 1 are used to create the message hash.
16 (AH(none, MD5))	IP packets are processed using the AH protocol, without encryption and with MD5 as message hash algorithm.

Table 6-6: Examples of ***PHASE 2: PROPOSALS***

Phase 2: Lifetime

Information on the lifetime of the proposal can be found at “Phase 1: Lifetime” on page 53. If you would like to define a certain IPSec SA lifetime for this peer, you can do this in the ***EDIT LIFETIME*** menu.

Use PFS

As PFS (Perfect Forward Secrecy) requires another Diffie-Hellman key calculation to create new encryption material, you must select the exponentiation features. If you activate PFS, the options are the same as for the configuration in ***PHASE 1: GROUP*** ("Phase 1: Group" on page 55). PFS is used to protect the keys of a re-encrypted phase 2 SA, even if the keys of the phase 1 SA have become known.

7 Submenu Certificate and Key Management

The ***CERTIFICATE AND KEY MANAGEMENT*** submenu is described below.

The ***CERTIFICATE AND KEY MANAGEMENT*** submenu provides access to the following submenus:

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

7.1 Submenu Key Management

The first menu window of ***CERTIFICATE AND KEY MANAGEMENT*** ➜ ***KEY MANAGEMENT*** shows information about the keys saved on your gateway:

```
VPN Access 25 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
```

This list contains a description of the key(s) and tells you the algorithm and key length used. You can also create new keys or request certificates for existing keys.

7.1.1 Key Creation

You can create a new key in the ***CERTIFICATE AND KEY MANAGEMENT*** ➜ ***KEY MANAGEMENT*** ➜ ***CREATE*** menu.

```
VPN Access 25 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
```

The menu enables you to configure the following parameters:

Field	Description
Description	Here you can enter the desired name for the key you are creating.
Algorithm	Here you can select one of the available algorithms. ➤➤ **RSA** and ➤➤**DSA** are available.

Field	Description
Key Size (Bits)	Here you can select the length of the key to be created. The possible values are from *512* to *4096* bits. Note that a key with a length of *512* bits could be rated as insecure, whereas a key of *4096* bits not only needs a lot of time to create, but also occupies a major share of the resources during IPSec processing. A value of *768* or more is, however, recommended and the default value is *1024 bits*.
RSA Public Exponent	(This field is only displayed if you are using the RSA algorithm.) The Public Exponent is part of the Public Key, which was created for RSA signatures and RSA encryption. If you do not receive any particular recommendation from your certification authority (CA), you can use the default value.

Table 7-1: ***IPSec → Certificate and Key Management → Key Management → CREATE***

7.1.2 Request Certificate

After you have created a key, you can request a certificate for this key by highlighting the relevant key and then pressing the "e" key on your keyboard. Alternatively, you can activate ***Request Cert*** and select the key you wish to certify.

If you request a certificate, the following submenu opens:

```
VPN Access 25 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
```

This menu contains the following fields:

Field	Description
Key to Enroll	Select the key you wish to certify.

Field	Description
Method	Here you select the way in which you want to request the certificate. Possible settings: ■ *SCEP* - The key is requested from a CA using the Simple Certificate Enrollment Protocol. ■ *Upload* - The gateway creates a PKCS#10 request for the key and this is sent to a CA server. The certificate must be imported into the gateway after it is issued. ■ *Show* - The gateway creates a PKCS#10 request and shows the result in a menu window.
CA Certificate	Only for ***METHOD*** = *SCEP*. Select the CA certificate of the certification authority (CA) from which you wish to request the certificate. If no CA certificates are available, the gateway will first download the CA certificate of the CA in question. It then continues with the enrollment process, provided no more important parameters are missing. In this case it returns to the ***REQUEST CERT*** menu. If the CA certificate contains no Certificate Revocation List (CRL) or a CRL distribution point and no certificate server is configured on the gateway, the variable ***NOCRLS*** is set to "True". Certificates from this CA are not checked for validity.

Field	Description
Autosave	Only for ***METHOD*** = *SCEP*. If you activate this option, the gateway automatically saves the various steps of the enrollment process. This is useful if the enrollment cannot be completed immediately or if the gateway must be rebooted. If the status has not been saved, the enrollment cannot be completed. As soon as the enrollment is completed and the certificate has been downloaded from the CA server, it is automatically saved in the gateway configuration. The selection options are *on* and *off*.
CA Domain	Only for ***METHOD*** = *SCEP*. Enter the ➤➤ **domain** name of the CA server to which the enrollment is sent, e.g. **enroll.ca.com**.
Password	Only for ***METHOD*** = *SCEP*. You may need a password from the certification authority to obtain certificates for your keys. Enter the password you received from the certification authority here.
Subject Name	Enter a subject name for the certificate you are requesting. The name you enter here must conform to the syntax for subject alternative names as per X.509.
Subject Alternative Names (optional)	Here you can enter additional information that can be used as subject name. You will find a list of the options in table “Subject Alternative Names,” on page 76 below.

Field	Description
State of Last Enrollment	Only for ***METHOD*** = *SCEP*. Shows the result of the last certificate request to the CA. This field cannot be edited.
Signing Algorithm to Use	Only for ***METHOD*** = *Upload*. Here you select the algorithm to be used for authenticating the certificate request. Possible settings: ■ *md5WithRSAEncryption* ■ *sha1WithRSAEncryption*.
Server	Not for ***METHOD*** = *Show*. Here you enter the ➤➤ **TFTP** server to which the certificate request is sent. You can enter either a resolvable host name or an IP address. Please note that you must not enter a protocol (like TFTP or HTTP) before the server address.
Certname/Filename	Not for ***METHOD*** = *Show*. Enter a name for the resulting certificate. For ***METHOD*** = *Upload* you can select whether the request is to be sent in *base64* or *binary* format.

Table 7-2: ***IPSEC ➜ CERTIFICATE AND KEY MANAGEMENT ➜ KEY MANAGEMENT ➜ REQUEST CERT***

The selection options for the ***SUBJECT ALTERNATIVE NAMES*** field are shown below. In the ***SUBJECT ALTERNATIVE NAMES – TYPE*** field you can select from various information types that can be used as subject alternative name. In the ***SUBJECT ALTERNATIVE NAMES – VALUE*** field you can enter the specific information you would like to provide. Three instances are available here; the default settings for the first two instances are the first IP address of your gateway and its ➤➤ **DNS** name.

The options for ***TYPE*** are:

Description	Meaning
IP	The ➤➤ **IP** address of your gateway is used as a subject alternative name.
DNS	A DNS name is used as subject alternative name (e.g.: MyGateway).
Email	An e-mail address is used as subject alternative name.
URI	A Uniform Resource Identifier is used as subject alternative name. URI is the addressing technique from which the URLs are derived. From a technical viewpoint, URLs such as HTTP:// and FTP:// are specific sub IDs of URIs.
DN	A DN (Distinguished Name) is used as subject alternative name.
RID	An RID (Registered Identity) is used as subject alternative name.

Table 7-3: Subject Alternative Names

7.2 Certificate Submenus

In the certificate submenus ***OWN CERTIFICATES***, ***CERTIFICATE AUTHORITY CERTIFICATES*** and ***PEER CERTIFICATES*** you can manage the certificates you need

for authentication methods that are based on ➤➤ **certificates** (e.g. DSA, RSA and RSA encryption).

Note

You generally only need to download a peer certificate in rare cases:

- If you have configured RSA encryption as authentication method, but have neither entered a CRL server nor saved a CRL statically on your gateway. Note that you create a major security gap if you do not enter a certificate server and have no statically configured CRLs available, as in this case certificates that have been blocked cannot be recognized automatically.
- If you do not receive the peer certificate during IKE negotiation. This is the case if sending certificates is disabled at the peer or no "Get Certificate Requests" are sent by the local PC. Both options can be set in the ***IPSec*** ➜ ***Advanced Settings*** menu by setting either ***Ignore Cert Request Payloads*** or ***Do not send Cert Request Payloads*** to *yes*.

The first menu window of all certificate submenus is almost identical:

```
VPN Access 25 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
```

The menu shows the ***Description***, all the possibly set ***Flags***, the ***Serial No.*** of the certificate in question and the data for the ***Subject Names***.

By highlighting an entry and confirming with ***ENTER***, you can open a window that shows the certificate and provides additional information about the window:

```
VPN Access 25 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
```

You cannot change the content of the certificate, but can make changes to the following data:

Field	Description
Description	Shows the description you entered on importing the certificate. You can now change this.
Type of Certificate	Here you can select between three types of certificate: ■ *Own Certificate* ■ *Certificate Authority* ■ *Peer Certificate* If you select *Certificate Authority* here, you must also indicate whether or not the certificate authority issues Certificate Revocation Lists (CRLs).

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

7.2.1 Certificate Import

Another submenu you can access from the first certificate menu (***CERTIFICATE AND KEY MANAGEMENT*** ➜ ***OWN CERTIFICATES***, ***CERTIFICATE AUTHORITY CERTIFICATES*** or ***PEER CERTIFICATES***) is the ***DOWNLOAD*** menu, which you can use to either download a certificate from a ➤➤ **TFTP** server or import into the Setup Tool by directly entering the certificate content.

This menu has the following structure:

```
VVPN Access 25 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
```

This menu contains the following fields:

Field	Description
Import a Certificate/CRL using:	Indicate how you wish to enter the certificate data: ■ *TFTP* ■ *Direct Input*
Type of Certificate	This field shows one of the following entries: *Certificate Authority, Own Certificate or Peer Certificate*. You cannot change this entry.

Field	Description
Please enter certificate data	Here you can enter (copy and paste) the content of the certificate you have received from the certification authority (CA) or your system administrator in the line provided for this purpose below this field. The line for entering the certificate data is only available if you previously selected *Direct Input*.
Server	Enter the TFTP server from which the certificate is to be downloaded. You can enter either an IP address or a resolvable host name. This command prompt appears only if you previously selected *TFTP*.
Name	Enter the name of the certificate to be downloaded (if you have selected *TFTP D*ownload) or which you have entered (if you have selected *Direct Input*). If you have downloaded the certificate via TFTP, this name is also used as file name.
auto/base64/binary	Select the type of coding, so that the gateway can decode the certificate. *auto* activates automatic code recognition. If downloading the certificate in *auto* mode fails, try with a certain type of coding.

Table 7-5: ***IPSec ➜ Certificate and Key Management ➜ Own Certificates ➜ DOWNLOAD***

For peer certificates you can also activate the ***Force trusted*** option. If ***Force trusted*** is activated, your Bintec gateway does not check the validity of the certificate with the certification authority.

7.3 Submenu Certificate Revocation Lists

Opening the Certificate Revocation Lists menu shows a list of the CRLs saved (Certificate Revocation Lists). The first menu window contains important information about the CRLs:

- the description you entered on downloading the CRL
- the issuer of the CRL (normally your certification authority)
- the serial number of the CRL
- the NumC (this is the number of certificate revocations contained in the CRL).

The menu has the following structure:

```
VPN Access 25 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
```

If you highlight an entry and confirm with ***ENTER***, a menu window opens with details of the CRL and you can change the description of the CRL in question. This window has the following structure:

```
VPN Access 25 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
```

You can also open the CRL ***DOWNLOAD*** menu from the first ***CERTIFICATE REVOCATION LISTS*** menu window. Here you can import the CRLs either via TFTP or by direct input. This process works in the same way as importing a certificate. Further details can be found in “Certificate Import” on page 79.

7.3.1 Submenu Certificate Servers

If you have entered certificate servers, these are listed in the first menu window of the ***CERTIFICATE SERVERS*** menu.

The following information is shown:

- the description you have entered for a certificate server
- the URL of the server
- the preference assigned to the server in question.

If you either highlight an entry and confirm with ***ENTER*** or select the ***ADD*** option, you enter the ***ADD/EDIT*** menu. Here you can either enter a new certificate server or change the settings of existing servers. Besides entering a ***DESCRIPTION*** and the ***URL*** of the server you can assign the server a ***PREFERENCE***. The gateway interrogates the certificate servers in the order of the preferences assigned to them, starting with *0*.

8 Submenu Advanced Settings

The *ADVANCED SETTINGS* submenu is described below.

The ***IPSEC*** ➜ ***ADVANCED SETTINGS*** menu is for adapting certain functions and features to the special requirements of your environment, i.e. mostly interoperability flags are set. The default values enable your system to work correctly to other Bintec gateways, so that you only need to change these values if you know special settings are necessary. These may be needed, for example, if the remote end operates with older IPSec implementations.

The ***ADVANCED SETTINGS*** menu is shown below:

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IPSEC][ADVANCED]: IPSec Configuration - Advanced Settings   MyGateway


  Ignore Cert Req Payloads :  no
  Don't Send Cert Req Payl. :  no
  Don't Send Cert Chains    :  no
  Don't Send CRLs           :  yes

  Don't Send Key Hash Payl. :  no
  Trust ICMP Messages       :  no
  Don't 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
```

The menu has the following fields and meanings:

Field	Description
Ignore Cert Req Payloads	Indicates whether or not ➤➤ **certificate** requests received by the remote end during the IKE are to be ignored. Possible values are *yes* or *no* (default value).

Field	Description
Don't Send Cert Req Payl.	Indicates whether or not payload is to be sent during IKE certificate requests. Possible values are *yes* or *no* (default value).
Don't Send Cert Chains	Indicates whether or not complete certificate chains are to be sent during IKE. Possible values are *yes* or *no* (default value). Select *yes* here, if you do not wish to send the peer the certificates of all levels from your level to the CA level.
Don't Send CRLs	Indicates whether or not CRLs are to be sent during IKE. Possible values are *yes* (default value) or *no*.
Don't Send Key Hash Payl.	Indicates whether or not key hash payload is sent during IKE. In the default setting, the public key hash of the remote end is sent together with the other authentication data. Only applies for ➤➤ **RSA** encryption; select *yes* to suppress this behavior. Possible values are *yes* or *no* (default value).
Trust ICMP Messages	Indicates whether or not the ➤➤ **ICMP** messages "Port Unreachable" and "Host Unreachable" are to be trusted during IKE. The ICMP messages "Port Unreachable" and "Host Unreachable" are only trusted if no datagrams have been received from the remote host during this negotiation. This means, if the local end receives the ICMP message "Port Unreachable" or "Host Unreachable" as first answer to the first packet of a new phase 1 negotiation, it ceases the negotiation immediately. Possible values are *yes* or *no* (default value).

Field	Description
Don't Send Initial Contact	Indicates whether or not IKE Initial Contact messages are also sent during IKE negotiations if no SAs with a peer exist. Possible values are *yes* or *no* (default value).
Sync SAs With Local Ifc	Ensures that all SAs are deleted whose data traffic was routed over an interface whose status has changed from *up* to *down*, *dormant* or *blocked*. Possible values are *yes* or *no* (default value).
Max. Symmetric Key Length	Indicates the maximum length of a key (in bits) that is accepted by the remote end. This limit prevents "denial-of-service" attacks in which the attacker asks for a huge key for an encryption algorithm that allows variable key lengths. The default value is *1024*.
Use Zero Cookies	Indicates whether or not zeroed ISAKMP cookies are to be sent. These are equivalent to the SPI (Security Parameter Index) in IKE proposals; as they are redundant, they are normally set to the value of the negotiation currently in progress. Alternatively, the gateway can use zeroes for all values of the cookie. Select *yes* for this option. Possible values are *yes* (default value) or *no*.
Cookies Size	Indicates the length in bytes of the zeroed SPI used in IKE proposals. This field is only effective if ***Use Zero ISAKMP Cookies*** is set to *yes*. The default value is *32*.
RADIUS Authentication	Here you can activate RADIUS authentication over IPSec. Possible values are *enabled* and *disabled* (default value).

Table 8-1: ***IPSec ➜ Advanced Settings***

9 Submenu Wizard

The *WIZARD* submenu is described below.

In the Wizard menu you can restart the IPSec Wizard of the Setup Tool, which you have already run through once at the start of the IPSec configuration. Although the Setup Tool does not force you to use the Wizard, the necessary profiles for phase 1 and phase 2 are not available without running through at least the non-interactive part of the Wizard.

When you select the IPSec menu from the Main Menu for the first time, the IPSec Wizard starts automatically. If you confirm that the Wizard is to run, the following window opens:

```
VPN Access 25 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
```

When you enter the Wizard menu for the first time, only two options are available: You can start the Wizard with ***START WIZARD*** or leave the Wizard menu with ***EXIT***. If you start the IPSec Wizard, you will be shown information about the

configuration steps in the window section below the heading for Configuration History:

```
VPN Access 25 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 settings)
+ Check default IPSec profile ...
  already configured (default settings)
+ 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
```

After starting the configuration using the IPSec Wizard, the following options are available for the ***WHAT TO DO?*** field:

Description	Meaning
clear config	This setting cancels all settings made during the configuration. After the configuration has been deleted, you should start the Wizard again. If the gateway already has public key pairs, these are not deleted, otherwise the validity of the existing ➤➤ **certificates** would be destroyed.
dump messages	The gateway saves the messages sent during the configuration, either locally or on a configured syslog host.

Description	Meaning
skip	This option enables you to skip a configuration step if it is not necessary (e.g. requesting a certificate when one is already available).
abort	This option is available for avoiding a necessary configuration step. The option ends the IPSec Wizard just like ***EXIT***, but you remain in the Wizard menu and can activate the Wizard again directly if necessary.
start (wizard)	This option either activates a specific operation that has not yet been executed or starts the Wizard from the beginning. It is only available if the Wizard configuration is still incomplete.

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

The IPSec Wizard step by step

The IPSec Wizard is not actually a menu, but a sequence of automatic routines. The Wizard guides you through the menus necessary for configuration. These do not differ from the menus that are also accessible from the ***IPSEC*** Main Menu. You can therefore adapt a configuration created with the Wizard to your needs at any time.

The Wizard runs through the following steps:

Step 1 (NAT settings) The Wizard checks whether ➤➤ **NAT** is activated on your gateway and adapts the settings if necessary so that a functioning IPSec configuration is assured and no data packets are discarded unnecessarily. If the Wizard makes changes to the NAT configuration, these are shown in the Configuration History.

Step 2 (creation of proposals) The Wizard assembles ➤➤ **encryption** and message hash algorithms into proposals. No configuration settings are made in this step; you can determine the proposals to be used later in the IPSec Main Menu or in the peer configuration. A default combination is selected during the Wizard configuration.

Step 3 (define authentication method) The Wizard requests the authentication method to be used. If you use preshared keys, proceed with step 8 and create a peer with the necessary password (the preshared key).

If you select a method based on ➤➤ **certificates**, the Wizard first creates a suitable key pair and continues with steps 4 to 7.

Step 4 (request certificate) The Wizard checks whether the gateway already has its own certificates installed for the available keys. If the Wizard has created a key pair, you are asked to request a certificate for this key.

If you want to request a certificate (you must have certain information available for this), the Wizard moves to the relevant menu ("Request Certificate" on page 71). After you have entered the necessary data you return to the Wizard menu.

Step 5 (own certificate) If you have either requested a certificate or skipped the relevant Wizard step, the Wizard asks if you want to import your own certificate. If you have not yet received your certificate, you can now end the Wizard and continue the configuration later. If you have requested your certificate using SCEP, it is saved by the gateway automatically as soon as the Certificate Authority has issued the certificate. In this case you can skip this step.

If you have requested the certificate manually, confirm this and the Wizard moves to the menu for certificate import, see "Certificate Submenus" on page 76. After you have entered the necessary data you return to the Wizard menu.

Step 6 (CA certificate) As soon as your certificate is installed on the gateway, the Wizard requests you to download a ➤➤ **CA** certificate. This is the certificate used by the CA that issued your certificate to authenticate itself. The Wizard changes to the relevant menu, see "Certificate Submenus" on page 76. After you have entered the necessary data you return to the Wizard menu.

Step 7 (CRL server / peer certificate) When both your certificate and the CA certificate are installed on the gateway, the Wizard requests you to enter a server from which Certificate Revocation Lists (CRLs) can be downloaded. This is necessary if the CA certificate does not indicate a CRL distribution point, but you have selected ➤➤ **RSA** encryption as authentication method.

If you want to enter a CRL server, the Wizard changes to the relevant menu, see "Submenu Certificate Servers" on page 82. After you have entered the necessary data you return to the Wizard menu.

If you do not enter a CRL server and no CRL distribution point is indicated in the CA certificate, but you have still selected RSA encryption as authentication method, the Wizard requests you to download a peer certificate. The Wizard changes to the relevant menu, see “Certificate Submenus” on page 76. After you have entered the necessary data you return to the Wizard menu.

Step 8 (peer) In the next step you are requested to configure an IPSec peer. The Wizard changes to the relevant menu, see “Submenu Configure Peers” on page 11. After you have entered the necessary data you return to the Wizard menu.

Step 9 (peer traffic / peer interface) When you have configured a peer, the Wizard requests you to specify the data traffic to be protected.

If you have configured the peer with a virtual interface, the Wizard changes to the menu for entering the peer IP settings, see “Submenu Interface IP Settings” on page 44. After you have entered the necessary data you return to the Wizard menu.

If you have configured the peer with traffic lists, the Wizard changes to the menu for defining a traffic list entry, see “Submenu Traffic List Settings” on page 40. After you have entered the necessary data you return to the Wizard menu.

Step 9 completes the IPSec Wizard configuration. The gateway now has a functioning IPSec configuration.

10 Submenu Monitoring

The *MONITORING* submenu is described below.

The ***IPSEC*** ➜ ***MONITORING*** submenu provides access to the following submenus:

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

IPSEC ➜ ***MONITORING*** is the last menu in the IPSec context. Here you can show the status of the global statistics, IKE Security Associations and IPSec Security Associations. The menu accordingly has three submenus, which are described in the following chapters.

10.1 Submenu Global Statistics

All the fields in the ***IPSEC*** ➜ ***MONITORING*** ➜ ***GLOBAL STATISTICS*** menu are read only, i.e. you can show the settings and statistics here, but cannot make any changes to the configuration.

The menu has the following structure (the values shown are only examples):

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[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
```

The meaning of the fields and their values is given below:

Field	Description
Peers Up	Shows the number of active peers (***OperStatus*** = *up*) from the number of configured peers.
Peers Dormant	Shows the number of inactive peers (***OperStatus*** = *dormant*).
Peers Blocked	Shows the number of blocked peers (***OperStatus*** = *blocked*).
SAs Phase 1	Shows the number of active phase 1 SAs (State = established) from the total number of phase 1 SAs.
SAs Phase 2	Shows the number of active phase 2 SAs (***State*** = *established*) from the total number of phase 2 SAs.

Field	Description
Packets In/Out	Shows the number of packets that have been processed in a certain way: ■ *Total*: The total number of processed packets. ■ *Passed*: The number of packets forwarded in plain language. ■ *Dropped*: The number of packets discarded. ■ *Protect*: The number of packets protected by IPSec. ■ *Error*: The number of packets in which errors occurred during processing.

Table 10-1: ***IPSec → Monitoring → Global Statistics***

10.2 Submenu IKE Security Associations

The next monitoring submenu (***IPSec*** ➜ ***Monitoring*** ➜ ***IKE Security Associations***) shows statistics for the IKE SAs. The menu has the following structure (the values shown are only examples):

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[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
```

The meaning of the characters in the ***TARSEH*** column (last column on the right below the help section of the menu window) is explained at the top of the menu window; the example shown above therefore has the following meaning:

Field	Description
Remote ID	Shows the ID of the remote peer. Authentication in the example uses certificates; the remote ID thus consists of quotes from the peer's certificate.
Remote IP	Shows the IP address of the remote peer.
Local ID	Shows the local ID. This ID also consists of quotes from the certificate used for authentication.

Field	Description
TARSEH	Shows the combination of the parameters explained in the help section of the menu window. The example ISREBM thus means: ■ Exchange type: id_protect (*I*) ■ Authentication method: RSA signature (*S*) ■ Role: Responder (*R*) ■ Status: Established (*E*) ■ Encryption algorithm: Blowfish (*B*) ■ Hash algorithm: MD5 (*M*)

Table 10-2: ***IPSec ➜ Monitoring ➜ IKE Security Associations***

10.3 Submenu IPSec SA Bundles

The next submenu (***IPSec ➜ Monitoring ➜ IPSec SA Bundles***) shows the IPSec Security Associations negotiated in IKE phase 2. The menu has the following structure:

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[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
```

The meaning of the abbreviation in the **SEA** column is also explained in the help section of the menu window. The fields have the following meaning:

Field	Description
Local	Shows the local ➤➤ **IP address**, the address range or the network protected by this SA.
LPort	Shows the local ➤➤ **port** number or port number range protected by this SA.
Pto	Shows the layer 4 protocol of the data traffic protected by this SA (*0* = any).
Remote	Shows the remote IP address, the address range or the network protected by this SA.
RPort	Shows the remote port number or port number range protected by this SA.
CEA	Shows which IPSec protocols are used for the SA. ■ *C* = IPComP ■ *E* = ESP ■ *A* = AH.
In	Shows the number of bytes received via this SA.
Out	Shows the number of bytes sent via this SA.

Table 10-3: ***IPSec ➜ Monitoring ➜ IPSec Security Associations***

Index: IPSec