IPSec

Version 3.0
August 2002

Purpose

This reference manual gives an overview of BinTec's IPSec feature set and provides IPSec configuration workshops for solution scenarios with BinTec Routers. 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 more recent release level. The latest release notes can always be found at www.bintec.net.

Liability

While every effort has been made to ensure the accuracy of all information in this manual, BinTec Communications AG 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, including changes and release notes for BinTec Routers, can be retrieved from www.bintec.net.

As a multiprotocol router, a BinTec Router sets up WAN connections (e.g. ISDN) in accordance with the system configuration. To prevent unintentional charge accumulation, the operation of the product should be carefully monitored. BinTec Communications AG 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 Communications AG.

All other product names and trademarks mentioned are the property of the respective companies.

Guidelines and standards

BinTec Routers comply with the following guidelines and standards:

- R&TTE Directive 1999/5/EC

- CE marking for all EU countries

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

How to reach BinTec

BinTec Communications AG
Südwestpark 94
D-90449 Nürnberg
Germany

Telephone: +49 911 96 73 0

Fax: +49 911 688 07 25

Internet: www.bintec.de

BinTec Communications 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

Table of Contents 5

REFERENCE

1 Overview

Practically all communication over the internet uses the Internet Protocol IP V4. IP allows information to be sent from one computer to another through a variety of intermediate computers with different platforms and separate networks before it reaches its destination. The great flexibility of IP has led to its worldwide acceptance as the basic internet and intranet communications protocol.

The popularity of the internet derives from its flexibility: The internet adapts itself to the way businesses communicate and the speed of communications is increasing, while the costs are decreasing. However, the weakness of IP-based networks is their lack of security.

The basic requirements for network security are:

- Authenticity
  Ensuring that the person or machine you believe you are communicating with really is that person or machine.
- Confidentiality
  Ensuring that no one can view transmitted data in clear text.
- Integrity
  Ensuring that communication has not been altered during transmission.

Motivation for IPSec

The motivation for IPSec (Internet Protocol Security) was the obvious demand for an IP security standard. IPSec is a framework of open standards for ensuring secure private communications across a public network. Based on standards developed by the Internet Engineering Task Force (IETF), IPSec transparently provides security services using modern cryptographic methods. IPSec provides protected traffic, irrespective of the application. Also, the provided security is transparent for end users.

1.1 The Security Issue in a Network Environment

As data on an (unsecured) IP network are visible and open to anyone, the origin, content and privacy of this data cannot be assumed to be secret and secure. The two main security risks specific to IP are data theft and data manipulation.

The following section contains a brief description of the most important security threats and how these threats can be met (section A, chapter 1.1.2, page 12).

1.1.1 Security Threats

Spoofing

Spoofing makes a packet coming from one source device appear to come from somewhere else. An attacker can easily counterfeit IP addresses in IP packet headers and pretend to be someone else.

Electronic Eavesdropping or Sniffing

Sniffing is an attack that is possible in Ethernet-based IP networks. In most Ethernet LANs, packets are available to every Ethernet node within the network. A "sniffer" is a type of software used by any network diagnostician working with Ethernets. The sniffer can record all network traffic on the Ethernet, allowing to determine quickly what is going through any segment of the network. However, in the wrong hands it is a powerful eavesdropping tool if someone wants to intercept sensitive communications. This person could easily collect company data and messages for later analysis.

Session Hijacking

In session hijacking the attacker attempts to take over and monitor an existing connection between two computers.

The session hijacker takes control of a network device on the LAN (e.g. a firewall or another computer). In this way, the session hijacker can steal the session or overload one of the involved computers so that it has to drop out of the communication.

1.1.2 How Can These Threats Be Met?

These security threats can be obviated through the use of cryptography. The main goals of cryptography are to maintain and provide security services such as authentication, confidentiality, integrity, non-repudiation and anti-replay.

Authentication

Authentication secures the origin and the integrity of a message by safeguarding the genuine identity of all communicating network nodes. The following authentication methods are commonly used:

- Software-based authentication systems:
  - Passwords: the simplest form of authentication. One-time password systems restrict the validity of a password to a single session, so that unauthorized use is restricted.
  - PAP: The Password Authentication Protocol (PAP) was originally designed as a simple way for one computer to authenticate itself to another computer when the Point-to-Point Protocol (PPP) is used. PAP is a two-way handshaking protocol; that is, the initiator of a communication sends a user ID and password pair to the responder, and then the responder (the authenticator) acknowledges that the computer is authenticated and approved for communication. With PAP the password is transmitted unencrypted.
  - CHAP: The Challenge Handshake Authentication Protocol (CHAP) was designed for the same uses as PAP, but CHAP is a more secure method for authenticating PPP links. CHAP is a three-way handshaking protocol. Like PAP, CHAP can be used at the start of a PPP link and then repeated after the link has been established.
- Hardware-based systems:
  - Smart Cards: Smart cards include an embedded microprocessor and memory. Smart cards can store a user's private key along with any installed applications, which simplifies the authentication process, especially for mobile users.
  - PC Cards: PC cards, formerly called PCMCIA cards, are small circuit boards that can be inserted into special slots on desktop computers, and particularly on laptops. These cards can offer some of the same functionality as smart cards but are restricted to PCs with PCMCIA slots. On the other hand, PCMCIA cards have the advantage of more

available memory and higher processing performance; this enabled them to store larger files for authentication purposes.

– Token Devices: Token-based systems (like RSA SecurID) usually are based on separate hardware (i.e. are not built into a PC). BinTec provides a TAF (Token Authentication Firewall) implementation. For more information, see the Software Reference.
– Biometric Systems: Biometrics depend on using a unique personal trait to identify the user. One approach is fingerprint scanning. There are other approaches like face analysis systems which operate on a PC with a low-cost, low-resolution camera.

Confidentiality

Confidentiality ensures that data is only revealed to the intended recipients. Data is encrypted before transmission, ensuring that the data cannot be read during transmission even if the packet is monitored or intercepted by an attacker. The most common encryption systems are:

- IPSec
  Provides network layer security.
- PPTP (Point-to-Point Encryption Protocol)
  Provides point-to-point connection security.
- ➤➤ **SSL** and ➤➤ **TLS**
  Provide general connection-oriented authentication and encryption.

Integrity

To protect data integrity, information must be protected from unauthorized manipulation while being transmitted. This ensures that any information received is exactly the same as the information that has originally been sent. Mathematical ➤➤ **hash functions** are used to compute a message digest which is encrypted and sent along with the message as a digital signature (see "MD and Digital Signature", page 20). The receiving computer checks the signature before opening the packet. If the signature (and therefore, the packet) has changed, the packet is discarded. The most commonly used hash algorithms are:

- ➤➤ **MD5** (Message Digest version 5)
- ➤➤ **SHA1** (Secure Hash Algorithm)

For all Phase 1 ("IKE Phase 1", page 32) exchanges BinTec routers additionally support the following hash algorithms:

- ➤➤ **RipeMD 160**
- ➤➤ **Tiger 192**

Non-repudiation By signing a message with a private key, the sender acknowledges that he or she has actually created and sent that message. He or she cannot, then, deny having sent the message, since the signature can be verified with the public key created together with the private key.

Anti-replay Also called replay prevention. Through safeguarding the uniqueness of each IP packet messages captured by an attacker cannot be reused or replayed to establish a session or gain information.

1.2 Benefits of IPSec

The IPSec protocol suite provides security services at the network-packet level. The Internet Engineering Task Force (IETF) has developed the IPSec standards to secure the network itself rather than the applications sending data across the network.

IPSec's main benefits:

- IPSec is currently the only accepted security standard available for IP encryption
- IPSec provides interoperability with other IPSec compliant manufacturers
- IPSec provides security services essential to protect a network environment:
  - authentication
  - confidentiality
  - integrity
  - non-repudiation
  - anti-replay
- IPSec is designed to work with both versions of the standard for IP addresses and routing, IPv4 and IPv6

Main application scenarios for IPSec are:

- VPNs
  - Intranets: Most large enterprises maintain costly wide-area networks where Virtual Private Networks ensure secure data transfer over potentially insecure connections like the Internet or WLANs.
  - Extranets: Companies can easily create secure links with their suppliers and business partners.
  - Remote Access: Using tunneling technology enables remote users to access the corporate network at maximum security.
- Host-to-Host connections
  Provides end-to-end security between two hosts across the network.

1.3 Simple Description of How IPSec Works

IPSec can provide a secure tunnel between two security gateways across insecure networks (like, e.g., the internet). It thus provides transparent security for all hosts on either side of the secure tunnel. The connection endpoints and the endpoints of the IPSec tunnel are not identical. On the other hand direct host to host connections are possible, too, in which case the tunnel and the connection endpoints are identical, but only the connecting nodes (e.g. hosts) take advantage of the IPSec tunnel.

The following figure illustrates this difference:

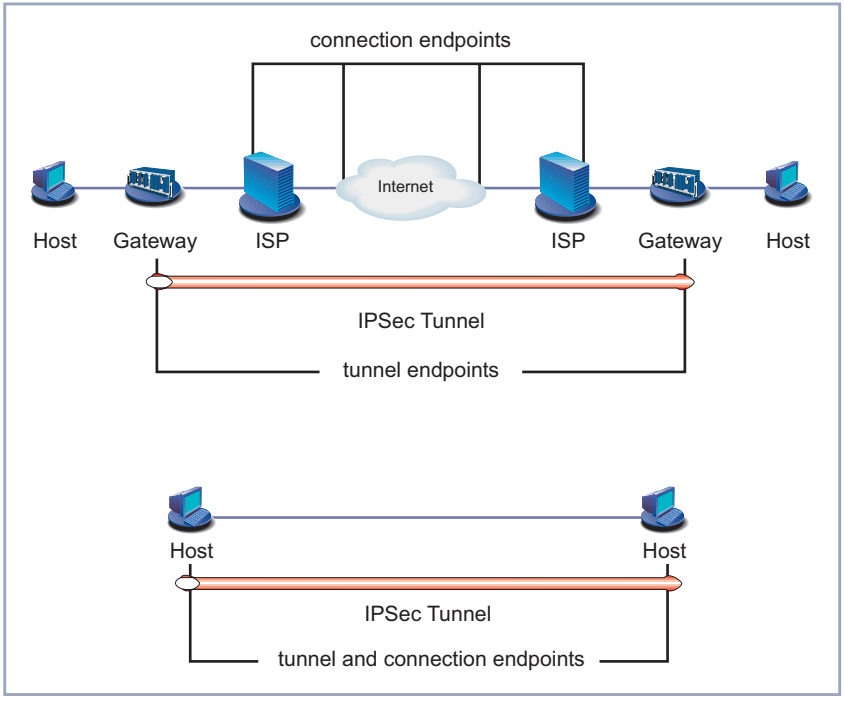


Figure A-1: Connection and tunnel endpoints

An Example of IPSec Processing

In the following example, Alice and Bob are two IPSec peers who want to exchange data, in this case an e-mail. An IPSec-protected data exchange usually consists of the following steps (the individual mechanisms will be explained in detail later in this document):

1 The general security parameters have to be defined:

- the kind of traffic to be protected: in our example, it is the mail traffic from Alice's computer to Bob's computer which has to be secured.
- how the traffic is to be protected: should the traffic be encrypted and/or authenticated?

2 The IPSec devices, e.g. routers, on each side must be configured according to the selected parameters.

3 Alice sends an e-mail to Bob.

4 Alice's router traps Alice's e-mail packet and checks its configuration. The settings in our example require that the e-mail traffic must be authenticated and encrypted.

5 Alice's router and Bob's router authenticate each other and establish a secure channel for key exchange (IKE SA) using the Diffie-Hellman mechanism.

   If the authentication is certificate-based, Alice and Bob will exchange their certificates and check their validity, eventually communicating with a certificate server.

6 The two routers use the previously established secure channel to negotiate security algorithms and exchange keys for a secure e-mail channel (IPSec SA).

7 Alice's router uses this secure e-mail channel to forward e-mail packets from Alice to Bob.

8 The secure channel (also called the tunnel) is closed again after the mail has been transmitted.

2 IPSec Basics

This chapter describes the basic technology used for IPSec. It covers the basics of cryptography and the IPSec protocols (section A, chapter 2.2, page 21) as well as a description of how IPSec processes the IP traffic (section A, chapter 2.3, page 27) and the use of certificates (section A, chapter 2.4, page 36).

2.1 Introducing Cryptography

Cryptography covers a number of algorithms used for encryption, authentication, key generation and decryption. For encryption to work properly, both the sender and receiver have to agree upon a set of rules to transform the original information into its coded form.

Encryption is based on the combination of an algorithm and a key used to secure information. A cryptographic algorithm, also called a cipher, is a mathematical function that combines plain text or other intelligible information with a string of digits called a key to produce unintelligible cipher text.

2.1.1 Secret-Key Cryptography

With this form of key-based cryptography called secret-key cryptography or symmetric encryption, the same key is used both for encryption and decryption of data. An example of a symmetric encryption algorithm is ➤➤ **Rijndael (AES)**, a standard encryption algorithm developed to replace the older DES algorithm which was used as certified standard for US government use.

Implementations of symmetric-key encryption can be highly efficient, so that users do not experience any significant lag due to encryption and decryption. Symmetric-key encryption also provides a degree of authentication, since information which can be decrypted successfully with a certain symmetric key must have been encrypted with exactly the same key. Thus, each party can be sure that it is actually communicating with a certain other party as long as the symmetric key is kept secret by both parties. If anyone else discovers the key, both

confidentiality and authentication are affected. An unauthorized person possessing the symmetric key can decrypt messages sent with that key as well as encrypt new messages and send them as if they came from one of the two parties originally using the key.

Since with symmetric encryption both the sender and the receiver must agree upon a shared secret key, management problems arise with the growing number of correspondents: the larger the number of correspondents, the more secret keys have to be managed. Each pair of correspondents must have their own key, i.e. the number of keys increases to the power of two with the number of correspondents. The keys have to be securely stored at both ends of the communication.

2.1.2 Public-Key Cryptography

Public-key cryptography or asymmetric encryption is based on the concept of a key pair. The public key and an algorithm are used for encryption, and the private key and an algorithm are used for decryption.

The public key is known to everyone while the private key is known only to the recipient of the message. When Bob sends a secure message to Alice, he uses Alice's public key to encrypt the message. Alice then uses her private key to decrypt it.

Advantages of asymmetric encryption schemes:

- The public key can be freely distributed on a key server, so that all correspondents can download the key when needed, and the sender does not have to send key copies to every correspondent.
- There is no secret information which has to be passed over insecure channels.
- Confidentiality is maintained as the sender uses the recipient's public key to encrypt a message; it will remain confidential until it is decrypted.
- Authenticity is maintained as the sender signs a message using the private key, a key to which only he or she has access.

- Non-repudiation is maintained, as the sender of a message signs this message with his or her private key and the recipient is able to verify the signature using the sender's public key.

MD and Digital Signature

Using public-key algorithms to encrypt messages requires more computation, since asymmetric encryption schemes typically use a much larger key than symmetric schemes. For this reason, a short, unique representation of the message, called message digest (MD) is generated using a one-way hash function. If, again, the message digest is encrypted with the private key, the resulting encrypted hash is the digital signature. Digital signatures indicate that data has not been altered.

The most commonly used public-key algorithms are:

- RSA
  The RSA (named after its inventors Rivest, Shamir, Adleman) algorithm is based on the fact that there is no efficient way to factor very large numbers. Deducing an RSA key, therefore, requires an extraordinary amount of computer processing power and time.
  - RSA Signature: provides non-repudiation for authentication
  - RSA Encryption: provides additional ID protection and allows encrypted IDs in Aggressive Mode, too.
- DSA (DSS)
  Digital Signature Algorithm (Digital Signature Standard). A signature-only mechanism supported by the United States government. Its design criteria have not been made public. Regarding key generation, DSA is faster than RSA. On the other hand, regarding key computation, DSA is slower than RSA.

Usually Diffie-Hellman is listed with the public-key algorithms, too: It is a key-agreement algorithm. It cannot encrypt, nor can it sign data. Diffie-Hellman enables the correspondents to use a nonsecret untrusted channel (like, for example, the internet) to securely establish a shared secret key.

Diffie-Hellman

A Diffie-Hellman exchange works like this: Two people independently and randomly generate a private value and use the Diffie-Hellman "algorithm" to compute a corresponding public value from it. Each sends their public value to the other and then combines the public key they received with the private (secret) key they just generated, using the Diffie-Hellman combination algorithm. The

resulting value is the same on both sides, and therefore can be used for fast symmetric encryption by both parties.

Diffie-Hellman is susceptible to ➤➤ **"man-in-the-middle"** attacks, but these can be prevented by having the correspondents authenticate their public values using another mechanism like, e.g., RSA or DSA.

2.1.3 Selecting Encryption Methods

When selecting an appropriate algorithm to use, the first thing to do is to determine how sensitive the data is and for how long it will have to be protected. Then, an encryption algorithm and key length – that will take longer to crack than the length of time for which the data will be sensitive – have to be selected.

BinTec's IPSec implementation supports several symmetric encryption algorithms so that interoperability is ensured. The supported algorithms are:

- ➤➤ **DES**
- ➤➤ **Triple DES**
- ➤➤ **Blowfish**
- ➤➤ **CAST**
- ➤➤ **Twofish**
- ➤➤ **Rijndael** (AES, Advanced Encryption Standard)

2.2 The Principal IPSec Protocols

IPSec works on the IP layer. The IP packet and the information it includes are fundamental for IPSec, i.e. information about source and destination and type of data being carried in the packet. IPSec defines two protocols for handling the authentication and encryption of IP packets, the encapsulating security payload (➤➤ **ESP**) for encryption and/or authentication purposes (section A, chapter 2.2.1, page 22) and the authentication header (➤➤ **AH**) for authentication purposes only (section A, chapter 2.2.2, page 23).

Security Association

In both protocols, IPSec uses so called Security Associations (SAs) to define the conditions and rules of a secure communication. An SA groups together all information necessary for secure communication with a peer. At least one SA is indispensable for each connection that is to be secured. The following list shows the contents specified in an SA:

- the security protocol used
- the peer's IP address
- the algorithms used
- the Security Parameter Index (SPI)
  The SPI is an arbitrary 32-bit number which identifies an SA among multiple SAs between the same peers.
- the selectors
  Selectors are used to specify a certain packet class, e.g. mail traffic from Alice to Bob.
- the keys and additional parameters (e.g. key length) necessary for the algorithms
- the lifetime of the SA

2.2.1 Encapsulating Security Payload

One of the two mechanisms IPSec uses for packet processing is called Encapsulating Security Payload (ESP). ESP can support any number of encryption algorithms; even different algorithms can be used for each correspondent. As a common basis all IPSec implementations support the DES algorithm in order to assure basic interoperability among different IPSec networks.

DES may be sufficient for applications requiring less or marginal security. If strong security is required, it is better to use 3DES. 3DES, also known as Triple-DES, is based on using DES three times (i.e. encrypt-decrypt-encrypt sequence with three different, unrelated keys).

If you need not use 3DES, you might consider using one of the new algorithms (Rijndael (AES) or Twofish) for increased security and speed.

ESP additionally supports authentication (see below, "Authentication within ESP", page 23).

This is what an ESP-protected IP packet looks like:

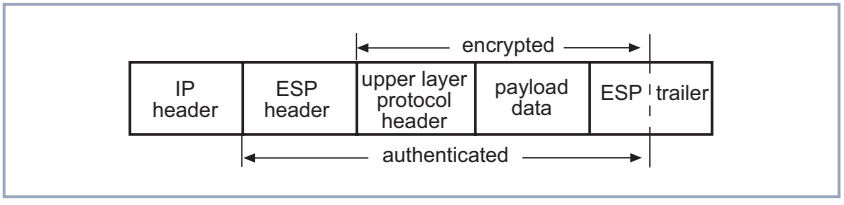


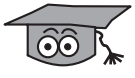
Figure A-2: An ESP-protected IP packet

The ESP header follows the standard IP header in an IP datagram, and contains both the data and all upper layer protocol headers relying on IP for routing. ESP has both, a header and a trailer, it encapsulates the data it protects. Due to a specified order of processing of ESP packets, some parts of the packet must be in plain text.

Authentication within ESP

ESP can also be used for authentication. The ESP authentication field, an optional field in the ESP header, contains a cryptographic checksum that is computed over the remaining part of the ESP packet. This checksum varies in length depending on the authentication algorithm used. It may also be omitted entirely, if authentication services are not selected for ESP. The authentication is calculated on the ESP packet when encryption is complete.

For further information about the Encapsulating Security Payload, refer to the corresponding RFC under http://www.ietf.org/rfc/rfc2406.txt.



It is possible to combine both protocols, ESP and AH, in one proposal. There are, however, only few applications for this, and the message overhead is significantly increased.

2.2.2 Authentication Header

The second IPSec protocol, called Authentication Header (AH), was designed to provide maximum authentication services for IP data. The Authentication Header is inserted after the IP header but before other higher level protocol in-

formation (like TCP or UDP or even IP, in case of Tunnel Mode). No changes are made to the packet's payload.

This is what an AH-protected IP packet looks like:

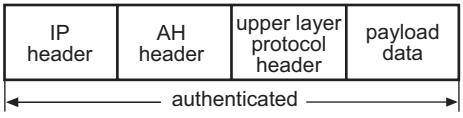


Figure A-3: IP packet protected by AH

The IPSec suite's Authentication Header protocol provides authentication services, but it does not provide confidentiality; an attacker could read the contents of packets but could not alter them unnoticed. All of the fields in the AH header are in plain text.

IPSec requires specific algorithms to be available for implementing AH. Any IPSec implementation must support at a minimum ➤➤ **HMAC-MD5** and ➤➤ **HMAC-SHA-1** to guarantee minimal interoperability.

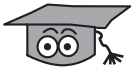
AH requires less computation than ESP because encryption is not performed. This applies also for ESP when used without authentication.

For further information about the Authentication Header, refer to the corresponding RFC under http://www.ietf.org/rfc/rfc2402.txt.

Where the differences are

The authentication provided by AH differs from that provided by ESP. ESP's authentication services do not protect the IP header that precedes the ESP header, although they do protect an encapsulated header in tunneling mode (see "ESP Tunnel Mode", page 25). The AH services protect this external IP header, along with the entire contents of the ESP packet.

AH is meant for occasions when only packet authentication is needed. On the other hand, when authentication and privacy are required, it is best to use ESP including ESP's authentication option.



Sometimes it is recommended to use both AH and ESP together as nested protocols: In this case ESP is applied to the packet first and then AH is used to authenticate the complete packet. With nested AH and ESP, the authentication option of ESP should be omitted to reduce the amount of network overhead and copying done during packet processing.

2.2.3 Tunnel Mode and Transport Mode

The IPSec specifications allow AH and ESP to be applied to an IP packet in two different ways, called modes. In Tunnel Mode, the entire IP packet is authenticated or encrypted. In Transport Mode, only the transport-layer segment of an IP datagram is processed (i.e. authenticated and/or encrypted).

IPSec tunneling

IPSec Tunneling encapsulates or hides the original packet inside a new packet. This new packet provides the necessary routing information, enabling the packet to travel through transit networks without showing the final destination. When the encapsulated packets reach their destination, the encapsulation header is removed and the original packet header is used to route the packet to its final destination.

The tunnel is the logical data path through which the encapsulated packets travel. When the tunnel is encrypted, it is referred to as a virtual private network (VPN).

ESP Tunnel Mode

ESP Tunneling takes the entire original IP packet and encapsulates it within the new payload. Then it adds to the packet a new IP header containing the address of a gateway.

This is what an ESP-tunneled IP packet looks like:

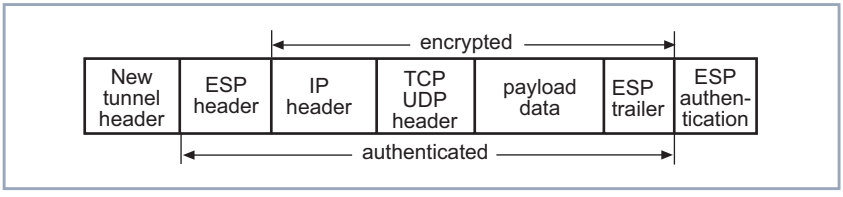


Figure A-4: ESP-tunneled IP packet

The "authenticated" area indicates where the packet has been integrity-protected. The "encrypted" area indicates what information is encrypted for confidentiality. The original header is placed after the ESP header. The entire packet is appended with an ESP trailer. Except for the ESP authentication trailer, everything following the ESP header is encrypted, including the original header because this is now considered to be part of the data portion. The entire packet is then encapsulated. The information in the new IP (tunnel) header is used to route the packet between tunnel endpoints.

AH Tunnel Mode

The only difference between AH and ESP Tunnel Mode is how the packet is handled. In AH tunnel mode, the entire packet is authenticated for integrity, including the new tunnel header. However, encryption is not provided.

This is what an AH-tunneled IP packet looks like:

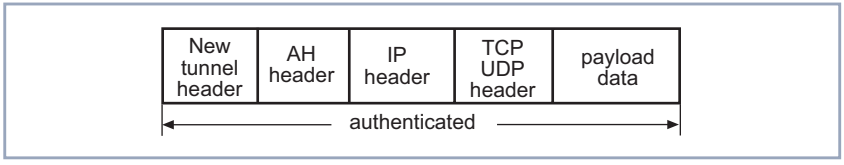


Figure A-5: AH-tunneled IP packet

ESP Transport Mode

In ESP Transport Mode, only the payload data of the original IP packet is protected. The payload is encapsulated by the ESP header and trailer. The original IP headers remain intact and are not protected by IPSec.

When two hosts are configured so that all transport layer packets travelling between them should be encrypted, ESP is used:

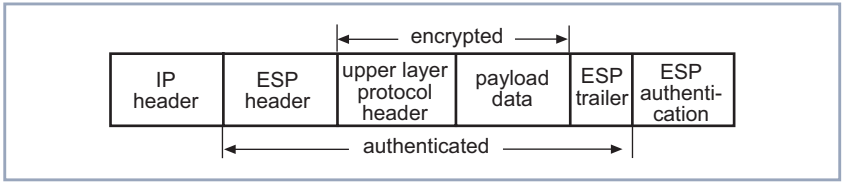


Figure A-6: ESP Transport Mode

AH Transport Mode

In AH Transport Mode, AH is inserted after the IP header and before an upper layer protocol (e.g. TCP, UDP, or ICMP), or before any other IPSec headers that already have been inserted. However, encryption is not provided. The IP address of the source and destination are still open to modification if the packets are intercepted. If only the transport layer packets are to be authenticated, then Transport Mode for AH may be used:

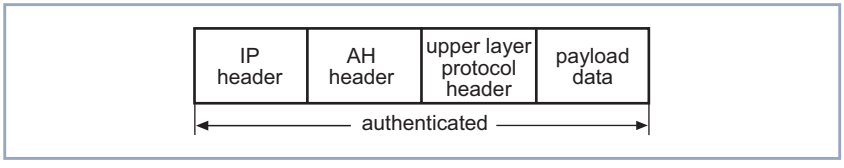


Figure A-7: AH Transport Mode

2.3 IPSec Processing

IPSec processing is complex, and it is done in different steps. You can find a concise description of these steps in the following chapter, more detailed information on Security Databases and key management follow in section A, chapter 2.3.2, page 28 and section A, chapter 2.3.3, page 30. The use of certificates is explained in detail in section A, chapter 2.4, page 36.

2.3.1 IPSec Processing – Concise Description

IPSec basically consist of three distinct steps:

- Step 1: Identify traffic that is to be protected and how it is to be protected.
- Step 2: If no information is available on how to protect the traffic specified for protection, security strategies (called Security Associations, SA) are negotiated between the peers. This step requires the most detailed configuration.
- Step 3: Protect data traffic by encrypting and/or authenticating IP packets.

The following figure illustrates this simplified view of IPSec processing:

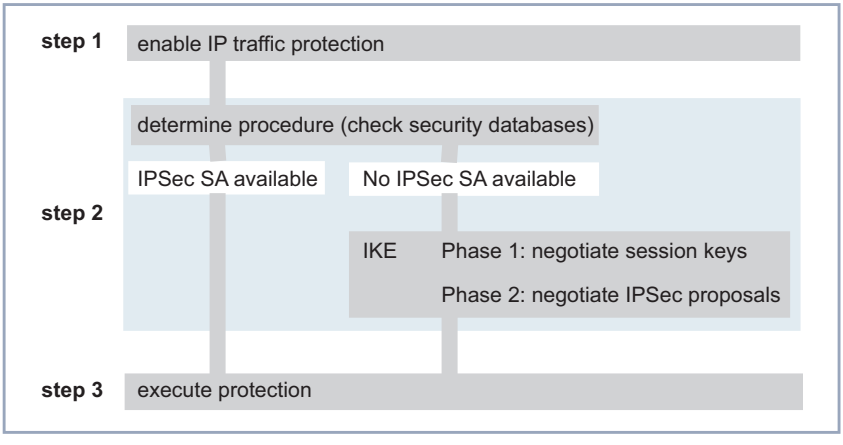


Figure A-8: IPSec overview

2.3.2 Security Databases

All parameters set during the configuration of IPSec are stored on your BinTec router. Certain combinations of this information are referred to as either the Security Policy Database (SPD) or the Security Association Database (SAD).

SPD The Security Policy Database specifies the security services offered to the IP traffic. These security services depend on parameters such as source, destination of the packet, etc.

SAD The Security Association Database contains information about each SA (while an SA is a sort of instance for an SPD entry), such as AH or ESP algorithms and keys, sequence numbers, protocol mode and SA lifetime. For outbound processing, an SPD entry points to an entry in the SAD. That is, the SPD determines which SA is to be used for a given packet. For inbound processing, the SAD is consulted to determine how the packet must be processed.

The following figure illustrates the procedure of checking the SPD and the SAD (this procedure is the first part of Step 2 in figure A-8, page 27):

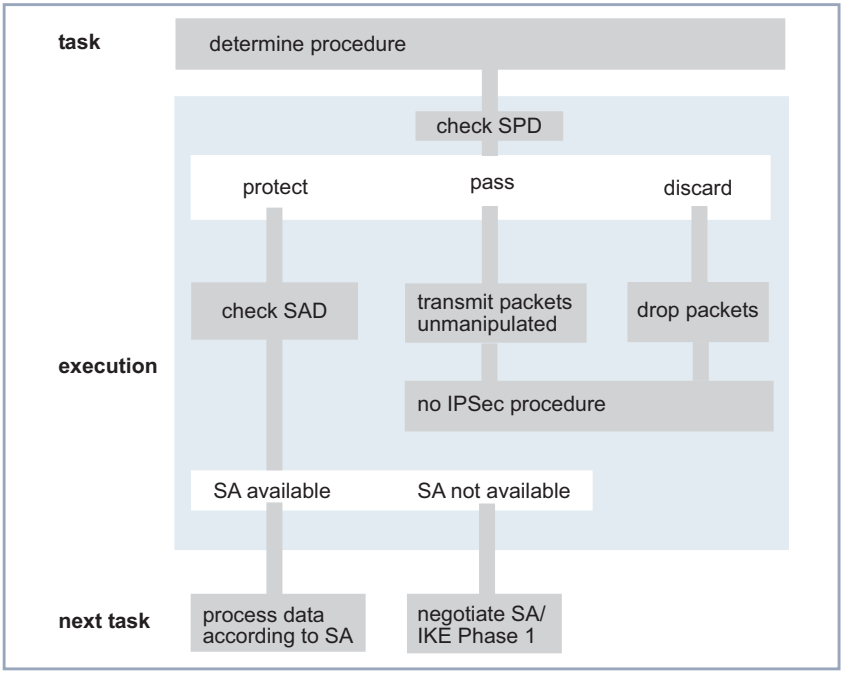


Figure A-9: Checking SPD and SAD

Outbound processing

A routed packet is sent to the WAN. The policy entries in the SPD are checked:

- If the policy says that the outgoing packet needs to be dropped, the packet will be discarded.
- If the policy says to transmit the outgoing packet without security processing, the packet will be transmitted in clear text.
- If the policy says that the outgoing packet needs security (ESP and/or AH), the policy manager checks if the corresponding SAs are already established:
  - if the SAs are not yet established, the policy manager triggers IKE (see section A, chapter 2.3.3, page 30) to establish the required SA(s).
  - if the SAs are already established, they are read from the SAD and IP packets are processed according to the configured parameters.

Inbound processing

An IP packet arrives from the WAN. Again, the policy entries in the SPD are checked:

- If the policy says that the incoming packet needs to be dropped, the packet will be discarded.
- If the policy says to transmit the incoming packet without security processing, the packet will be transmitted in clear text.
- If the policy says that the incoming packet has to be encrypted and/or authenticated:
  - an unencrypted and/or unauthenticated packet will be dropped.
  - an encrypted and/or authenticated packet will be processed as follows:
    The IPSec engine extracts the SPI (Security Parameter Index) from the ESP or AH header as well as the source and destination IP addresses and protocols.
    The IPSec engines reads the SA specified by the SPI from the SAD.
    If the SAD does not find the SA, an error is logged and the packet is dropped.
    If the SAD returns the SA, the IPSec layer processes the packet according to the processing rules of ESP and AH.
    The resulting packet is again checked in the SPD to verify if the policy has been applied appropriately according to the defined rules and sequences. If this is not the case, an error is logged and the packet will be dropped.

2.3.3 Key Generation and Management (Internet Key Exchange)

There are currently two ways to handle key exchange and key management within BinTec's IPSec architecture: manual keying and automated Internet Key Exchange (IKE). Both of these methods are mandatory requirements of the IPSec specification, but manual keying has some severe drawbacks in comparison to IKE.

Manual keying

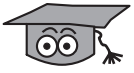
When deciding on the use of manual security associations, two IPSec peers have to agree on equal configuration information in both systems: there is no negotiation of security associations. Manual SAs do not provide for replay pro-

tection. Thus it is very important to properly select keys and to pay great attention to keeping them secret. Moreover, the keying material is the same for all exchanges until the keys are manually changed while IKE provides fresh keying material every time it is applied.

Since Manual Keying is less secure than IKE and more difficult to administrate, it is not supported by BinTec.

Internet Key Exchange (IKE)

IKE, on the other hand, provides the infrastructure for an automated key distribution and protocol negotiation between communicating parties.



IKE, the IPSec concept for protocol negotiation and key exchange through the internet, integrates the Internet Security Association and Key Management Protocol (ISAKMP) with the Oakley key exchange scheme. ISAKMP/Oakley is the obsolete name for IKE.

There are three modes of exchanging keying information and setting up SAs: two for IKE phase-1 exchanges (Main Mode and Aggressive Mode, see "IKE Phase 1", page 32), and one for phase-2 exchanges (Quick Mode, "IKE Phase 2", page 34).

IKE provides a way to:

- agree on protocols, algorithms, and keys to use and ensure that key exchanges are handled safely
- ensure authentication services from the very beginning of the IPSec exchange
- manage the involved keys

IKE provides secure key exchange:

- ➤➤ **Denial-of-Service Attacks** can be prevented:
  Main Mode provides a better DoS protection than Aggressive Mode, although DoS attacks can never be entirely eliminated. Aggressive Mode leaves an attacker the possibility to intercept the packet and perform replay attacks.
- Perfect Forward Secrecy (PFS) can be provided:
  Refreshing a shared secret key involves combining the current key with a random number to create a new key. PFS enforces that each refreshed key will be derived without any dependence on predecessor keys. The reason

is to avoid that an attacker derives a particular secret key by means of a compromised old key.
PFS can be set to either enabled or disabled. If enabled, there always is a Diffie-Hellman exchange during Phase 2. If disabled, the keying material derived from the Diffie-Hellman mechanism in Phase 1 is reused.

- IKE is not susceptible to replay attacks.

IKE works in two phases which are described below.

IKE Phase 1

During Phase 1, the two IKE peers authenticate each other and establish a secure channel for doing IKE, called the IKE SA (sometimes also called ISAKMP SA). This is negotiated via a Diffie-Hellman exchange. There are three methods of authentication IKE can be configured for:

- Authentication with pre-shared keys
- Authentication with digital signatures
- Authentication with public-key encryption.

Main Mode (ID Protect Mode)

Main Mode accomplishes a phase-1 IKE exchange by establishing a secure channel using six exchanges (between the initiator and the responder). The negotiation differs depending on the authentication method used:

- Main-mode authentication with pre-shared keys
  This kind of authentication provides for identity protection. It is, however, not possible to use Main Mode if the peer ID is unknown, i.e. domain names or dynamic IP addresses cannot be authenticated with pre-shared keys using Main Mode.
  The pre-shared keys have to be kept secret: no intelligible words or short passwords should be taken: as a reference value, always 20 characters at a minimum should be used.
- Main-mode authentication with digital signatures (DSA or RSA)
  With digital signatures, other IDs than the IP address are possible.
- Main-mode authentication with RSA encryption
  With RSA encryption, other IDs than the IP address are possible; moreover, the authentication is encrypted.

Aggressive Mode

Aggressive Mode is another, faster way of accomplishing a phase-1 exchange. Aggressive Mode does not provide identity protection for the negotiating nodes as they must transmit their identities before having negotiated a secure channel. The following kinds of authentication are possible:

- Aggressive-mode authentication with pre-shared keys
- Aggressive-mode authentication with digital signatures (DSA or RSA)
- Aggressive-mode authentication with RSA Encryption

The following figure illustrates the phase-1 exchanges (this procedure starts the second part of Step 2 in figure A-8, page 27):

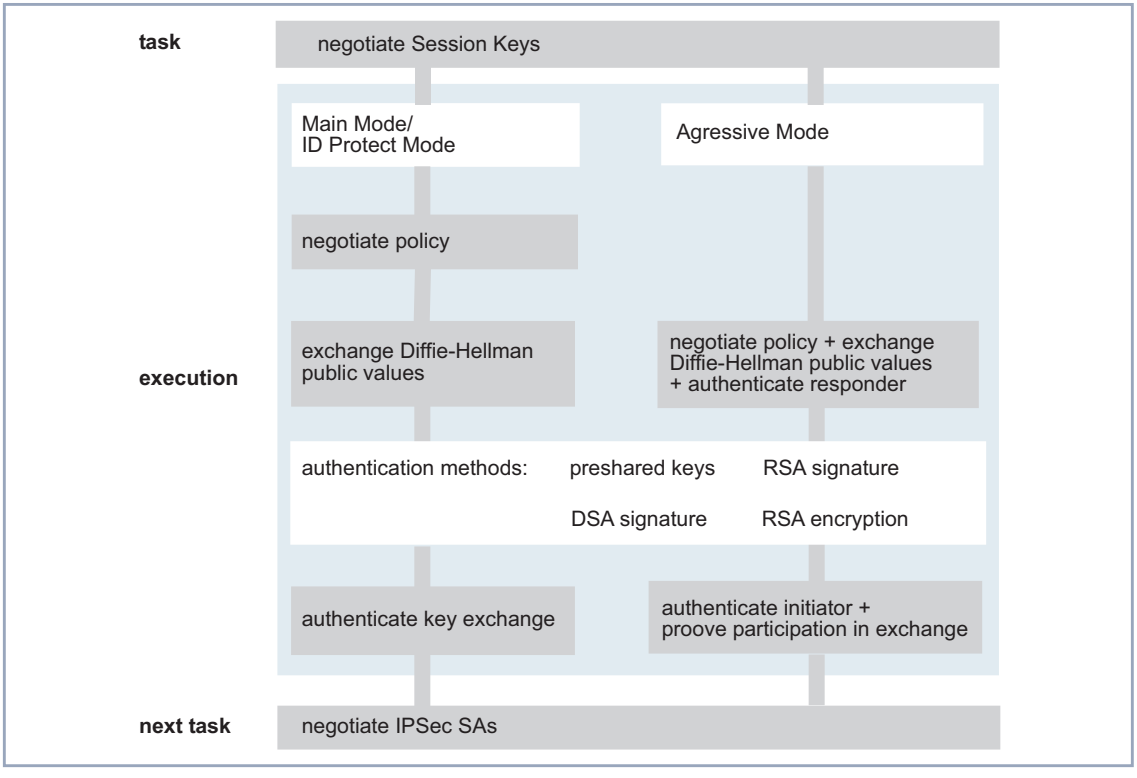


Figure A-10: IKE Phase 1

IKE Phase 2

In Phase 2, the two IPSec peers negotiate the IPSec SAs proper, i.e. they negotiate the SAs and keys that will protect user data exchanges. These phase-2 IKE messages are, again, protected by the phase-1 IKE SA. Phase-2 exchanges are less complex, so keys are refreshed more often than in Phase 1.

In Phase 2 the so called Selectors and the IPSec proposals are negotiated: Source and destination address, address ranges, source and destination port are used as Selectors, i.e. these are the factors that determine which kind of IP packets are filtered for IPSec processing. The IPSec Proposals, on the other hand, determine in which way a filtered packet will be processed. The IPSec Protocol (ESP or AH) and the combination of encryption algorithms and hash algorithms are the main factors of an IPSec proposal.

During negotiation the key is generated according to the algorithms chosen, and it is exchanged through the secure channel created by IPSec Phase 1. IPSec uses the same set of encryption algorithms for Phase 1 and Phase 2.

The following figure illustrates IKE Phase 2 (this procedure concludes the second part of Step 2 in figure A-8, page 27):

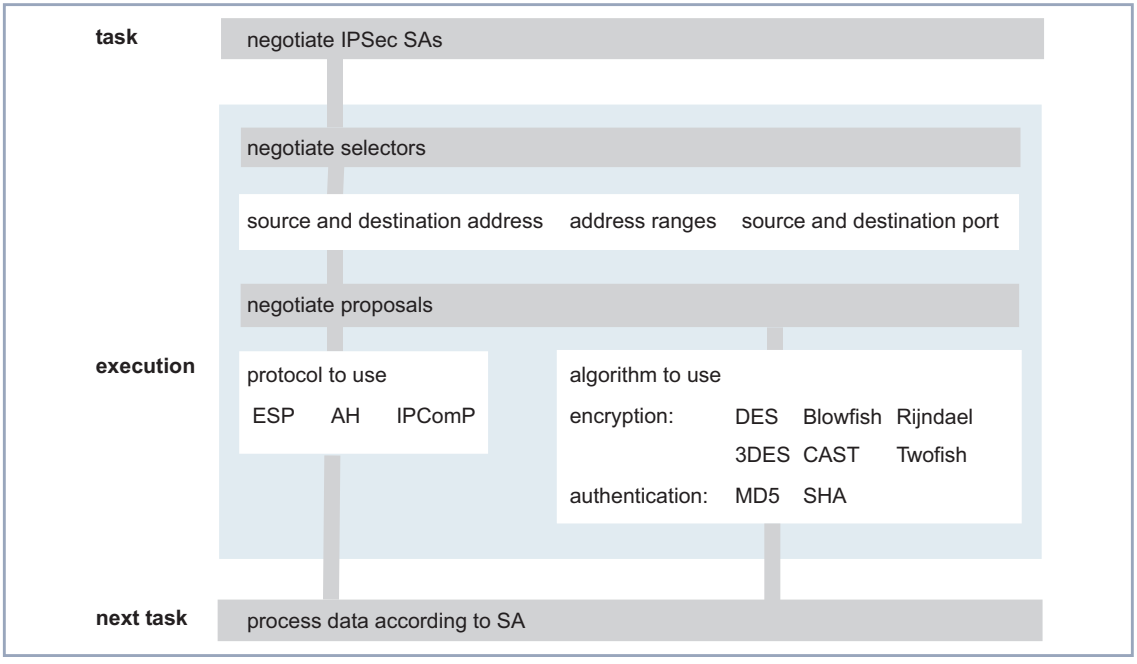


Figure A-11: IKE Phase 2

Quick Mode

Only one mode is specified for IKE Phase 2, the so called Quick Mode. Quick Mode accomplishes a phase-2 exchange after the phase-1 IKE SAs have been established by means of Main Mode or Aggressive Mode. Quick mode negotiates general IPSec services and refreshes the keys more quickly since the new keying material is derived from the material created during the phase-1 exchanges.

Normally Quick Mode does not provide for Perfect Forward Secrecy (PFS), since PFS requires that multiple keys are not derived from a single Diffie-Hellman exponentiation (the exponentiation takes place during the phase-1 exchanges).

PFS can be achieved by exchanging yet another key exchange payload so that a new exponentiation takes place and no keys are derived from previously used material.

2.4 Certificates

When two IPSec peers want to exchange IPSec-protected data, they first authenticate each other. The authentication itself works as described in section A, chapter 2.3.3, page 30. If RSA or DSA algorithms are used for authentication, public keys are usually safeguarded using certificates. This section explains the basics of certification (this chapter) as well as how certificates are issued (section A, chapter 2.4.1, page 39), the interconnection of Certificate Authorities (section A, chapter 2.4.2, page 40), the role of LDAP (Lightweight Directory Access Protocol) servers (section A, chapter 2.4.3, page 42) and the role of certificates in key management (section A, chapter 2.4.4, page 43).

A certificate identifies someone or something. This may be an individual, an object, a company, or an application. The certificate associates that identity with a public key. Public-key certificates are specially formatted data blocks (e.g. binary- or base64-encoded) which provide a safe method of distributing public keys. Public-key certificates are certified by an issuing organization called a certification authority (CA).

CA

Certification authorities, often also called certificate authorities, can be either independent third parties (certified or not certified) or organizations issuing their own certificates.

Contents of a certificate

The standard for certificates is the ➤➤ **X.509** standard designed by the International Telegraph Union (ITU). This standard specifies the format of the certificate and the conditions under which certificates are created and used.

This is what a sample certificate can look like (as seen using the cert tool described in section A, chapter 5.1, page 120):

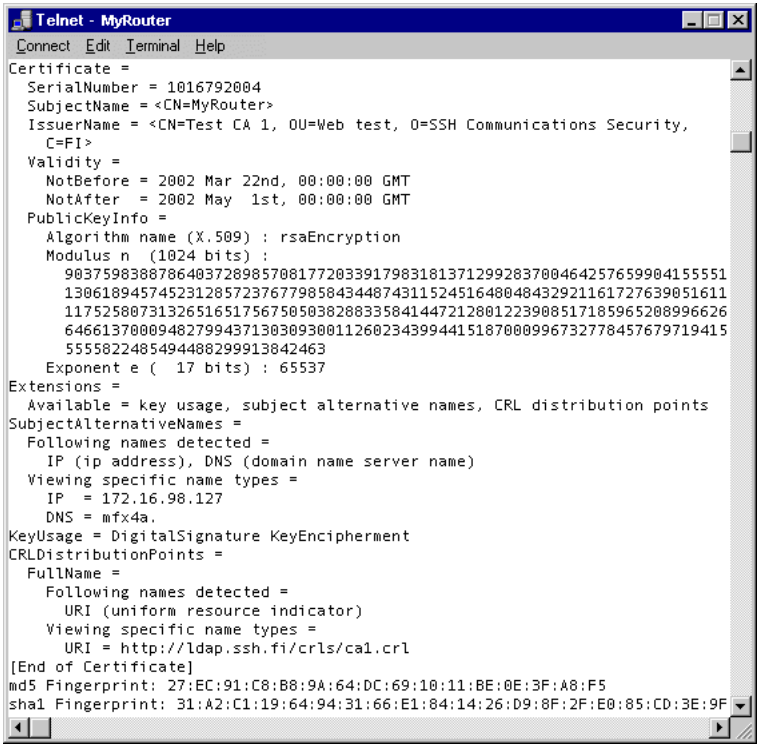


Figure A-12: Sample Certificate

The following list shows the typical X.509 v1–v3 certificate structure by means of example entries:

- Subject's distinguished name
  A name uniquely identifying the subject of the certificate
  Example: CN=Alice, OU=Development, O=BinTec Communications AG, C=DE

- Issuer's distinguished name
  A name uniquely identifying the certification authority that signed the certificate
  Example: CN=CAIssuer Class 1 root, O=CAIssuer, C=US

- Subject's public key
  The subject's public key
  Example: 1024-bit RSA key
- Issuer's signature
  The certification authority's digital signature from which the certificate derives its authenticity
  Example: RSA encryption with MD5 hash
- Validity period
  Dates between which the certificate is valid
  Example: Not before Mon, Oct 18, 1999, 09:15:40; Not after Fri, Oct 18, 2000, 18:00:00
- Serial number
  A unique number generated by the certification authority for administrative purposes (e.g. CRL)
  Example: 12:34:56:78:90

The abbreviations used above have these meanings:

- E: e-mail address;
- CN: the common name (which can be a person's name, an object's Fully-Qualified Domain Name (FQDN) or IP address, software package, etc.);
- O: organization;
- C: country;
- OU: organization unit

Certificates and Public Key Infrastructure

The set of standards and services that facilitate the use of public-key cryptography and certificates is called a public key infrastructure (PKI). A PKI makes it possible to use keys and certificates, and to manage the keys, certificates, and security policies in a network environment. A PKI addresses the following certificate management issues:

- Issuing Certificates (section A, chapter 2.4.1, page 39)
- Certification Hierarchies (section A, chapter 2.4.2, page 40)
- LDAP (section A, chapter 2.4.3, page 42)
- Key Management (section A, chapter 2.4.4, page 43)

- Renewing and Revoking Certificates (section A, chapter 2.4.5, page 43)

2.4.1 Issuing Certificates

CAs issue, manage and revoke certificates for their user community. CAs build up certificate policies and maintain a certificate revocation list (CRL). The process for issuing a certificate depends on the chosen certification authority and the purpose for which the certificate will be used. Different CAs have different procedures for issuing different kinds of certificates. In some cases, the only requirement may be specifying an e-mail address. In other cases, for certificates that identify people who make sensitive decisions, the issuing process may require notarized documents, a background check, and a personal interview.

Registration Authorities

Issuing certificates is one of several management tasks that can also be handled by separate Registration Authorities (RAs).

In some situations it may be advisable to separate some of the certificate administration tasks from the CA. Such tasks could be: registration for certification, certificate retrieval, certificate renewal, certificate revocation, and key backup and recovery.

These separate service tasks can be handled by a Registration Authority (RA). An RA acts as a front end to a CA by receiving the applicants' requests, authenticating them, and forwarding them to the CA. After receiving a response from the CA, the RA notifies the applicant of the results. RAs can be helpful if the PKI stretches across different departments, geographical areas, or other operational units with varying policies and authentication requirements.

Sample Certification and Registration Process

One possible certificate distribution process is shown in the following scenario.

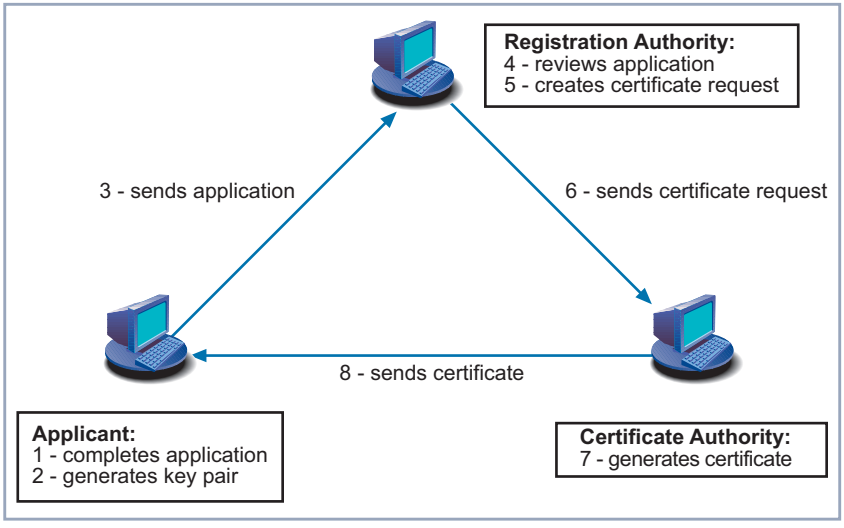


Figure A-13: Registration and Certificate Process

1, 2, 3 The applicant chooses a certification authority to enroll with and completes the application form. He or she then generates a public key pair and sends the public key along with the application to a Registration Authority. Depending on the CA chosen, the CA itself may function as Registration Authority; moreover, it may be possible for applicants to generate a certificate request themselves and apply for a certificate directly.

4, 5, 6 The Registration Authority reviews the application and if all requirements are met creates the certificate request which it then sends to the CA.

7, 8 The CA generates the certificate and eventually sends it to the applicant.

2.4.2 Certification Hierarchies

As the number of correspondents using certificates grows in the network environment, not all users will have certificates issued by the same CA. Thus a means of interoperability is needed. In large organizations, it may be appropri-

ate to delegate the responsibility for issuing certificates to several different certification authorities.

There are two ways to ensure interoperability by establishing hierarchical certification models:

- Cross certification
- Certificate hierarchy chain

Cross certification

Cross certification is an approach to bridge otherwise separated certification domains. In this approach, cross certification relationships are established.

Such a cross-certification model could look like this:

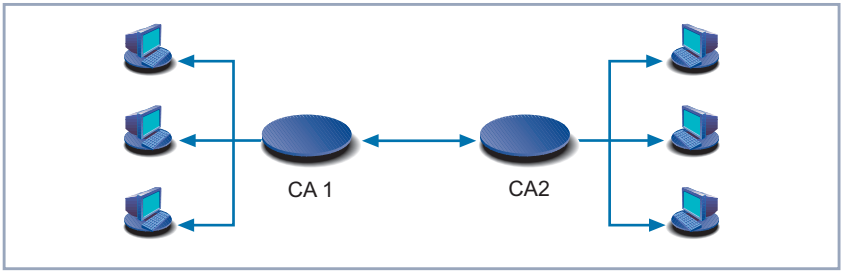


Figure A-14: Cross certification model

In this scenario, each CA first signs the certificates of its own domain. Since both CAs have, however, agreed on a trust relationship, CA1 can now sign the certificates of CA2's domain and vice versa. This is done if the certificate of a host from the other CA's domain has already been signed by the domain CA itself. This means that, e.g., CA1 considers the signature of CA2 evidence enough to sign any certificate already signed by CA2.

Certificate hierarchy chain

To harmonize different certification practices and certificate policies, so called root certificates and subordinate certificates are established. Any client or server software that supports certificates maintains a collection of trusted CA certificates. These CA certificates determine which other issuers of certificates the software can trust. A trusted CA certificate can be part of a chain of CA certificates, each issued by the CA above it in a certificate hierarchy. The X.509 standard includes a model for setting up a hierarchy of CAs.

Such a hierarchy model could look like this:

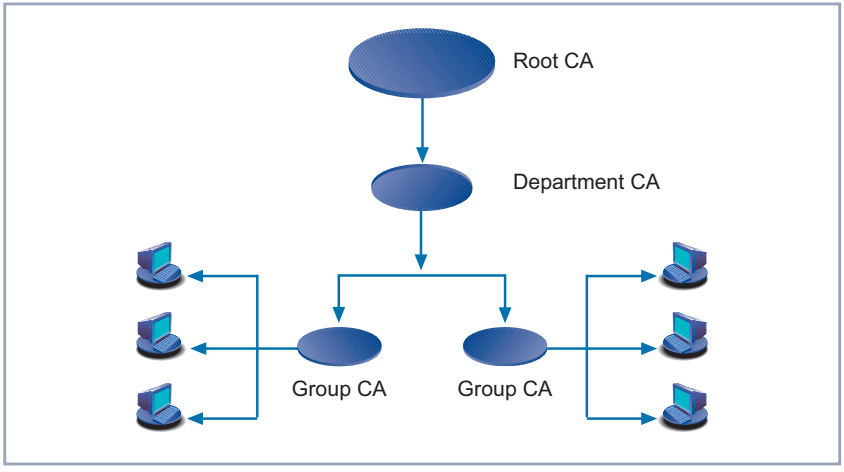


Figure A-15: CA hierarchy model sample for a company

Like in the CA hierarchy example shown in above, most companies have different departments with different groups. In this scenario, a member of some workgroup can have a certificate signed by the security team of the same group (Group CAs). Their certificate, in turn, can be signed by the security group of the department (Department CA), whose certificate, again, is signed by the corporate security group of the company (Root CA). Each group in the company has their certificate validated by the next higher node or trust point.

Each certificate is signed with the private key of its issuer, and the signature can be verified with the public key in the issuer's certificate. The CA at the top of the hierarchy is called the root CA.

2.4.3 LDAP – Automation in Key Management

When working with public-key systems you need to know the recipient's public key to encrypt a message for him or her. Likewise, you need this key to validate messages signed with a person's private key. What is needed, therefore, is a global registry of public keys and certificates, which is handled by the LDAP protocol.

The Lightweight Directory Access Protocol (➤➤ **LDAP**) for accessing directory services supports the management of certificates within an organization. System administrators can store much of the information required to manage certificates in an LDAP-compliant directory.

Other routine management tasks, such as key management and renewing and revoking certificates, can be automated with this kind of directory.

2.4.4 Certificates and Key Management

Before a certificate can be issued, the public key it contains and the corresponding private key must be generated. Sometimes it may be useful to issue a single person one certificate and key pair for signing operations, and another certificate and key pair for encryption operations.

Separate signing and encryption certificates make it possible to keep the private signing key on the local machine only. A backup of the private encryption key can be stored in some central location where it can be retrieved in case the user loses the original key or leaves the company.

There are two approaches to generating public-key pairs:

1. Keys can be generated by client software. The user generates a public-key pair, retains the private key, and delivers the public key to the certification authority to produce a certificate.
2. Keys can be generated centrally by the CA, which produces the signed certificate, and then delivers both the key pair and the certificate to the user.

2.4.5 Renewing and Revoking Certificates

A certificate specifies a period of time during which it is valid. Attempts to use a certificate for authentication before or after its validity period will fail. Therefore, mechanisms for managing certificate renewal are essential for any certificate management strategy. Also, it is sometimes necessary to revoke a certificate before it has expired, for example, if an employee leaves a company.

Certificate Revocation List (CRL)

The most common approach to revoking certificates is through CRLs, i.e. through a list of revoked certificates. These are published by Certificate Author-

ities at regular intervals, and BinTec routers can be configured to check this list during each authentication process. Authentication attempts with a certificate on the CRL will fail.

Public-key cryptography can only verify that a private key used to sign some data corresponds to the public key in a certificate. So it still remains the user's responsibility to carefully protect a machine's physical security – i.e. the access to individual machines or passwords – and to keep the private-key password secret.

2.5 DynIPSec

In unsupplemented IPSec, just as in other services, certain restrictions apply when dynamic IP addresses come into play; the gravest one is that no tunnel creation is possible for IPSec proper if both peers have dynamic IP addresses. This is due to the fact that for establishing a tunnel the address at least of one of the peers must be known so that the initiator "knows" where to direct the tunnel request. If only one peer has a dynamic IP address ("dynamic peer"), it is possible to establish an IPSec tunnel if this peer requests the tunnel and the other peer (having a static IP address, "static peer") assumes the role of responder. If both peers have dynamic IP addresses, this is not possible, either: none of the peers knows where he or she would have to direct a tunnel request.

IPSec can, however, be supplemented by another service to allow IPSec with dynamic IP addresses on both sides of the tunnel. What is needed for this is an implementation of the DynDNS service and its protocols, and a means to connect the IPSec service to the DynDNS service.

In order to establish a tunnel between peers that both have dynamic IP addresses, both peers need to configure the DynDNS service. This involves registering a hostname with a DynDNS service provider, e.g., www.dyndns.org. Once you have registered, you can set your router up to publicize its (dynamic) IP address to the DynDNS service provider every time it changes. The peer router can then refer to the provider to obtain the current IP address of your router and, thus, can initiate a tunnel creation. Likewise, the peer router can publicize its (dynamic) IP address to the DynDNS service provider so your router can request its IP address and you can initiate tunnel creation.

There is a large number of DynDNS providers, most of which have created proprietary protocols for the process of IP address propagation. BinTec up to now has implemented seven protocols:

- *dyn dns*
  (www.dyndns.org)
- *static dyn dns*
  (www.dyndns.org)
- *ods*
  (http://www.ods.org)
- *hn*
  (http://hn.org)
- *dyns*
  (http://dyns.cx)
- *GnuDIP HTML*
  (http://gnudip2.sourceforge.net)
- *GnuDIP TCP*
  (http://gnudip2.sourceforge.net)

Further protocols will follow.

The GnuDIP protocols can be used to set up a DynDNS server of your own. Refer to the GnuDIP's project site at the address given above.

You can, of course, use any of the providers that have created these protocols (as indicated by the internet addresses above); if you would like to use a different provider, however, you must make sure that the protocol used by your designated provider is compatible with one of those supported.

In order to make use of the DynDNS service at least one of the peers with dynamic IP addresses must run the DynDNS service, so that the other peer can retrieve the IP address and initiate tunnel creation. If the roles of initiator and responder cannot or should not be predetermined, both peers must run the DynDNS service.

Other restrictions concerning IPSec with dynamic IP addresses are not remedied by the DynDNS service. Thus if authentication is not done with certificates, but with preshared keys, you still cannot choose the ID Protect Mode, and the IDs (local and peer ID) have to be chosen and configured carefully (see "IDs in IPSec", page 66 for information on choosing IDs).

3 IPSec Menus – Overview

This chapter gives you an overview of the Setup Tool menus, fields and values relevant for BinTec's IPSec configuration. It describes the IPSec Wizard (section A, chapter 3.1, page 48) as well as all Menus collected under the IPSec main menu (section A, chapter 3.2, page 54 and following).

Remember that you need an IPSec license to be able to use IPSec. If you happen to have an IPSec software image, you can access the IPSec menu and enter a configuration even if you do not have a license. If, however, you activate IPSec on a router without a license, all IP traffic will be dropped! A warning message is displayed that you should disable IPSec.

After entering `setup` from the shell prompt, the Setup Tool's Main Menu is displayed as below. Depending on your hardware setup and software configuration your router's menu may differ:

```
BinTec Router Setup Tool                          BinTec Communications AG
                                                                  MyRouter

Licenses            System

LAN Interface:   CM-100BT, Fast Ethernet

WAN Interface:   CM-1BRI, ISDN S0

Serial-WAN: CM-Serial, Serial

WAN Partner
IP  PPP  Credits  IPSEC  QoS

Configuration Management
Monitoring and Debugging
Exit

Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to
enter
```

If you configure IPSec for the first time, a Setup Tool wizard will lead you through a partially automated configuration of several prerequisite tasks.

If you update your system software from any pre 6.2.2 release to release 6.2.2, make sure to start the IPSec Wizard once, even if you already have a functional IPSec configuration. System Software Release 6.2.2 offers a much larger number of IKE and IPSec proposals. These proposals are created by the IPSec Wizard, and if you do not allow the Wizard to run at least until it first prompts you for input, the new proposals will not be available.

An existing configuration is not changed by allowing the Wizard to run, and you can abort its operation at the first prompt. If your existing configuration is sound, the Wizard alternatively allows you to skip all prompts so that finishing the Wizard does not change your configuration, either.

3.1 The IPSec Setup Wizard

The IPSec Wizard quickly takes you through the process of determining a number of basic and essential parameters. When you enter the IPSec menu for the first time and choose to use the IPSec Wizard, the following menu will open:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][WIZARD]: IPSec Configuration - Wizard Menu              MyRouter

 IPsec 1st step configurations wizard

   Configuration History:



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

                                        Exit

Use <Space> to choose <Return> to select
```

There are only two options here if you enter the ***IPSec*** ➧ ***Wizard*** menu for the first time: You can either start the IPSec wizard by choosing *start wizard* in the **What to do?** field, or you can skip the entire IPSec Wizard by highlighting **EXIT** and pressing **Return**. If you start the wizard, information about the procedure and its results are displayed in the space below the heading **Configuration History**.

Note that you must allow the IPSec Wizard to start and complete the first two steps as described in "IPSec Wizard – Step 1 (NAT Settings)", page 51 and "IPSec Wizard – Step 2 (Proposal Creation)", page 51. This is necessary for the IPSec Wizard to create the IKE- and IPSec proposals which you will need irrespectivly of how you wish to configure an IPSec service.

If you do not want to use the IPSec Wizard for the configuration tasks proper, you can abort the process at the first prompt you are presented with (which is choosing an authentication method).

The menu window will then look like this (the screenshot shows a snapshot of the IPSec Wizard window at an arbitrary moment):

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][WIZARD]: IPsec Configuration - Wizard Menu              MyRouter

IPsec 1st step configurations wizard

   Configuration History:
   - Start IPsec wizard -                                                =
   Check NAT settings (ipNatOutTable/ipNatPresetTable) ...               |
     NAT disabled - no settings necessary                                |
   Check IKE default proposals ...                                       |
     created                                                             |
      - for ESP:  Blowfish/MD5,   DES3/MD5,  CAST/MD5 DES/MD5            |
                  DES3/SHA1,      CAST/SHA1, DES/SHA1                    |
      - for AH:   none/SHA1,      none/MD5                               |
   Check IPSEC default proposals ...                                     |
     created:                                                            |
      - for ESP:  NULL Rijndael Twofish Blowfish CAST DES DES3           |
                   MD5 SHA1 NOMAC                                        |
      - for AH:   SHA1 MD5                                               |
   Check IPSEC Default Authentication Method ...                         |
     changed from none to Pre Shared Keys                                |
   Check for public key pair ...                                         |
     created Key RSA 1024 e=65537                                        v

What to do?                                              clear config
                                                        (choose: <Space> )
                                                        (select: <Return>)

                                        Exit

Use <Space> to choose <Return> to select
```

The **What to do?** field can now take different values:

Possible Values	Meaning
clear config	This reverts all changes made to your configuration by the IPSec Wizard. After the configuration has been cleared you should choose to run the IPSec Wizard again. Any public key pairs stored on the router are not deleted by this command. This is to avoid accidentally invalidating your certificates.
dump messages	The router will store the messages printed to the Configuration History during IPSec Wizard operation either locally or on any configured syslog host. Refer you **User's Guide** for information on syslog messages and how to store them.
skip	This skips past a process that may be unnecessary (like enrolling for a certificate when you already have one).
abort	This option is available only when you choose not to perform a mandatory configuration step. It ends the IPSec Wizard like hitting **EXIT**. Only will you remain in the IPSec Wizard menu.
start (wizard)	This either starts a specific process like certificate enrollment or the wizard in general. The option is available only if there actually is anything to start.

Table A-1: **What to do?**

The IPSec Wizard can be accessed at any time from the ***IPSEC*** main menu. If you have completed some steps, but not others, you can continue where you have aborted the procedure. The IPSec Wizard allows you to either skip past all steps you have already completed or to go through them again.

3.1.1 The IPSec Wizard – Step by Step

The IPSec Wizard is not a menu in the strict sense, but a sequence of automated procedures. Its operation is divided into several steps. The menus the IPSec Wizard takes you to can be accessed at any later time from the ***IPSEC*** main menu; the paths to those menus are noted for each step, and the menus are described in chapters section A, chapter 3.2, page 54 and following.

Detailed information about what the IPSec Wizard does is printed to the message section of the Setup Tool window. Some steps the IPSec Wizard completes without any prompts for input. Most of these steps are not described here. If you want to keep track of the changes made by the IPSec Wizard, saving the syslog messages is a good idea.

IPSec Wizard – Step 1 (NAT Settings)

- The IPSec Wizard checks if NAT is activated on your router and if necessary adjusts the NAT settings so as to make sure IPSec functions properly and no data packets are unnecessarily dropped. If the IPSec Wizard makes any changes, they will be printed to the configuration history window of the Setup Tool.

IPSec Wizard – Step 2 (Proposal Creation)

- The IPSec Wizard creates possible combinations of encryption and message hash algorithms; no actual configuration is made here. You choose from the proposals created here in the ***IPSEC*** main menu, see section A, chapter 3.2, page 54.
  The IPSec Wizard defines a default combination of encryption and hash algorithms (Blowfish and MD5). You can later change this default setting.

IPSec Wizard – Step 3 (Authentication Method)

- The IPSec Wizard prompts you to decide for one of the available authentication methods. If no keypair is available, the IPSec Wizard creates a standard public key pair (1024 bit RSA key with public exponent=65537, called "automatic key RSA 1024 e65537").
  - If you choose *preshared_keys*, you are then taken to **Step 8** to configure your peer with the necessary preshared key.
  - If you choose a certificate based authentication method (*DSA, RSA, RSA encryption*), **Steps 4** to **7** are performed before peer configuration (for key generation: ***IPSEC*** ➧ ***CERTIFICATE AND KEY MANAGEMENT*** ➧ ***KEY MANAGEMENT*** (section A, chapter 3.9.1, page 92), for choosing the default authentication method: ***IPSEC*** ➧ ***IKE (PHASE 1) DEFAULTS*** (section A, chapter 3.7, page 89)).

IPSec Wizard – Step 4 (Certificate Enrollment)

- The IPSec Wizard checks if there are any own certificates installed for the key(s) found on your router. If the IPSec Wizard has created the key, you will be prompted whether you want to initiate a certificate enrollment.
  If you choose to request a certificate (you will need to know certain data to do this), the IPSec Wizard takes you to the certificate enrollment menu (***IPSEC*** ➧ ***CERTIFICATE AND KEY MANAGEMENT*** ➧ ***KEY MANAGEMENT*** ➧ **REQUEST CERT** ("Certificate Request", page 93)).

IPSec Wizard – Step 5 (Own Certificate)

- If you have either completed or skipped the certificate enrollment, the IPSec Wizard prompts you whether you want to download an own certificate. If you have not yet received your certificate, you can stop the wizard here and return to it at any other time.
  If you choose to import a certificate now, the IPSec Wizard takes you to the appropriate menu (***IPSEC*** ➧ ***CERTIFICATE AND KEY MANAGEMENT*** ➧ ***OWN CERTIFICATE*** ➧ **DOWNLOAD** ("Certificate Import", page 99)).

If you enroll for a certificate through a web interface and then copy/paste it to a word processor or directly into the Setup Tool: Make sure that what appears as line breaks really are line breaks (carriage returns). Some word processors will interpret the line breaks copied from the web interface as spaces, so that the entire certificate would be in a single line. Lines in the Setup Tool have a maximum length of 64 characters, and certificates cannot be entered in just one long line.

If you happen to do this though, an error message is displayed in the certificate review window.

IPSec Wizard – Step 6 (CA Certificate)

- Once you have imported an own certificate, the IPSec Wizard prompts you to download a Certificate Authority certificate. This is the certificate the CA your own certificate comes from uses to authenticate itself. You must import one for certificate based authentication to work properly.
  The IPSec Wizard takes you to the CA certificate menu (***IPSEC*** ➧ ***CERTIFICATE AND KEY MANAGEMENT*** ➧ ***CERTIFICATE AUTHORITY CERTIFICATES*** ➧ **DOWNLOAD** ("Certificate Import", page 99)).

IPSec Wizard – Step 7 (CRL Server/Peer Certificate)

- When both own and CA certificates have been imported, the IPSec Wizard prompts you to specify a server from which certificate revocation lists (CRLs) can be downloaded. This is necessary if no CRL distribution point is specified in the certificate itself and you have chosen RSA Encryption as authentication method. If you choose to specify a CRL server, the IPSec

Wizard takes you to the Certificate Servers menu (***IPSEC*** ➧ ***CERTIFICATE AND KEY MANAGEMENT*** ➧ ***CERTIFICATE SERVERS*** ➧ **ADD** (section A, chapter 3.9.4, page 103)).
If you do not specify a LDAP server, and if no CRL distribution point is specified in the certificate, and if you have chosen RSA Encryption for authentication, the IPSec Wizard prompts you to download a peer certificate. (***IPSEC*** ➧ ***CERTIFICATE AND KEY MANAGEMENT*** ➧ ***PEER CERTIFICATES*** ➧ **DOWNLOAD** ("Certificate Import", page 99)).

IPSec Wizard – Step 8 (Peer)

- Next, you are prompted to configure an IPSec peer. The IPSec Wizard takes you to the respective menu where you can add a peer entry (***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **APPEND** (section A, chapter 3.4.1, page 64)).

Once you have configured a peer, the default rule (the last one of the Post IPSec rules) is set to *pass*; otherwise all traffic that is not allowed by the peer traffic list entry you are prompted to configure in the next step would be dropped.

The router is now configured as an IPSec enabled standard router, i.e. it continues to route unprotected traffic and protects only such traffic as is specified by the peer traffic list entry you are about to create.

IPSec Wizard – Step 9 (Peer Traffic)

- When you have configured a peer, you are asked whether you want to configure a traffic list entry for the specific peer (***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **EDIT** ➧ **APPEND** (Traffic List, section A, chapter 3.4.6, page 83)).
  The IPSec Wizard allows you to configure one traffic entry only.

Step 9 concludes the IPSec Wizard. You now have a functional IPSec configuration that allows you to protect traffic that travels from your router to the peer you have configured. Which kind of traffic will be protected depends on the traffic list entry you have generated during IPSec Wizard operation.

3.2 IPSec Menus – *Main Menu*

After you have completed the IPSec Wizard process and have exited the respective menu window, the IPSec Main Menu opens. It looks like this:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC]: IPSec Configuration - Main Menu                        MyRouter

  Enable IPSec     : yes

  Pre IPSec Rules >
  Configure Peers >
  Post IPSec Rules >

  IKE (Phase 1) >
  IPsec (Phase 2) >
  Certificate and Key Management >

  Advanced Settings >
  Wizard >

  Monitoring >

                          SAVE                          CANCEL


Use <Space> to select
```

Note that you need to run the IPSec Wizard at least up to the first prompt it presents you with. At the first prompt you can abort the IPSec Wizard and continue configuration in the IPSec menus.

This is necessary because if you do not allow the IPSec Wizard to adjust your Network Address Translation settings and create the IKE- and IPSec proposals, additional configuration is mandatory. Part of the additional efforts (the creation of proposals) is not supported by the Setup Tool and would have to be done using the SNMP shell to edit the MIB tables.

The overall IPSec menu structure looks like this:

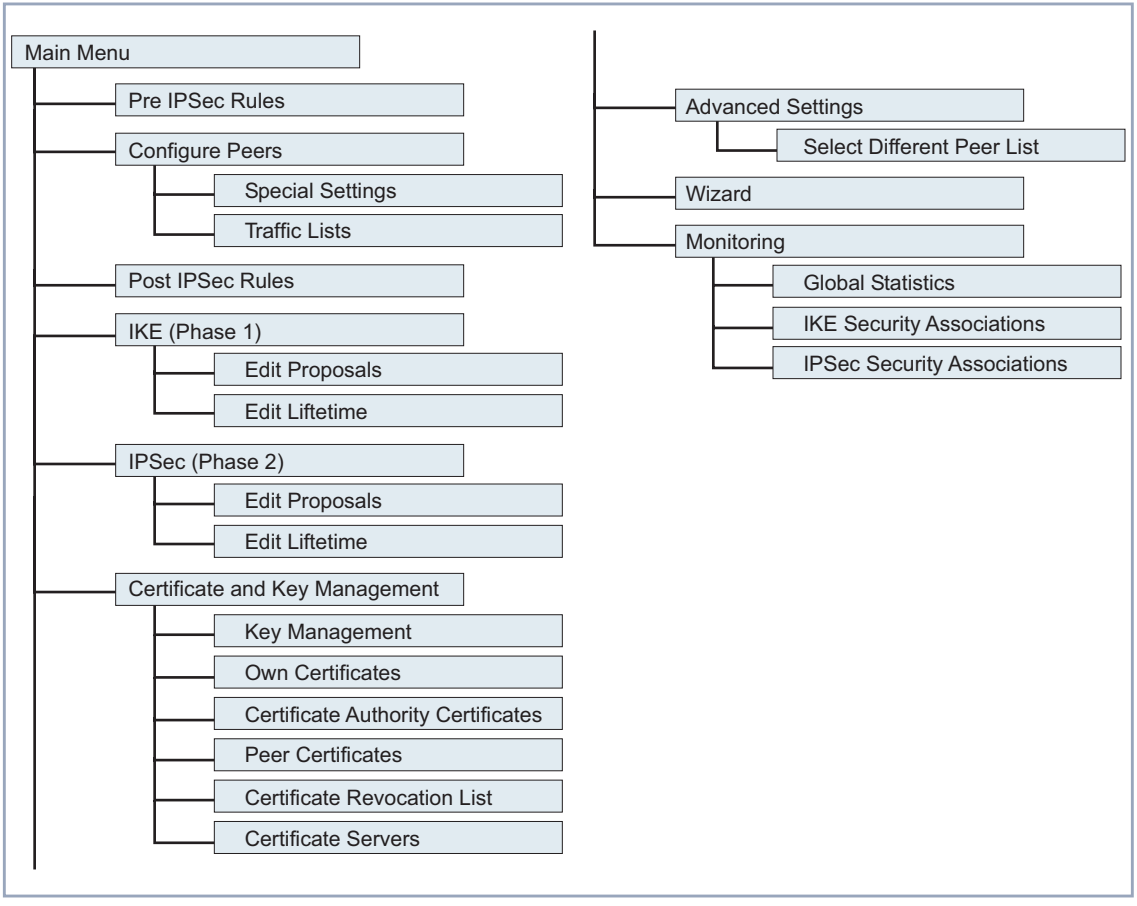


Figure A-16: IPSec menu structure

There is only one field in the ***IPSEC*** main menu where you can directly choose from a number of options: The **Enable IPSec** field.

Enable IPSec This field can take the following values:

Possible Values	Meaning
no	IPSec is not activated, independently of any configuration entered. If IPSec is currently activated, it is stopped as soon as you confirm with **SAVE**. As long as IPSec is not activated, none of the IPSec menus can be accessed.
yes	IPSec is activated as soon as you confirm with **SAVE**. If you do not have a valid IPSec license, all IP packets will be dropped until you deactivate IPSec again.

Table A-2: **Enable IPSec**

3.3 IPSec Menus – *PRE IPSEC RULES*

If you enable IPSec on your router, you must configure rules according to which traffic is handled before the IPSec SAs are applied. You must, e.g., allow specific packets to pass in plain text to enable certain essential functions.

In the first window of the ***PRE IPSEC*** menu, you find all previously configured rules displayed in a list:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][Pre IPSEC TRAFFIC]: IPSec Configuration -
                            Configure Traffic List              MyRouter

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

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




     APPEND              DELETE              EXIT

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

The values here are read-only and depend on the settings made in ***IPSEC*** ➧ ***PRE IPSEC RULES*** ➧ **APPEND/EDIT**. For further information on the setting, please see the following chapter ("The Submenu APPEND/EDIT", page 59).

The following parameters are displayed:

Field	Meaning
Local Address	Displays the local IP address of the rule.
M/R	Displays the length of the network mask (if the rule has been configured for a network) or the number of consecutive IP addresses if the rule has been configured for an IP address range. Thus *M32* stands for a 32 bit netmask (255.255.255.255, i.e. a single host) and *R10* for a range of 10 IP addresses counting from the one specified.
Port	Displays the local, respectively the remote, port number used to filter packets; applies only to UDP and TCP ports (*0* = any).

Field	Meaning
Proto	Displays the protocol used for filtering packets by this rule.
Remote Address	Displays the remote IP address of the rule.
A	Displays the action that is triggered by the rule. The filtered packets can be either dropped (*DR*), or be allowed to pass (*PA*) unchanged.
Proposal	Displays the IPSec proposal applied. In case of Pre IPSec rules this is without relevance, since there are no SAs applied to IP packets.

Table A-3: ***IPSec*** ➧ ***Pre IPSec Rules***

There is one option for you to configure here: You can specify which of the traffic list entries is the first active rule in the rule chain. Additionally you can move the rules you have defined up and down within the list, and thus you can shape the Pre IPSec rules according to your needs. Any rule prior to the rule specified as "active traffic list" is ignored. How to select the active traffic list is described in the help section of the menu window.

3.3.1 The Submenu APPEND/EDIT

Pre IPSec rules are either edited or added in the ***IPSEC*** ➧ ***PRE IPSEC RULES*** ➧ **APPEND/EDIT** menu The menu window that opens looks like this in both cases (if you edit an existing entry, the values for this entry are displayed):

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][Pre IPSEC TRAFFIC][ADD]: Edit Traffic Entry            MyRouter

Description:


     Protocol:      dont-verify

     Local:
          Type: net   Ip:                / 0

     Remote:
          Type: net   Ip:                / 0


     Action:        pass

                    SAVE                                  CANCEL
```

The fields in this menu have the following possible values:

Field	Meaning
Description	Enter a description that allows to identify the kind of rule you have defined.
Protocol	You can specify if the traffic considered for this rule is applied only to the packets of a specific protocol. You can choose between specifying a protocol and the option *dont-verify*, which means that the protocol is not used as a filter criterion.
Local: Type	Enter the local address settings. For details, see table A-5, page 61 below.

Field	Meaning
Remote: Type	Enter the remote address settings. The options are largely identical with the options in the **Local: Type** field, with one exception: The option *own* does not exist and is replaced with the option *peer*. This, however, is relevant only in peer configuration.
Action	You can choose between two options here: ■ *pass* ■ *drop* For details, see table A-6, page 61 below.

Table A-4: ***IPSec*** ➧ ***Pre IPSec Rules*** ➧ **APPEND/EDIT**

Local/Remote: Type These are the options for the **Local/Remote: Type** field:

Possible Values	Meaning
host	Specify the IP address of a single machine to fall under this rule. If you have chosen certain protocols to narrow down the traffic considered, you may be prompted to specify a **Port** number. This, however, applies to UDP and TCP protocols, only.
net	Specify the IP address of a local network and the corresponding netmask to fall under this rule. The prompt for the netmask appears automatically when you choose *net*. It is separated from the IP address prompt by a "/". Again, you may be prompted to specify a **Port** number.

Possible Values	Meaning
range	Specify a range of IP addresses to fall under this rule. The prompt changes automatically to allow entering two IP addresses, separated by a "-". Again, you may be prompted to specify a **Port** number.
own/peer	If you choose this option, the dynamic IP address of the router (if applicable) will be automatically assumed to fall under the rule. No further adjustments are necessary. Even though this entry can be chosen here, it is not functional for Pre IPSec rules. It is significant for peer configuration (see section A, chapter 3.4.6, page 83).

Table A-5: **Local: Type**

Action These are the options for the field **Action**:

Possible Values	Meaning
pass	This option will allow the packets specified to pass IPSec unchanged.
drop	This option will have any packet that matches the configured filters dropped.

Table A-6: **Action**

Make sure to carefully configure the Pre IPSec rules. They are essential for the proper functioning of all traffic that is not to be protected by IPSec procedures.

It is especially important to let IKE traffic pass in plain text. This can be accomplished by specifying a Pre IPSec rule with the following specifications:

- **Protocol**= *udp*
- **Local Type**: *net* (leave the fields for IP address and netmask empty)
- **Local Port**: *500*
- **Remote Type** : *net* (again, leave the fields for IP address and netmask empty)
- **Remote Port**. *500*
- **Action**: *pass*

The IPSec Wizard will adjust the settings if it is necessary.

3.4 IPSec Menus – *CONFIGURE PEERS*

In this menu you can configure the peer lists. IPSec operates with just a single peer list, but you can define more than one list, save it on the router and switch between them. See section A, chapter 3.10, page 103 for further information.

You can choose an arbitrary peer to be the first active peer in the list. Any peer that is higher in the list will remain inactive, i.e. connections with this peer are not possible and their traffic lists are ignored.

Note that any change of the entry point of the peer list is immediately effective without further confirmation.

Upon entering the ***CONFIGURE PEERS*** menu, you see a list of already configured peers:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][PEERS]: IPSec Configuration - Configure Peer List      MyRouter

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

Description    PeerID          PeerAddr         IKEProp    TrafficList
*peer_1        peer_1          198.16.13.1      default             5
 peer_2        peer_2          198.16.13.2      default             6




     APPEND              DELETE              EXIT
```

You can organize the list entries according to the help section in the menu window, and you can edit or add/insert entries to the list.

The following settings are displayed; again, they are read-only and depend on the settings made in the **APPEND/EDIT** menu (see section A, chapter 3.4.1, page 64):

Field	Meaning
Description	Displays the description of the peer.
PeerID	Displays the peer ID. See "IDs in IPSec", page 66 for further information.
PeerAddr	Displays the peer's IP address. When using ID Protect Mode and preshared keys, the peer's IP address must be specified.
IKEProp	Displays the IKE proposal that will be used. You can choose from the proposals created by the IPSec Wizard in the **APPEND/EDIT** menu.
TrafficList	Displays the index number of the traffic list configured for this peer.

Table A-7: ***IPSEC*** ➧ ***CONFIGURE PEERS***

3.4.1 The Submenu APPEND/EDIT

Existing entries are edited and new entries are created in the ***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **APPEND/EDIT** menus. Both menus are accessed from the ***IPSEC*** ➧ ***CONFIGURE PEERS*** menu.

APPEND

If you want to add a peer to you peer list, you have to access the APPEND menu. In this menu you can only specify the basic parameters of the peer. Further editing of the peer settings is made in the **EDIT** menu.

The **APPEND** menu looks like this:

```
BinTec Router Setup Tool                      BinTec Communications AG
[IPSEC][PEERS][ADD]: IPSec Configuration -
                     Configure Peer List                      MyRouter

     Description:
     Peer Address:
     Peer IDs:




                        SAVE                CANCEL
```

For a description of the fields in this menu, see the description of the **EDIT** menu below.

EDIT

In order to configure traffic lists for a peer and adjust the basic as well as special settings to your needs, you have to access the ***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **EDIT** menu.

It looks like this (the screenshot shows an existing peer for which so far no traffic lists have been configured):

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][PEERS][EDIT]: IPSec Configuration -
                      Configure Peer List                       MyRouter


     Description: My_Peer
     Peer Address:192.168.13.1
     Peer IDs:191.168.13.1
     Pre Shared Key:

     Special Settings >

Traffic List: 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


      APPEND             DELETE             SAVE              CANCEL
```

To configure a peer, only few settings have to be made:

Field	Meaning
Description	Enter a name for the peer.
Peer Address	Enter the peer's IP address or a resolvable host name, alternatively. If neither is known, you can leave this field empty, but in Main Mode only certificate based authentication will be functional, and in Aggressive Mode you need to configure Peer IDs.

Field	Meaning
Peer ID	Enter the ID the peer will have to use for authentication. If you want to accept any ID from your peer, leave this field empty. In this case, however, there must be other ways to identify the peer, i.e. either a static IP address or a certificate. Note that if you want to use the ID Protect Mode and preshared keys for authentication, the Peer Address must be known.
Pre Shared Key	(This field appears only if you have chosen pre-shared keys as authentication method.) Enter a random key. You will be prompted to re-enter it. Make sure that the settings are configured identically by the peer. Note that if you ever change the authentication method from certificate based to preshared key authentication, it is here where you enter the key while you change the authentication settings in ***IPSec*** ➧ ***Configure Peers*** ➧ **EDIT** ➧ ***Special Settings*** ➧ ***Phase 1***.

Table A-8: ***IPSec*** ➧ ***Configure Peers*** ➧ **APPEND/EDIT**

IDs in IPSec

When configuring IPSec you will encounter two types of IDs: so called Peer IDs and Local IDs. Both are used to mutually identify peers. These IDs must be chosen carefully, since if they are configured incongruently on the peer routers, Phase 1 cannot be completed and no connection is established. There is, however, a simple scheme for choosing IDs, one for authentication with certificates, one for authentication with preshared keys.

- IDs in certificate authentication
  Certificates are designed to identify the certified user, i.e. when using certificates, you should use the ID contained in the certificate, the Subject Name (see section A, chapter 2.4, page 36).
  Thus, Peer1 would choose the X.509 name contained in Peer 2's own certificate as Peer ID for Peer 2, and the X.509 name contained in his or her own certificates as Local ID (see "Phase 1: Local ID", page 78).

- IDs in preshared keys authentication
  Things are a little different with preshared keys. Since no certificate is available, another token must be used to identify a peer. If both peers have static IP addresses, it is a good idea to use those as identifiers. Thus Peer 1 would use Peer 2's static IP address as Peer ID and his or her own static IP address as Local ID (again, see "Phase 1: Local ID", page 78).
  This, however, is not possible if one of the peers has a dynamic IP address. In this case, a random ID must be chosen for the peer with the dynamic IP address. Thus, if Peer 1 has a static IP address, he would use his static IP address as Local ID and the randomly chosen ID as Peer ID for Peer 2. Peer 2 would choose the same randomly chosen ID as Local ID and Peer 1's static IP address as Peer ID for Peer 1.

3.4.2 The Submenu EDIT – *SPECIAL SETTINGS*

From the submenu ***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **EDIT** you can enter the menu ***SPECIAL SETTINGS***. It looks like this:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][PEERS][EDIT]: IPSec Peer Special Settings                MyRouter

     Options:

       Verify Padding:        yes
       Granularity:           default (coarse)
       Keep Alive:            no

     Phase 1 >
     Phase 2 >

     Select Different Traffic List >

                          SAVE                              CANCEL
```

Here you can configure security parameters for the peer you are editing. There are three fields in which you can directly choose from different options as well as three further menus.

There are default values for all settings you can configure here. If you do not specify any values, these default values are assumed. E.g. the values configured in ***IPSEC*** ➧ ***IKE (PHASE 1) DEFAULTS*** are assumed for Phase 1 and the values configured in ***IPSEC*** ➧ ***IKE (PHASE 2) DEFAULTS*** for Phase 2.

The parameters **Verify Padding**, **Granularity** and **Keep Alive** cannot be configured in the Phase 1 or Phase 2 default menus. They represent options that are of interest mainly for specialized configurations and need not be changed.

Verify Padding

Possible Values	Meaning
yes	The router verifies if the padding of ESP packets received complies with RFC 2406. If this is not the case, the packets are dropped. This is the default setting.

Possible Values	Meaning
no	The padding of ESP packets is not checked, and packets are accepted even if the padding is not RFC compliant.

Table A-9: **Verify Padding**

Granularity

Possible Values	Meaning
default	The router uses the granularity specified in the **ipsecGlobals** table.
coarse	The router uses the coarsest granularity as specified by the traffic entry.
ip	The router negotiates one SA pair per host pair, i.e. for each pair of peers specified in a traffic entry.
proto	The router negotiates one SA pair per protocol specified in the traffic list entry (e.g. TCP, UDP, ICMP).
port	The router negotiates one SA pair per session. This setting results in a large number of SAs which may exhaust the system resources of your router.

Table A-10: **Granularity**

Keep Alive

Possible Values	Meaning
no	An SA is rekeyed at the end of its lifetime only if at least one packet has been encapsulated using this SA. Otherwise the SA is deleted. This is the default setting.

Possible Values	Meaning
yes	An SA is rekeyed at the end of its lifetime irrespective of whether any packets have been encapsulated using it or not. This has the effect that the tunnel is not dropped, and a peer with a dynamic IP address can still be reached. Note, however, that keeping the tunnel up may incur costs.

Table A-11: **Keep Alive**

3.4.3 The Submenu EDIT – *SPECIAL SETTINGS* – *PHASE 1*

From the ***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **EDIT** ➧ ***SPECIAL SETTINGS*** menu you can access another two submenus where you can configure specific IKE and IPSec proposals to be used with this peer: In the ***PHASE 1*** menu, you can choose IKE settings. In future software releases it will even be possible to edit and/or add proposals.

The parameters you choose here determine how IKE Phase 1 as illustrated in figure A-10, page 33 is negotiated with this peer.

It looks, e.g., like this:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][PEERS][EDIT][PHASE 1]: IPSec Configuration -
                                Phase 1 (IKE) Settings          MyRouter

   Proposal              :  1 (Blowfish/MD5) (def)
   Lifetime              :  900 Sec/0 Kb (def)
   Group                 :  1 ( 768 bit MODP) (def)
   Authentication Method :  RSA Encryption (def)
   Mode                  :  id_protect RSA (def)
   Local ID              :
   Local Certificate     :  2 (zu_1)

   View Proposals >
   Edit Lifetimes >


                          SAVE                          CANCEL
```

The fields of this menu are described below.

The "(def)" you can see behind the values in he screen above means that the configuration for this peer uses the default settings made in ***IPSEC ➧ IKE (PHASE 1) DEFAULTS***.This means that if you change the default values there, the values here will change, too.

Phase 1: Proposal

This field allows you to choose any combination of encryption and message hash algorithms your router can use for IKE Phase 1. The combination of six encryption algorithms and four message hash algorithms yields 24 possible values for this field. Additionally you can choose not to apply any encryption/message hash combination.

Please note that as long as you choose *none* as a value for this field, IPSec will not be functional for this peer.

The next two tables list the available encryption and message hash algorithms:

Algorithm	Description
Blowfish	Blowfish is a fairly strong algorithm which is fairly fast, also. Twofish might be considered the successor of Blowfish.
3DES	3DES is an extension of the DES algorithm with an effective key length of 112 bits, considered strong today. The slowest algorithm supported by now.
DES	DES is an older encryption algorithm which is now considered weak because of its short effective key length of 56 bit.
CAST	CAST also is a quite strong algorithm a bit slower than Blowfish but still much faster than 3DES.
Twofish	Twofish was one of the final candidates for AES (Advanced Encryption Standard). It can be considered equally secure as Rijndael (AES), but is slower.
Rijndael	Rijndael has been chosen as AES for its quick key setup, low memory requirements, for its high security against attacks and for its overall speed.

Table A-12: Encryption algorithms

These are the hash algorithms available:

Algorithm	Description
MD5 (Message Digest #5)	MD5 is an older hash algorithm. Used with 96 bit of digest length for IPSec.
SHA1 (Secure Hash Algorithm #1)	SHA1 is a hash algorithm designed by the NSA (United States National Security Association). It is considered secure, but is slower than MD5. Used with 96 bit of digest length for IPSec
RipeMD 160	RipeMD 160 is a 160-bit cryptographic hash function. It is intended to be used as a more secure replacement for MD5 and RipeMD.
Tiger 192	Tiger 192 is a fairly new and very fast hash algorithm.

Table A-13: Message hash algorithms

Please note that the descriptions of the encryption and authentication or hash algorithms are based on the knowledge and the personal opinion of the author at the time this document was written. Especially the strength of an algorithm can hardly be specified in an absolute way and may change due to progress in mathematics or cryptography.

In future implementations you will be able to edit the existing proposals or create specific ones in the menu ***PHASE 1*** ➧ ***VIEW PROPOSALS***. For the time being,

once you enter the menu, you will see a list of all the proposals created by the IPSec Wizard:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][IKE PROPOSALS]: IKE Proposal                              MyRouter


    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
```

Note that the function of editing or adding IKE proposals should be used primarily by experienced users. Changing a proposal might affect other configurations that make us of the same proposal, and creating a new one only makes sense if specific security associations are imperative.

Phase 1: Lifetime This field displays the lifetime that is allowed to pass before phase-1 keys have to be refreshed by another Diffie-Hellman exchange. It can either be configured as a value in seconds, as an amount of data processed (in Kb) or as a combination of both. The default value is *900 sec/11000 Kb* which means that the keys are refreshed depending on whether 900 seconds have passed or 11000 Kb of data have been processed first. If you have configured any additional lifetimes you can choose among them here.

If you decide to configure additional lifetimes, you can do so in the ***EDIT LIFETIMES*** menu which is accessible from the***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **EDIT** ➧ ***SPECIAL SETTINGS*** ➧ ***PHASE 1*** menu. The mask looks like this:

```
BinTec Router Setup Tool                    BinTec Communications AG
[IPSEC][LIFETIME]: IPsec Configuration - Life Times          MyRouter

     Edit Lifetime Values

          Lifetime Restriction Based On: Time and Traffic
               900          Seconds
               11000        Kb


                    SAVE                                  Exit
```

The menu comprises the following fields:

Field	Meaning
Lifetime Restriction Based On	Choose the criterion for ending the key lifetime, possible values: ■ *Time and Traffic* ■ *Time* ■ *Traffic* Depending on your choices you will see either of the next fields or both.
Seconds	Enter the lifetime for phase-1 keys in seconds. The value can be any 32 bit integer value.
Kb	Enter the lifetime for phase-1 keys as determined by the amount of processed data in Kb.The value can be any integer value up to 32 bit.

Table A-14: ***IPSEC*** ➧ ***LIFETIME***

Phase 1: Group

The group defines the set of parameters used for the Diffie-Hellman agreement during Phase 1. "MODP" as supported by BinTec routers stands for "modular exponentiation". There are three different primes that can be applied using 768, 1024 or 1536 bit.

The field can take the following values:

Possible Values	Meaning
1 (768 bit MODP)	768 bit modular exponentiation will be used during the Diffie-Hellman exchange to generate the keying material.
2 (1024 bit MODP)	1024 bit modular exponentiation will be used during the Diffie-Hellman exchange to generate the keying material.
5 (1536 bit MODP)	1536 bit modular exponentiation will be used during the Diffie-Hellman exchange to generate the keying material.

Table A-15: **Phase 1: Group**

Phase 1: Authentication Method

This field displays the authentication method you have chosen during IPSec Wizard configuration and allows you to change it:

Possible Values	Meaning
none	This means that so far no authentication for the phase-1 exchanges has been configured. You will now have to choose one of the options offered, since Phase 1 is not functional without authentication. This value is not an option if you change peer settings, but i it possible that it is activated, nevertheless, if *none* is chosen in the ***IPSec*** ➧ ***IKE Phase 1) Default*** menu, and if the peer is configured to use the global defaults. In this case it will appear as *nonexistent (def)*.

Possible Values	Meaning
Pre Shared Keys	If you do not want to use certificates for authentication, you can choose *Pre Shared Keys*. These are configured during peer configuration in ***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **EDIT**.
DSA Signatures	Phase-1 exchanges are authenticated using the DSA algorithm. For further information on the DSA algorithm, see section A, chapter 2.1.2, page 19.
RSA Signatures	Phase-1 exchanges are authenticated using the RSA algorithm. For further information on the RSA algorithm, see section A, chapter 2.1.2, page 19.
RSA Encryption	With RSA Encryption the ID payload is additionally encrypted for extra security.
... (def)	You will see this value (which is composed of any of the available authentication methods and the *(def)* "suffix") if you have configured the peer to use the global defaults.

Table A-16: **Authentication Method**

Phase 1: Mode The mode field displays the currently configured phase-1 mode and allows to change the settings:

Possible Values	Meaning
id_protect	This mode (also called Main Mode) requires six messages for a Diffie-Hellman exchange and thus for creating the secure channel over which the IPSec SA proper is negotiated. It presupposes that both peers have static IP addresses if preshared keys are used for authentication.

Possible Values	Meaning
aggressive	Aggressive Mode is required if one of the peers does not have a static IP address and pre-shared keys are used for authentication, and it only requires three messages for creating a secure channel.

Table A-17: **Mode**

In ID Protect Mode the peers' IDs are encrypted. This is not a problem if authentication is done with certificates, since they provide a unique ID for all peers. If authentication is done with preshared keys, however, the IDs must be exchanged before the keys are, and since the IDs are encrypted, the router needs a static IP address entry to select the appropriate key. Therefore, pre-shared key authentication cannot be used in ID Protect Mode with dynamic IP addresses.

Since no payloads are encrypted in Aggressive Mode, this can be used if one of the peers has a dynamic IP address only. It does, however not provide for identity protection.

Phase 1: Local ID

This is the ID you give your router. If you leave this field empty, the router chooses default values. These are:

- for preshared key authentication: the local IP address as specified by the **ipsecPeerLocalAddress** field in the **ipsecPeerTable**
- for certificate authentication: the first subject alternative name specified in the certificate or, if none is specified, the subject name of the certificate.

If you use certificates for authentication and your certificate contains Subject Alternative names (see "Certificate Request", page 93), you must pay attention here, since the router per default chooses the first subject alternative name. Make sure that 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 allows you to choose any one of your own certificates for authentication. It displays the index number of that certificate and the name it has been stored under. This field is only shown in certificate based authentication settings; specifying a certificate is mandatory.

3.4.4 The Submenu EDIT – *SPECIAL SETTINGS* – *PHASE 2*

From the ***SPECIAL SETTINGS*** menu you can also access the ***PHASE 2*** menu. Like in the Phase 1 menu, you can choose IPSec security association parameters to be specifically used with this peer; with upcoming implementations you will be able to edit existing or create custom proposals, this time for IPSec.

The parameters you choose here largely determine how IKE Phase 2 as illustrated in figure A-11, page 35 is negotiated with this peer.

The menu looks like this:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][PEERS][EDIT][PHASE 2]: IPSec Configuration -
                                Phase 2                          MyRouter


   Proposal              :         1 (ESP(All(No Des)/All)) (def)
   Lifetime              :         900 Sec/0 Kb (def) (def)
   Use PFS               :         no (def)IPSec


   View Proposals >
   Edit Lifetimes >


                         SAVE                              CANCEL
```

The fields of this menu are described below.

Phase 2: Proposal

This field allows you to choose any combination of an IPSec protocol, an encryption algorithm and/or a message hash algorithm. The following tables display the elements of these potential combinations:

IPSec Protocol	Description
ESP (Encapsulated Security Payload)	ESP offers payload encryption as well as authentication. For further information, see section A, chapter 2.2, page 21.

IPSec Protocol	Description
AH (Authentication Header)	AH offers authentication alone, but no payload encryption. For further information, see section A, chapter 2.2, page 21. If you choose any combination involving the AH protocol, *none* is shown as encryption algorithm, e.g. *(AH (none, MD5)).*

Table A-18: IPSec protocols

In addition to encryption and authentication, BinTec's IPSec implementation supports compression of IP payloads through IPComP (IP Payload Compression Protocol). IP payload compression is a protocol to reduce the size of IP datagrams. This protocol will increase the overall communication performance between a pair of communicating hosts/gateways ("nodes"). It compresses the datagrams, provided the nodes have sufficient computation power, through either CPU capacity or a compression coprocessor, and the communication is over slow or congested links.

IP payload compression is especially useful when encryption is applied to IP datagrams. Encrypting the IP datagram causes the data to be random in nature, rendering compression at lower protocol layers (e.g., PPP Compression Control Protocol [RFC1962]) ineffective. If both compression and encryption are required, compression must be applied before encryption.

All IPSec proposals that do not specify a setting for IPComP are IPComP enabled. This means that during SA negotiation they will accept all proposals irrespectively of whether they suggest the use of IPComP or not. If the local machine initiates the negotiation, it suggests the use of IPComP as preferred proposal, but allows the responder to choose a non-IPComP proposal.

You can change this behavior by choosing an IPSec proposal which specifies one of the following settings for ➤➤ **IPComP**:

IPComp Option	Description
no Comp	Your router will not accept SAs that specify the use of IPComp. If the peer has configured his or her router to propose IPComP, IPSec SA negotiation fails and no connection is made.
force Comp	Your router requires that IPComP can be agreed upon in negotiation the IPSec SA. If the peer does not accept this, no connection is made.

Table A-19: IPComP options in IPSec proposals

Since the principal encryption and hash algorithms have already been described, they are simply listed here. Only the NULL algorithm is not available in Phase 1:

Algorithm	Description
Blowfish	See table A-12, page 72 for descriptions of the encryption algorithms.
3DES	
DES	
CAST	
Twofish	
Rijndael	
NULL	The NULL "algorithm" does not change the IP packet in terms of encryption, but is necessary if IP packets need authentication through the ESP protocol without encryption.

Table A-20: Phase-2 encryption algorithms

These are the available hash algorithms:

Algorithm	Description
MD5	See table A-13, page 73 for description of the message hash algorithms.
SHA1	
NULL	If the NULL "algorithm" is applied for authentication, no message hash is created under ESP and the payload is only encrypted.

Table A-21: Phase-2 message hash algorithms

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

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

A phase-2 proposal would thus, e.g. look like this:

Example Values	Meaning
1 (ESP(Blowfish, MD5))	IP packets will be processed using the ESP protocol, Blowfish encryption and MD5 message hash.
10 (ESP(NULL, SHA1))	IP packets will be processed using the ESP protocol; the NULL encryption and SHA 1 will be used to create the message hash.
16 (AH(none, MD5))	IP packets will be processed using the AH protocol, no encryption and MD5 is used as message hash algorithm.

Table A-22: Examples for **Phase 2: proposals**

Just like future releases will enable you to edit Phase 1 Proposals, you will be able to edit exiting proposals or create custom ones. The menu ***VIEW PROPOSALS*** is very similar to the one described in "Phase 1: Proposal", page 71. Only are the proposals displayed here IPSec proposals and not IKE proposals.

Phase 2: Lifetime For information on the proposal's life time, see "Phase 1: Lifetime", page 74. If you want to create a specific IPSec SA lifetime for this peer, you can do so in the menu ***PHASE 2*** ➧ ***EDIT LIFETIME***.

Use PFS Since PFS (Perfect Forward Secrecy) requires another Diffie-Hellman exchange to create fresh keying material, you have to choose the exponentiation characteristics. If you activate PFS, the options are the same as in **Phase 1: Group** configuration ("Phase 1: Group", page 76). PFS is used to protect the keys of a rekeyed phase-2 SA even if the keys of the phase-1 SA have been compromised.

3.4.5 The Submenu EDIT – *SPECIAL SETTINGS* – *SELECT DIFFERENT TRAFFIC LIST*

In this menu the traffic lists configured for this peer are displayed. If you have configured more than one traffic list, you can choose which one to activate. A list of all available traffic lists will be displayed and you can choose among them as is described in the help section of the menu window. See section A, chapter 3.3, page 56 for a description of the menu.

3.4.6 The Submenu EDIT – APPEND/EDIT (Traffic Lists)

You need to configure a traffic list for the peer you have just created. If you are editing an already existing peer, the traffic list is displayed in the lower part of the ***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **EDIT** menu The menu is almost the same as for Pre IPSec Rules configuration, (section A, chapter 3.3.1, page 59). Only will you find an additional value for the **Action** field: If you choose *protect*, any packet matching the filter will be protected according to the settings specified in the phase-1 and phase-2 proposals.

If you are creating a new peer, the **APPEND** option for peer traffic lists is not immediately available. You first need to save your peer. Then you can access the **EDIT** menu for that peer from the ***CONFIGURE PEERS*** menu. This has been done to avoid orphan traffic list entries should peer creation be aborted after configuring the traffic list entries.

Moreover the options *peer* and *own* as values for the **type** field are significant here, but only in combination with the *protect* option. They take the local or remote addresses as values and will allow, e.g., for IPSec tunnels between an PC running IPSec client software and a security gateway.

The Submenu EDIT – APPEND/EDIT (Traffic Lists) – *SPECIAL SETTINGS*

If you choose *protect* as **Action** for the newly configured list entry, you additionally can access another ***SPECIAL SETTINGS*** menu (***IPSEC*** ➧ ***CONFIGURES PEERS*** ➧ **EDIT** ➧ **APPEND/EDIT** (Traffic Lists) ➧ ***SPECIAL SETTINGS***):

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][PEERS][EDIT][TRAFFIC][SPECIAL]: Customize Traffic
                                        Settings              MyRouter

     Proposal:           default (ESP(All(No Des)/All))
     Lifetime:           900 Sec/0 Kb (def)

     Keep Alive:         default
     Force Tunnel Mode:  false
     Granularity:        default (coarse)

     View Proposals >
     Edit Lifetimes >

                    SAVE                                CANCEL
```

Here you can specifically modify the IPSec settings for the traffic specified by the rule you have created. The menu offers a combination of options available in two other menus: ***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ ***EDIT*** ➧ ***SPECIAL SETTINGS*** and ***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ ***EDIT*** ➧ ***SPECIAL SETTINGS*** ➧ ***PHASE 2***. For information on the fields and possible values, see section A, chapter 3.4.2, page 68 and section A, chapter 3.4.4, page 79. The values that

are displayed when you first enter this menu are the ones you have configured for the peer in general.

Force Tunnel Mode

There is, however, one field that does not appear in any of the other menus, the **Force Tunnel Mode** field. It can either take the value *true* or the value *false*. If you activate this option your router will use the protocol chosen (ESP in the example screen above) in Tunnel Mode, even if Transport Mode would be possible. For information on Transport and Tunnel Mode, see section A, chapter 2.2.3, page 25.

3.5 IPSec Menus – *POST IPSEC RULES*

Just as you have to configure Pre IPSec Rules that apply to all traffic before IPSec SAs are applied, you need to configure Post IPSec Rules that are applied once a packet has passed the peer traffic lists, i.e. if no traffic list entries have matched the packet.

If your configuration is sound, then you may need to configure only a single Post IPSec Rule, since all packets that need to be dropped or passed are handled by the Pre IPSec Rules and all packets that need be protected are handled by the Peer Traffic Lists. Thus the only decision you will have to make here is whether to drop all "left-over" packets or whether to let them pass. This decision is made by choosing a value for the field **What to do with anything that didn't match** which you find in the first window of the ***IPSEC*** ➧ ***PRE IPSEC RULES*** menu.

This field can take the following values:

Possible Values	Meaning
drop it	All packets that do not match any of the IPSec rules are dropped after IPSec has been applied.
let pass	Alternatively, all packets not covered by the IPSec rules can be allowed to pass.

Table A-23: **What to do with anything that didn't match**

3.6 Some Words on Filtering

Filtering specific packets from the IP traffic and specifying what is to be done with them is at the core of IPSec configuration. Basically the filtering done by the IPSec traffic lists functions in a similar way as IP access lists do (see your **User's Guide** for IP access lists).

The basic procedure is as follows: You define which packet is to be processed in a specific way. To filter the packet you can choose from a variety of options like the source IP address and the source port of the packet or the protocol that is used (like e.g. TCP or FTP). You then specify what is to be done with this packet (e.g. that it has to be dropped), and thus create a rule. If you define a number of rules, each rule will have an index number and a rule chain is created.

Every packet arriving at the router either from the LAN or the WAN has to pass through this rule chain and is checked for matches with any of the rules within the chain. As soon as a packet matches a rule, the rule is applied, i.e. if a rule says that a certain packet has to be dropped, then this packet is dropped immediately and other rules that would eventually match the packet are not effective. Therefore, the exact sequence of rules within the chain is important: A "drop" rule in an early position might block traffic you do not want to block indiscriminately, and a "pass" that comes too late might disable e.g. IKE.

The following figure shows the details of IPSec traffic filtering. Note that the Pre IPSec rules, the IPSec (Peer) traffic lists and the Post IPSec rules all form a single rule chain:

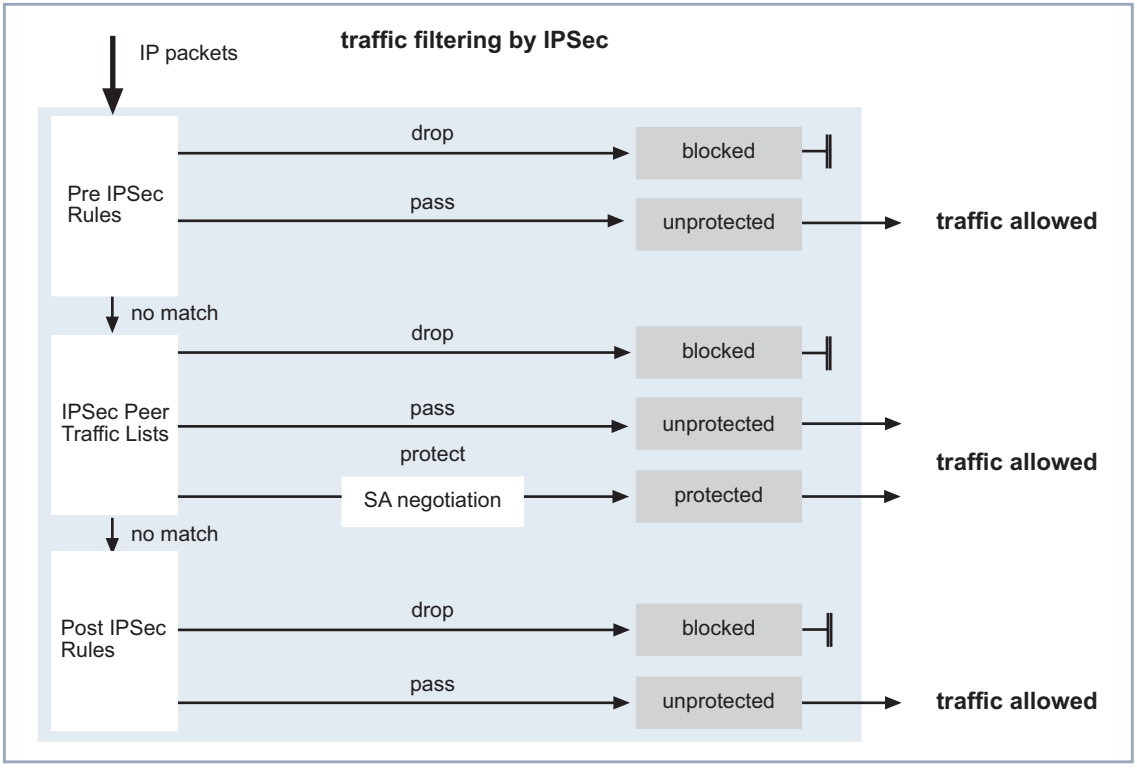


Figure A-17: IPSec filter rules

IPSec filters do not replace IP access lists, but are applied additionally. In case of inbound traffic IPSec filters are applied before IP access lists, in case of outbound traffic they are applied after IP access lists. This means that any packet that is dropped by IPSec is ultimately lost even if it would have been allowed by the IP access lists. Likewise, a packet that is allowed by IPSec, but dropped by the IP access lists, is ultimately lost. So careful configuration of both list sets is essential.

The following figure illustrates the sequence of filter application for inbound traffic. The IPSec (inbound) filters are applied before IP access lists:

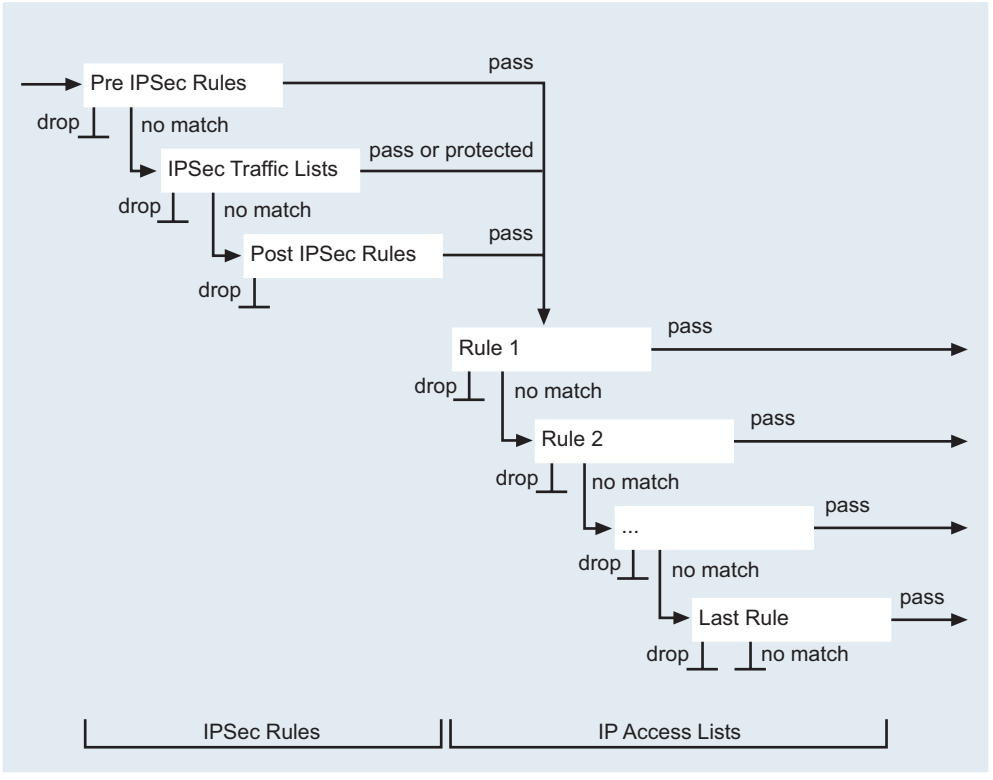


Figure A-18: Filter Sequence

Making a Decision

An IPSec connection is realized through any of the WAN interfaces you have configured on your router; IPSec rules are applied independently of WAN interfaces, i.e. it does not make a difference whether IPSec rules are applied to traffic that is realized through interface 1 or through interface 2. This is different with IP access lists: they are applied to the WAN interfaces specifically. IP access

lists are, therefore, very flexible, but need much configuration if you want to organize the rule set for each WAN interface separately.

If there are no IP access rules at all, then traffic is passed on, but if there are any rules, and a packet that matches none of them is discarded. So if you do not define any IP access rules at all, all packets allowed by IPSec will be routed, while a single active rule causes all packets that do not match this rule to be dropped. So if you configure any IP access lists, you will either have to ensure that every kind of traffic that needs to be passed is actually covered by a rule; or you need to configure a last rule that allows all traffic not covered by any of the rules in the IP access lists to pass.

3.7 IPSec Menus – IKE (Phase 1) Defaults

In this menu you can configure the basic parameters for all IKE exchanges. These parameters will be used for each peer as long as no special configuration has been made for the relevant peer in ***PEER CONFIGURATION*** ➧ ***SPECIAL SETTINGS*** ➧ ***PHASE 1***.

The menu looks like this when you enter it for the first time:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][PHASE 1]: IPSec Configuration -
                  Phase 1 (IKE) Settings                        MyRouter

   Proposal              :  1 (Blowfish/MD5)
   Lifetime              :  900 Sec/0 Kb (def)
   Group                 :  1 ( 768 bit MODP)
   Authentication Method :  RSA Signatures
   Mode                  :  id_protect
   Local ID              :
   Local Certificate     :  none

   View Proposals >
   Edit Lifetimes >



                    SAVE                          CANCEL
```

As you can see the menu is the same as described in section A, chapter 3.4.3, page 70. The specific difference is just in the way the settings made in the two

menus are applied: Changes in ***CONFIGURE PEERS*** ➧**EDIT** ➧ ***SPECIAL SETTINGS*** ➧ ***PHASE 1*** are applied only to the peer they are configured for while changes in this menu are applied to all peers that do not have a specific configuration.

In Phase 1, the default settings apply to all peers with dynamically assigned IP addresses, even if the DNS name of a host is specified and settings different from the defaults are configured. This is due to the fact that a peer with a dynamic IP address cannot be identified in advance. Therefore, the router cannot pick a specifically configured IKE SA.

3.8 IPSec Menus – *IPSEC (PHASE 2) DEFAULTS*

The same goes for the ***IPSEC*** ➧ ***IPSEC (PHASE 2) DEFAULTS*** menu. The menu is the same as described in section A, chapter 3.4.4, page 79. Again, settings made here are applied to all peers that do not have a specific configuration made in ***CONFIGURE PEERS*** ➧ **EDIT** ➧ ***SPECIAL SETTINGS*** ➧ ***PHASE 2***.

3.9 IPSec Menus – *CERTIFICATE AND KEY MANAGEMENT*

You have encountered the ***IPSEC*** ➧ ***CERTIFICATE AND KEY MANAGEMENT*** menus during the IPSec Wizard process. This menu offers the opportunity to manage keys and certificates in general.

The menu window looks like this:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][CERTMGMT]: IPSec Configuration -
                   Certificate and Key Management              MyRouter

     Certificate and Key Management


        Key Management>

        Own Certificates>
        Certficate Authority Certificates>
        Peer Certificates>

        Certficate Revocation Lists>

        Certificate Servers>

                                EXIT
```

Upon entering any of the menus, you are presented with a list of previously configured keys, certificates, CRLs or certificate servers. These lists display the details of the configurations and allow to enter the **APPEND** and **EDIT** menus.

If you have completed the IPSec Wizard, the different submenus you see are largely known to you.

3.9.1 The Submenu *KEY MANAGEMENT*

The first menu window of ***CERTIFICATE AND KEY MANAGEMENT*** ➧ ***KEY MANAGEMENT*** displays information about the keys stored on your router:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][CERTMGMT][KEYS]: IPSec Configuration -
                         Configure Keys                          MyRouter

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
```

The list informs you about the description of the key(s), the algorithm used and the key length. Moreover you can create new keys or request certificates for existing ones.

Key Generation

if you decide to create a new key, you can do so in the ***CERTIFICATE AND KEY MANAGEMENT*** ➧ ***KEY MANAGEMENT*** ➧ **CREATE** menu:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][CERTMGMT][KEYS][CREATE]: IPSec Configuration -
                                 Create Keys                    MyRouter

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




                    Create                              Exit
```

The menu allows you to configure the following parameters:

Field	Meaning
Description	Here you can enter a random name for the key you are about to create.
Algorithm	Here you choose from either of the available algorithms. *RSA* and *DSA* are available. For further information on the algorithms see section A, chapter 2.1.2, page 19.
Key Size (Bits)	Here you can choose the length of the key to be created. Available values range from 512 to 4096 bit. Note that a key of 512 bit length might be considered unsafe while a key of 4096 bit will not only take considerable time to create, but requires a substantial share of resources during IPSec processing. A value of 768 or more is, however, recommended, the default is set to *1024 bit*.
RSA Public Exponent	(This field is only shown if you have chosen to use the RSA algorithm.) The public exponent is part of the public key created for RSA signatures and RSA encryption. If you do not receive any specific recommendation from your CA, you can leave the default value unchanged

Table A-24: ***IPSEC*** ➧ ***CERTIFICATE AND KEY MANAGEMENT*** ➧ ***KEY MANAGEMENT*** ➧ **CREATE**

Certificate Request

Once you have created a key you can request a certificate for this key by highlighting the respective key and then pressing the "e" key on your keyboard. Alternatively you can choose **Request Cert** and choose the key you want to have certified in the ***CERTIFICATE AND KEY MANAGEMENT*** ➧ ***KEY MANAGEMENT*** ➧ **Request Cert** menu**.**

If you choose to request a certificate, a submenu opens:

```
BinTec Router Setup Tool                      BinTec Communications AG
[IPSEC][CERTMGMT][ENROLL]: IPSec Configuration -
                           Certificate Enrollment              MyRouter

     Key to enroll:              1 (automatic key RSA 1024 (e 65537))

     Subject Name:

     Subject Alternative Names (optional):
       Type   Value

       IP     172.16.98.127
       DNS    mfx4a.
       NONE


     Signing algorithm to use:   md5WithRSAEncryption
     Server:
     Filename:                                                 base64

                    Start                              Exit
```

This menu contains the following fields:

Field	Meaning
Key to enroll	Select the key you intend to have certified.
Subject Name	Enter a subject name for the certificate you request. The name you enter here must follow the syntax for X.509 subject distinguished names outlined in section A, chapter 2.4, page 36.
Subject Alternative Names (optional)	Here you can enter additional information that can be used as a subject name. For a list of options, see table A-26, page 96 below.
Signing Algorithm to use	This field can have the following values: ■ If you request a certificate for a RSA key: – *md5WithRSAEncryption* – *sha1WithRSAEncryption* ■ If you request a certificate for a DSA key: – *dsaWithSHA-1*
Server	Here you specify the TFTP server the certificate request is uploaded to. You can either enter a resolvable hostname or an IP address. Note that you must not enter a scheme (like TFTP or HTTP) before the server address itself.
Filename	Here you specify a filename for the certificate request.
binary/base64	Here you choose in which way you want to have the certificate request encoded. If you want to copy/paste the certificate into a web interface or into an e-mail, choose *base64*.

Table A-25: ***IPSEC*** ➧ ***CERT. AND KEY MNGMNT.*** ➧ ***KEY MNGMNT.*** ➧ **Request Cert**

Below are the options for choosing the **Subject Alternative Names** field. Under the field **Subject Alternative Names – Type**, you can choose from different types of information to be used as subject alternative name. Under the field **Subject Alternative Names – Value**, you can enter the specific information you want to provide.There are three instances available, the default for the first two instances is the first IP address of your router and its DNS name.

The options for **Type** are:

Possible Values	Meaning
IP	Your router's IP address is used as a subject alternative name.
DNS	A DNS name is used as subject alternative name (e.g.: MyRouter).
Email	An e-mail address is used as subject alternative name
URI	An Uniform Resource Identifier is used as subject alternative name. URI is the addressing technology from which URLs are created. Technically, URLs such as HTTP:// and FTP:// are specific subsets of URIs.
DN	An Distinguished Name is used as subject alternative name. It has to comply with the specifications laid out in section A, chapter 2.4, page 36.
RID	An RID (Registered Identity) is used as subject alternative name.

Table A-26: **Subject Alternative Names**

3.9.2 The Certificate Submenus

In the certificate submenus ***Own Certificates***, ***Certificate Authority Certificates*** and ***Peer Certificates***, you can manage the certificates you

need for certificate based authentication methods (i.e. DSA, RSA and RSA encryption).

In general you need to download a peer certificate only in a small number of cases:

- If you have configured RSA Encryption as authentication method, but have neither specified a CRL server nor have a CRL statically stored on your router.
  Note that not specifying a certificate server and not using statically configured CRLs constitutes a significant security hole, since certificates that have been revoked cannot be automatically identified.
- If you do not receive the peer certificate inline during IKE negotiation. This is the case if the peer has disabled sending certificates or no "get certificate requests" are sent by the local machine. 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 looks almost the same:

```
BinTec Router Setup Tool                    BinTec Communications AG
[IPSEC][CERTMGMT][OWN]: IPSec Configuration -
                        Certificate Management                MyRouter

  Description     Flags   SerialNo       Subject Names
  own.cer         0       1013591521 ,   CN=myro


     DOWNLOAD            DELETE              EXIT
```

The menu displays the **Description**, any **Flags** possibly set, the **Serial No** of the certificate in question and quotes from the **Subject Names**.

If you highlight an entry and confirm with **ENTER**, you can access a window which displays the certificate and additional information about it:

```
BinTec Router Setup Tool                      BinTec Communications AG
[IPSEC][CERTMGMT][OWN][EDIT]: IPSec Configuration -
                              Certificate Management          MyRouter

 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
```

While you cannot change the content of the certificate, you can change the following settings:

Field	Meaning
Description	Here the description you have entered when importing the certificate is displayed. You can now change it.
Type of Certificate	Here you can switch between the three types of certificates: ■ *Own Certificate* ■ *Certificate Authority* ■ *Peer Certificate* If you choose *Certificate Authority* here, you must additionally specify if the CA issues CRLs or not.

Table A-27: ***IPSEC*** ➧ ***CERTIFICATE AND KEY MANAGEMENT*** ➧ ***OWN CERTIFICATES*** ➧ **EDIT**

Certificate Import

Another submenu you can access from the initial certificate menu (***CERTIFICATE AND KEY MANAGEMENT*** ➧ ***OWN***, ***CA*** or ***PEER CERTIFICATES***) is the **DOWNLOAD** menu where you can either download a certificate from a TFTP server or import it by directly pasting the content of the certificate into the Setup Tool.

It looks like this:

```
BinTec Router Setup Tool                      BinTec Communications AG
[IPSEC][CERTMGMT][GETCERT]: IPSec Configuration -
                            Get Certificate                   MyRouter

    Import a Certificate/CRL using:  TFTP

      Type of certificate: Own Certificate



     Server:
     Name:                                                  auto

                    START                                  EXIT
```

This menu contains the following fields:

Field	Meaning
Import a Certificate/CRL using:	Specify the way in which you want to enter the certificate data: ■ *TFTP* ■ *Direct Input*
Type of Certificate	This field will display either of the following entries: *Certificate Authority*, *Own Certificate* or *Peer Certificate*. You cannot change this entry.
Please enter certificate data	You can copy/paste the content of the certificate you have received from a CA or from your system administrator into the space provided below this field. The space for entering certificate data will be available only if you have chosen *Direct Input*.
Server	Specify the TFTP server from which the certificate can be downloaded. You may either enter an IP address or a resolvable host name. This prompt is only shown if you have chosen *TFTP*.

Field	Meaning
Name	Specify the name of the certificate that is to be downloaded (if you have used the *TFTP* download) or you have entered (if you have used *Direct Input*). If you have downloaded the certificate via TFTP, this name will be used as filename, also.
auto/base64/binary	Select the type of encoding, so that the router can decode the certificate. *auto* will enable automatic encoding detection. If the certificate download fails in *auto* mode, try specifying an encoding.

Table A-28: ***IPSEC*** ➧ ***CERTIFICATE AND KEY MANAGEMENT*** ➧ ***OWN CERTIFICATES*** ➧ **DOWNLOAD**

Additionally you can activate the **Force trusted** option for peer certificates. If **Force trusted** is active, your BinTec router will not check back with a CA whether the certificate is valid or not.

3.9.3 The Submenu – Certificate Revocation Lists

Upon entering the Certificate revocation List menu you are presented with a list of stored CRLs. The first menu window displays vital information about the CRLs:

- the description you have specified when downloading the CRL
- the issuer of the CRL (usually your CA)
- the Serial Number of the CRL
- the NumC (the number of revoked certificates contained in the CRL).

The menu looks like this:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][CRLS]: IPSec Configuration - CRL Management            MyRouter

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, you can access a menu window that displays the details of the CRL as well as allows you to change the description of the CRL in question. It looks, e.g., like this:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][CERTMGMT][CRLS][EDIT]: IPSec Configuration -
                               CRL Management                MyRouter

     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
```

From the initial ***CERTIFICATE REVOCATION LISTS*** menu window, you can also access the CRL **DOWNLOAD** menu. Here you can import CRL either via TFTP or via direct input. The process functions in the same way as a certificate import. See "Certificate Import", page 99 for details.

3.9.4 The Submenu – Certificate Servers

If you have specified any certificate servers, they are listed in the first menu window of the ***CERTIFICATE*** Servers menu.

The following information is displayed:

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

If you either highlight an entry and confirm with **ENTER** or if you choose **ADD**, you can access the **ADD/EDIT** menu. Here you can either specify a new certificate server or change the settings of already existing ones. Apart from specifying a **Description** and the **URL** of the server, you can assign a **Preference** to the server. The router will check certificate servers in the order of the preference assigned to them, beginning with *0*.

3.10 IPSec Menus – *ADVANCED SETTINGS*

In the menu ***IPSEC*** ➧ ***ADVANCED SETTINGS*** you can adjust certain functions and features to specific needs of your environment, i.e. for the most part they set interoperability flags. The default values will enable your system to run properly against other BinTec routers, so you only need to change them if you know you will need specific settings. This may be necessary if the remote side uses older IPSec implementations.

The ***ADVANCED SETTINGS*** menu looks like this:

```
BinTec Router Setup Tool                          BinTec Communications AG
[IPSEC][ADVANCED]: IPSec Configuration - Advanced Settings    MyRouter


   Ignore Cert Request Payloads       :  no
   Do not send Cert Request Payloads  :  no
   Do not Send Full Certificate Chains:  no
   Do not send CRLs                   :  yes

   Do not send Key Hash Payloads      :  no
   Trust ICMP Messages                :  no
   Do Not Send Initial Contact        :  no
   Sync SAs With Local Interface      :  no
   Max. Symmetric Key Length          :  1024
   Use Zero Cookies                   :  no
   Cookies Size                       :  32


   Peer List Management>


                          SAVE                              CANCEL

Use <Space> to select
```

The fields and their relevance are as follows:

Field	Meaning
Ignore Cert Request Payloads	Specifies whether or not certificate requests received from the remote side during IKE should be ignored. Possible values are *yes* or *no*.
Do not send Cert Request Payloads	Specifies whether or not certificate requests should be sent during IKE. Possible values are *yes* or *no*.
Do not Send Full Certificate Chains	Specifies whether or not full certificate chains should be sent during IKE. Possible values are *yes* or *no*. Choose *yes* here if you do not want to send all certificates from your own one to that of the CA requested.

Field	Meaning
Do not send CRLs	Specifies whether or not CRLs should be sent during IKE. Possible values are *yes* or *no*.
Do not send Key Hash Payloads	Specifies whether or not key hash payloads are sent during IKE. By default the hash of the remote side's public key is sent along with the other authentication data. Applies to RSA encryption only; choose *yes* to suppress this. Possible values are *yes* or *no*.
Trust ICMP Messages	Specifies whether IKE should trust ICMP port and host-unreachable error messages. ICMP port and host-unreachable messages are only trusted if no datagrams from the remote host have been received in this negotiation. This means, if the local side receives an ICMP port or host-unreachable message as the first response to the initial packet of a new phase-1 negotiation, it cancels the negotiation immediately. Possible values are *yes* or *no*.
Do Not Send Initial Contact	Specifies whether or not to send IKE initial contact messages in IKE negotiations even if no SA's exist with a peer. Possible values are *yes* or *no*.
Sync SA With Local Interface	Ensures that all SAs are deleted that had their traffic routed over an interface that has changed from an *up* state to either *down*, *dormant* or *blocked*.
Max. Symmetric Key Length	Specifies the maximum length of an encryption key (in bits) that is accepted from the remote end. This limit prevents denial-of-service attacks where the attacker asks for a huge key for an encryption algorithm that allows variable length keys.

Field	Meaning
Use Zero Cookies	Specifies whether or not *zeroed* ISAKMP cookies should be sent. They are equivalent to the SPI in IKE proposals; since they are redundant they are usually set to the value of the negotiation in progress. Alternatively, the router can use all zeroes for the values of the cookie. Choose *yes* for this option. Possible values are *yes* or *no*.
Cookie Size	Specifies the length of the zeroed SPI (Security Parameter Index) in bytes, which is used in IKE proposals. This field takes effect only if **Use Zero ISAKMP Cookies** is set to *yes*.

Table A-29: ***IPSec*** ➧ ***Advanced Settings***

Below the fields described above, you find the ***Peer List Management*** menu:

```
BinTec Router Setup Tool                    BinTec Communications AG
[IPSEC][PEERS]: IPSec Configuration - Configure Peer List     MyRouter

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

Description     PeerID          PeerAddr        IKEProp   TrafficList
peer_1          198.16.13.1     198.16.13.1     default            1
peer_2          198.16.13.2     198.16.13.2     default            0
-------------------------------------------------------------------------
peer_3          198.16.13.3     198.16.13.3     default            0
-------------------------------------------------------------------------
peer_4          198.16.13.4     198.16.13.4     default            0
peer_5          198.16.13.5     198.16.13.5     default            0


 APPEND              DELETE              EXIT

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

This menu will display all peer lists you have created with their respective details. Each group of peers separated by a dotted line from another group is a peer list. Moreover, this menu allows for advanced peer list management: You can create separate peer lists and switch between them for testing purposes.

The help section of the menu window tells you how to select a list as active peer list. You can choose any peer within a list to be the first active peer. All peers above this peer will be ignored. You can insert peers into any list as is described in the help section of the menu window. In that case and by choosing **APPEND**, you enter the same menu as is described in section A, chapter 3.4.1, page 64. By using **APPEND**, however, you only append a new entry to the bottom peer list.

3.11 IPSec Menus – *WIZARD*

If you enter this menu, you can access the IPSec Wizard you have already encountered when first entering the ***IPSEC*** menu. The functions available are the same as describes in section A, chapter 3.1, page 48.

3.12 IPSec Menus – *MONITORING*

The last menu of the IPSec context is ***IPSEC*** ➧ ***MONITORING***. Here you can view the status of the global statistics, IKE Security Associations and IPSec Security Associations. Accordingly, it contains three submenus which are described in the following chapters.

3.12.1 The Submenu *GLOBAL STATISTICS*

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

It looks like this (the values shown are examples, only):

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][MONITORING][STATS]: IPSec Monitoring -
                            Global Statistics                   MyRouter

      Global IPSec Statistics

         IKE SA's:            0              IPSec SA's:          0

        Packet Statistics:
         IP:                  151            Non-IP:              0
         AH:                  0              ESP:                 0
         Dropped:             0              Plain:               151
         Triggers:            0              Cur. Frag. Bytes:    0
         Cur. Frag. Pkt:      0              Cur. Frag. Nonfirst: 0
         Decrypt Errors:      0              Auth. Errors:        0
         Replay Errors:       0              Policy Errors:       0
         Other Errors:        0              SendErrors:          0
         Unknown SPI:         0


                                    EXIT
```

The fields and the meaning of the values displayed are as follows:

Field	Meaning
IKE SA's	Displays the current number of IKE SAs.
IPSec SA's	Displays the number of current IPSec SAs.
IP	Displays the number of "processed" IP packets.
Non-IP	Displays the number of processed non-IP packets.
AH	Displays the number of packets processed using the AH protocol.
ESP	Displays the number of packets processed using the ESP protocol.
Dropped	Displays the number of dropped packets.
Plain	Displays the number of packets that have been transmitted unchanged by IPSec.

Field	Meaning
Triggers	Displays the number of packets that have triggered an IKE negotiation.
Cur. Frag. Bytes	Displays the total size (in bytes) of the packet fragments that are currently reassembled.
Cur. Frag. Pkt.	Displays the number of packet fragments that are currently reassembled.
Cur. Frag. Nonfirst.	Displays the number of packet fragments that are queued for reassembly with the first packet fragment still missing.
Decrypt Errors	Displays the number of decryption errors.
Auth. Errors	Displays the number of authentication errors.
Replay Errors	Displays the number of replay errors.
Policy Errors	Displays the number of policy errors.
Other Errors	Displays the number of other receive errors.
Send Errors	Displays the number of send errors.
Unknown SPI	Displays the number of unknown SPI errors.

Table A-30: ***IPSEC*** ➧ ***MONITORING*** ➧ ***GLOBAL STATISTICS***

3.12.2 The Submenu *IKE SECURITY ASSOCIATIONS*

The next monitoring submenu (***IPSEC*** ➧ ***MONITORING*** ➧ ***IKE SECURITY ASSOCIATIONS***) displays statistics about the IKE SAs. It looks like this (values are examples, only):

```
BinTec Router Setup Tool                      BinTec Communications AG
[IPSEC][MONITORING][IKE SAS]: IPSec Monitoring -
                              IKE SAs                          MyRouter

T: xch.-Type: B=Base I=Id-protect 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=Negotiating E=Establ. D=Delete W=Waiting-for-remove
E: Enc.-Alg : d=DES D=3ES B=Blowfish C=Cast R=Rifjndael 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
C=DE, O=TC TrustCenter AG, OU=TC    10.1.1.2   C=DE, O=TC Trus  ISREBM


   DELETE              EXIT
```

The meaning of the characters in the **TARSEH** column (it is the last column to the right below the help section of the menu window) is explained in the upper part of the menu window, so that the example shown above translates as follows:

Field	Meaning
Remote ID	Displays the ID of the remote peer. In the example authentication is done by certificates; thus the remote ID consists in quotes from the peer's certificate.
Remote IP	Displays the remote peers IP address.
Local ID	Displays the local ID. Again, the ID consists of quotes from the certificate used for authentication.

Field	Meaning
TARSEH	Displays the combination of the parameters explained in the help section of the menu window. *ISREBM,* as found in the example, thus means: ■ Exchange Type: id_protect (*I*) ■ Auth.-Meth.: RSA-signature(*S*) ■ Role: Responder (*R*) ■ State: Established (*E*) ■ Enc.-Alg.: Blowfish (*B*) ■ Hash-Alg.: MD5 (*M*)

Table A-31: ***IPSEC ➧ MONITORING ➧ IKE SECURITY ASSOCIATIONS***

3.12.3 The Submenu *IPSEC SECURITY ASSOCIATIONS*

The next submenu (***IPSEC ➧ MONITORING ➧ IPSEC SECURITY ASSOCIATIONS***) displays the IPSec Security associations negotiated in IKE Phase 2. The menu looks like this:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][MONITORING][IPSEC SAS]: IPSec Monitoring -
                                IPSec SAs                       MyRouter

S: Sec. Proto : E=ESP A=AH C=IPComP
E: Enc. Alg.  : D=DES3 B=Blowfish C=Cast d=DES R=Rijndael T=Twofsh
A: Auth. Alg. : M=MD5 S=SHA1
C: Comp-Alg.  : D=Deflate
Direction     : >=outbound  <=inbound
Address-Syntax:  <host> or <first>+<num-following> or
                                    <netaddr>/<masklen>
type 'h' to toggle this help

Local        LPort    Pto     Remote          RPort   SEAC   Pkts  Bytes
172.16.96.3   0        0      <192.168.157.1   0     EBMD    0      0
172.16.96.3   0        0      >192.168.157.1   0     EBMD    2    208

   DELETE              EXIT
```

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

Field	Meaning
Local	Displays the local IP address, address range or network protected by this SA.
LPort	Displays the local port number or range of port numbers protected by this SA.
Pto	Displays the layer 4 protocol of the traffic protected by this SA (*0* = any).
Remote	Displays the remote IP address, address range or network protected by this SA.
RPort	Displays the remote port number or range of port numbers protected by this SA.
SEAC	Displays the combination of IPSec protocol, encryption algorithm and hash algorithm used by the SA as is described in the help section of the menu window.
Bytes	Displays the number of bytes processed for this SA.
Pkts	Displays the number of packets processed for this SA.

Table A-32: ***IPSec*** ➧ ***Monitoring*** ➧ ***IPSec Security Associations***

4 Configuring DynIPSec

The use of dynamic IP addresses has the drawback that an IPSec peer can no longer be identified and located within the internet as soon as his or her IP address has changed. DynDNS obviates this problem and ensures that your router is reachable under a unique hostname, even if its IP address has changed. To use the DynDNS service for establishing IPSec tunnels, all you have to do is direct traffic intended for the "dynamic peer" to the unique hostname registered with any one of the supported DynDNS providers. As soon as your router tries to connect to the machine "behind" that hostname, it is first directed to the DynDNS provider from where it obtains the (dynamic) IP address the "dynamic peer" has been assigned.

Configuration of DynIPSec, thus, consists of two steps:

- Configuring the DynDNS service on all routers that have their IP addresses assigned dynamically and that need to be reachable from within the internet (section A, chapter 4.1, page 113).
- Configure peers so that the **Peer Address** points at the unique hostname registered with a supported DynDNS provider (section A, chapter 4.2, page 118).

4.1 Configuring DynDNS

In order for your or your router to be able to publicize its IP address, you first need to register a unique hostname with a DynDNS provider. Most providers offer a choice of different domain names which, together with a username, form the unique hostname you need, e.g. ***dyn-peer.dyndns.org***. Once you have registered a hostname, you can configure the DynDNS service on you router.

4.1.1 Adding a DynDNS Service

Configuration is done in the ***IP*** ➧***DYNDNS*** menu. The first menu window to open displays a list of previously configured DynDNS services. For a generic example configuration, it will look like this:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IP][DYNDNS]: Dynamic DNS Service                                MyRouter

  DynDNS Services:

  Host Name              Interface        Permission      State
  dyn-peer.dyndns.org    isp              enabled         up_to_date


 DynDNS Provider List >

     ADD                 DELETE             EXIT
```

From here you can access the submenus **ADD/EDIT** where you can configure new DynDNS services or edit exiting ones, and the ***EDIT DYNDNS PROVIDER*** menu where you can add new entries to the list of providers and edit such entries you have created yourself (you cannot edit or delete the preset providers).

For the configuration of a new service, the **ADD/EDIT** menu looks like this:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IP][DYNDNS][ADD]: Dynamic DNS Service                           MyRouter


          Host Name
          Interface
          User
          Password

          Provider
          MX
          Wildcard                  off
          Permission                enabled


                    SAVE                                CANCEL
```

Here you configure DynDNS services. The fields in the menu window have the following relevance:

Field	Meaning
Host	Here you enter the complete hostname you have registered, e.g. ***dyn-peer.dyndns.org***.
Interface	Here you choose the WAN interface the IP address of which is to be publicized (in general this will be the interface of your ISP).
User	Here you enter the username under which you have registered with your DynDNS provider.
Password	Here you enter the password to use in order to authenticate you to the DynDNS provider.
Provider	Here you choose from the set of preconfigured DynDNS providers. They are: ■ *dyndns* (www.dyndns.org) ■ *stat dyndns* (http://www.dyndns.org) ■ *ods* (http://www.ods.org) ■ *hn* (http://hn.org) ■ *dyns* (http://dyns.cx) ■ *orgdns* (http://www.orgdns.de) Further providers will be added. Even if you have not yet added any new DynDNS providers, you can choose among five different providers. You can add and edit further providers in the ***IP*** ➧ ***DynDNS*** ➧ **ADD/EDIT** ➧ ***Edit DynDNS Provider***.
MX	If you determine that the router "behind" a certain hostname should not receive any e-mail, you can specify a different hostname here and thus redirect any mail traffic. Ask your DynDNS provider about this service.

Field	Meaning
Wildcard	Here you can activate additional name resolution within your local network. You must run a DNS server to use this option. Possible values for this field are *on* and *off*, the default value is *off*.
Permission	Here you can activate or deactivate the service you have just configured. The possible values for this field are *enabled* and *disabled*, the default value is *enabled*.

Table A-33: ***IP*** ➧ ***DynDNS*** ➧ **ADD/EDIT**

4.1.2 Adding a DynDNS Provider

If you want to add a DynDNS provider, you can do so in the ***IP*** ➧ ***DynDNS*** ➧ **ADD/Edit** ➧ ***Edit DynDNS Provider*** menu:

```
BinTec Router Setup Tool                    BinTec Communications AG
[IP][DYNDNS][DYNDNS PROVIDER]: Edit DynDNS Provider          MyRouter

 DynDNS Service Provider:


 Name                  Protocol              Server

 dyndns                dyndns                 members.dyndns.org
 stat dyndns           static dyndns          members.dyndns.org
 ods                   ods                    update.ods.org
 hn                    hn                     dup.hn.org
 dyns                  dyns                   www.dyns.cx


    ADD                DELETE              EXIT
```

Again, the first menu window displays a list of all DynDNS providers that have already been configured, i.e. when you enter the menu for the first time you will see the five preset providers.

If you decide to add one you can access the **ADD** menu from here. If you enter it in order to add a provider, it will look like this:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IP][DYNDNS][DYNDNS PROVIDER][ADD]: Edit DynDNS Provider      MyRouter

          Name
          Server
          Path
          Port                          80

          Protocol                      dyndns

          Minimum Wait (sec)            300


                     SAVE                                  CANCEL
```

The menu contains the following fields:

Field	Meaning
Name	Here you can enter a convenient name for the provider you are about to configure.
Server	Here you enter the address of the DynDNS provider's server.
Path	Her you enter the path on which the script for publicizing your IP address can be found.
Port	Here you enter the port which your router uses to address the provider's server. Ask your provider for the port to use.
Protocol	Here you choose from on of the supported DynDNS protocols (see section A, chapter 2.5, page 44 for a list).
Minimum Wait (sec)	Here you enter the minimum time your router will wait until he publicizes its IP address again.

Table A-34: ***IP*** ➧ ***DynDNS*** ➧ ***Edit DynDNS provider*** ➧ **ADD**

Note that you should configure a comparatively long shorthold for the interface used to update the IP address on the DynDNS provider's server. Updating the IP address may take a moment, and if the shorthold is effective before the IP address has been successfully updated, the DynDNS service will not be functional.

4.2 Adjusting IPSec Peer Configuration

Once you have configured the DynDNS service on the router that has a dynamically assigned IP address, you need to adjust the peer configuration of all peers that need to initiate IPSec connections with the "dynamic router".

If you have not yet created the "dynamic peer (***dyn-peer.dyndns.org***)", see section A, chapter 3.4, page 62 for information on how to do so. In the ***IPSec*** ➧ ***Configure Peers*** ➧ **APPEND** menu, enter the hostname of the "dynamic peer" instead of an IP address.

The menu window then looks like this (note the value for the **Peer Address** field):

```
BinTec Router Setup Tool                        BinTec Communications AG
IPSEC][PEERS][ADD]: IPSec Configuration - Configure Peer List MyRouter

     Description:   dyn-peer
     Peer Address:  dyn-peer.dyndns.org
     Peer IDs:




                       SAVE                CANCEL
```

If you intend to change an existing peer's settings so as to allow the use of DynIPSec, you can change the settings for this peer in the ***IPSEC*** ➧ ***PEER CONFIGURATION*** ➧ **EDIT** menu to look like this:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][PEERS][EDIT]: IPSec Configuration -
                      Configure Peer List                       MyRouter


     Description: dyn-peer
     Peer Address:dyn-peer.dyndns.org
     Peer IDs:

     Special Settings >

Traffic List: 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
*10.1.1.0       M24  -     all     10.1.2.0         M24  -    PR default

   APPEND              DELETE               SAVE                CANCEL
```

As soon as traffic is directed toward the "dynamic peer", the hostname is resolved and the traffic is directed to the IP address propagated by the "dynamic peer". You can now initiate tunnel creation with this ("dynamic") peer.

Make sure to have at least one name server configured. Otherwise you will not be able to resolve the hostname of the "dynamic peer" to obtain the current dynamic IP address.

In case you have changed the IPSec default rule from *let pass* to *drop it*, make sure that DNS traffic directed at the configured nameserver is allowed, e.g. by adding a Pre IPSec Rule that allows all traffic to and from the name server over UDP port 53.

5 BinTec Certificate and Key Management Tools

In addition to the certificate and key management options of the Setup Tool, there are two tools available in the SNMP shell: `cert` for certificate management and `key` for key management.

For information about certificate and key management with the Setup Tool, please see the following chapters: section A, chapter 3.9, page 90.

5.1 The `cert` Application

If you enter `cert` in the SMNP shell command prompt, you will see the following text:

```
MyRouter:> cert
cert: Too few arguments
cert: Certificate Management Tool.
usage:
syntax: cert -h? | (<command> <args>... )

            -?, -h: displays this help message
         <command>: The command to execute.
                    Possible commands are:
                    put: export a certificate, crl or pkcs#10 request
                    get: import a certificate or crl
                    destroy: destroy a certficate or crl
                    view: view the contents of a certificate/crl
         <args>...  command specific argument list
MyRouter:>
```

Table A-35: BinTec's `cert` tool

Help is available for the single commands, too, when you type `cert <command> -?`.

Through the `cert` tool, you can perform the same basic certificate management tasks as in the ***KEY AND CERTIFICATE MANAGEMENT*** menu of the Setup

Tool. Additionally you can use cert put to export the certificate or an certificate request.

cert put

This command will export a certificate or CRL to a specified location:

```
cert put [-b] [crl] <dest> <cert>].
```

This command will generate a ➤➤ **PKCS#10** request for a specified key:

```
cert put pkcs10 [-s <subj_name>] [-a <subj_altname>] [-n
<request_id>] [-c <algorithm>] <dest> <key> [<filename>].
```

The options and arguments in the syntax have the following relevance:

- -b: is used to create a binary file instead of a base64 encoded one.
- crl: is used to export a CRL from the **certRevListTable** rather than a certificate.
- <dest>: can be either console, in which case the result is printed out on the console and the -b flag and <filename> are ignored, or the IP-address or hostname of an external TFTP server.
- <cert>: specifies the name of the certificate/CRL to export.
- -s <subj name>: specifies the X500 directory name of subject, the default is none.
- -a <subj_altname>: specifies a subject alternative name, multiple alternative names possible.
  The syntax is as follows:
  -a NONE (no subject alternative name is specified), or
  -a <type>=<data>, where <type> can be IP, DNS, EMAIL, URI, DN or RID and <data>: type specific data. The defaults are: 1. system unique IP 2. all other IP addresses currently in **ipAddrTable** 3. hostname as DNS.
- -n <request_id>: specifies the request ID of this certificate request, the default is 0.
- -c <algorithm>: specifies the algorithm to use, possible algorithms are:
  RSA (md5WithRSAEncryption or sha1WithRSAEncryption)
  DSA: (dsaWithSHA-1).
  The default for RSA is md5WithRSAEncryption.

- `<key>`: specifies the key to use for the certificate request, you may specify a key index or a key name.
- `<filename>`: specifies the name of target file, the default is `<keyname>.pkcs10` where `<keyname>` is taken from `<key>`.

5.2 The key Application

To manage keys from the SNMP shell without the use of the Setup Tool, there is the key tool. Its basic help screen looks like this:

```
MyRouter:> key -?
key: Key Management Tool.
usage:
syntax: key -h | ( create [-a <algorithm>] [-s <bits>] [-e <public_e>]
                           [<description>] )
                | ( destroy ( <index> | <description> ) )
                | ( export [-c] | import <dst/src> ( <index> | <descrip
                   tion> ) [<password>] )

             create: create a new key for algorithm <algorithm>
                     with size <bits>
     -a <algorithm>: rsa | dsa, default rsa
                     rsa: RSA algorithm
                     dsa: DSA algorithm (Digital Signature Algorithm)
         -s <bits>: key size in bits, default 768
      -e <public_e>: use the fixed public exponent <public_e> for RSA
      <description>: the description for the new key
                     (default "keys/<new_index>"
            destroy: destroy the key with index <index> or description
                     <description>
                     or the name of the key to destroy (destroy)
            <index>: the index of the key to destroy
      <description>: the description of the key to destroy.
           <export>:
           <import>: export/import the key with index <index> or des
                     cription
                     <description> as encrypted pkcs#8 data
                -c: use compatibility mode: 56 bit key length only!
       <dst/src>: destination (export) / source (import) of the key,
                  syntax:
                   <scheme>[://<server_name>[:<port>][/<file_name>]]
                   <scheme>:      console | tftp
                   <server_name>: name of tftp or http server
                   <port>:        port used for tftp (default: 69)
                                   or http (default80)
                   <file_name>:   name of the file for tftp or http
                                   (default <key_description>.pk8)
            <index>: the index of the key to export
      <description>: the description of the key to export / import.
       <passphrase>: optional passphrase to use. If this field is omit
                     ted, the admin password is used
```

Table A-36: BinTec's key tool

The only function that is not available through the Setup Tool is the export/import function. It is executed through the command `export/import`.

key export/import

`key export [-c] <dst> <index> [<password>] or`

`key export [-c] <dst> <description> [<password>]`

- `export`: either exports the key with with either index `<index>` or description `<description>` as encrypted PKCS#8 data.
- `-c`: uses compatibility mode, 56 bit key length only (PBES1).
- `<dst>`: specifies the destination of the key.
  The syntax is as follows:
  <scheme>[://<server_name>[:<port>][/<file_name>]];
  `<scheme>` can either be `console` or `tftp`,
  `<server_name>` is the name of the tftp or HTTP server the key shall be exported to,
  `<port>`: is the port used for tftp (default: 69) or HTTP (default = 80),
  `<file_name>`: is the name of the file for TFTP or HTTP (default `<key_description>.pk8`).
- `<index>`: specifies the index of the key to export if no description is specified.
- `<description>`: specifies the description of the key to export if no index is specified.
- `<passphrase>`: specifies an optional passphrase to use. If this field is omitted, the admin password is used.

If you want to import a key, the syntax is the same, only you use `key import` and do not specify the destination the key should be set to, but the source you want to download it from:

`key import <src> <index> [<password>]or`

`key import <src> <description> [<password>]`

Note that the `-c` option is not available for import; the compatibility mode is detected automatically, and the flag need not bet set.

6 Key Terms

AH Authentication Header

One of the two principal IPSec protocols, used for authentication only, Data encryption is not supported.

3DES (Triple DES) See ➤➤ **DES**.

Block Cipher Modes Block ciphers take a fixed-size block of data (usually 64 bits), and transform it to another block of the same size using a function selected by the key.

Blowfish An algorithm developed by Bruce Schneier. It is a block cipher with a 64-bit block size and variable length keys (up to 448 bits).

CAST A 128-bit encryption algorithm whose operation is similar to DES. See ➤➤ **Block Cipher Modes**.

CBC Cipher Block Chaining

A plaintext block is combined with the encryption result of the previous block and the resulting value is encrypted. This procedure requires an Initialization Vector (IV) for the first block. See ➤➤ **Block Cipher Modes**.

Certificate A certificate identifies someone or something, an individual, a company, or an application. The certificate associates that identity with a public key. Public-key certificates are data blocks which provide a safe method of distributing public keys. Public-key certificates are certified by an issuing organization called a certification authority (CA).

CA Certificate Authority

See ➤➤ **Certificate**.

Denial-Of-Service Attack A Denial-of-Service (DoS) attack is an attempt to flood a router or a host in a LAN with forged requests so that it is completely overloaded. This means, the system or a certain service can no longer be used.

DES Data Encryption Standard

A ➤➤ **block cipher** with 64-bit block size. It uses 56-bit keys. A safer variant of DES, Triple-DES or 3DES is based on using DES three times (i.e. encrypt-decrypt-encrypt sequence with either two or three different, unrelated keys).

DOI Domain Of Interpretation

The DOI for IPSec specifies all the parameters associated with the ISAK-MP/Oakley protocols, and assigns them unique identifiers.

DSA (DSS) Digital Signature Algorithm (Digital Signature Standard). A signature-only mechanism supported by the United States government. Its design criteria have not been made public. Regarding key generation, DSA is faster than RSA. On the other hand, regarding key computation, DSA is slower than RSA.

ECB Electronic Code Book mode

If the same block is encrypted twice with the same key, the resulting ciphertext blocks are the same. See ➤➤ **Block Cipher Modes**.

ESP Encapsulating Security Payload

One of the two principal IPSec protocols, supporting data encryption as well as authentication.

hashing The process of deriving a number, called a hash, from a string of text. A hash is usually much smaller than the text stream from which it originated. The hashing algorithm is designed to generate the hash with a very low probability that hashing a different meaningful text string might generate an identical hash value.

Encryption devices use hashing to ensure that intruders have not modified transmitted messages.

HMAC Hashed Message Authentication Code

A message authentication mechanism that uses cryptographic hashing functions such as MD5 and SHA-1, in combination with a shared secret key. HMAC allows easy replacement of the underlying hashing function, as when security requirements change or when faster or more secure hashing functions become available.

HMAC-MD5 Hashed Message Authentication Code - using Message Digest version 5 algorithm.

HMAC-SHA1 Hashed Message Authentication Code - using Secure Hash Algorithm version 1

ICV Integrity Check Value

Usually an HMAC algorithm using Message Digest 5 (MD5) or SHA-1 hash functions checks if data has been modified.

IETF Internet Engineering Task Force

IPComP IP payload compression

IPComP is a protocol to reduce the size of IP datagrams. This protocol will increase the overall communication performance between a pair of communicating hosts/gateways ("nodes") by compressing the datagrams, provided the nodes have sufficient computation power, through either CPU capacity or a compression coprocessor, and the communication is over slow or congested links.

Key Escrow Escrowed keys can be accessed by the government. Particularly the US government establishes key escrows to handle the problem that criminals could hide their criminal acts by encrypting their data.

LDAP Lightweight Directory Access Protocol

LDAP is a lightweight version of the X.500 client access Directory Access Protocol (DAP), which specifies how a client accesses a directory server. LDAP was defined by the IETF in order to encourage adoption of X.500 directories. LDAP defines a relatively simple protocol for updating and searching directories running over TCP/IP (default port is 389).

Man-in-the-Middle Attack Public key encryption presupposes the exchange of the public encryption keys. During this exchange, the unprotected keys could be easily intercepted and open the possibility of the "man-in-the-middle" attack. The attacker could plant his or her own key early in the process so actually a key known to the "man-in-the-middle" would be used instead of the party's key you believed to communicate with.

MD5 See ➤➤ **HMAC-MD5**.

PGP Pretty Good Privacy

A cryptographic authentication scheme typically used by internet e-mail users to authenticate the identity of the sending party, and the integrity of their message.

PKCS Public-Key Cryptography Standards

The PKCS are a set of standards for public-key cryptography. The PKCS are designed for binary and ASCII data and are also compatible with the ITU-T X.509 standard. The published standards are PKCS #1, #3, #5, #7, #8, #9, #10, #11, #12, and #15. PKCS #10 describes syntax for certification requests.

Rijndael (AES) Rijndael (AES) has been chosen as AES for its quick key setup, low memory requirements and for its high security against attacks. For more information about the AES, see http://csrc.nist.gov/encryption/aes.

RipeMD 160 RipeMD 160 is a 160-bit cryptographic hash function. It is intended to be used as a more secure replacement for MD5 and RipeMD.

RSA The RSA (named after its inventors Rivest, Shamir, Adleman) algorithm is based on the fact that there is no efficient way to factor very large numbers. Deducing an RSA key, therefore, requires an extraordinary amount of computer processing power and time.

RSA Signature provides non-repudiation for authentication, RSA Encryption provides for confidentiality

SAD The Security Association Database contains information about each SA (while an SA is a sort of instance for an SPD entry), such as AH or ESP algorithms and keys, sequence numbers, protocol mode and SA lifetime. For outbound processing, an SPD entry points to an entry in the SAD. That is, the SPD determines which SA is to be used for a given packet. For inbound processing, the SAD is consulted to determine how the packet must be processed.

SHA1 See ➤➤ **HMAC-SHA**.

SPD The Security Policy Database specifies the security services offered to the IP traffic. These security services depend on parameters such as source, destination of the packet, etc.

SSL Secure Sockets Layer

A technology developed by Netscape, and now standardized, usually used to secure HTTP traffic between a web browser and a web server.

Tiger 192 Tiger 192 is a fairly new and very fast hash algorithm.

TLS Transport Layer Security

The TLS protocol provides communications privacy over the internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. It is based on SSL 3.0 and is intended as successor of that protocol. Refer to http://www.ietf.org/rfc/rfc2246.txt.

Twofish Twofish was one of the final candidates for AES (Advanced Encryption Standard). It can be considered equally secure as Rijndael (AES), but is slower.

X.500 The set of ITU-T standards covering electronic directory services, compare: ➤➤ **LDAP**. For example, white pages is a directory service for locating individuals by name (by analogy with the telephone directory). The internet supports several databases that contain basic information about users, such as electronic mail addresses, telephone numbers and postal addresses. These databases can be searched to get information about particular individuals.

X.509 The set of ITU-T standards defining the format of certificates and certificate requests as well as their use.

A Key Terms

WORKSHOP

1 How to Configure an IPSec LAN-to-LAN Connection

The LAN-to-LAN connection is the most common application of IPSec with routers. A Host-to-Host connection is usually realized using an IPSec client running directly on the connecting hosts (PCs). A Host-to-LAN connection (e.g. field staff dialing in to the company head office) usually combines router configuration as described here (on the head office side) and client configuration (on the field staff side). The configuration of an IPSec client is not described in this document.

1.1 Introduction

Two distant networks, a corporate central site, ***Head Office***, and a partner's network, ***Branch Office,*** can be connected over the Internet via a secure tunnel using BinTec's IPSec.

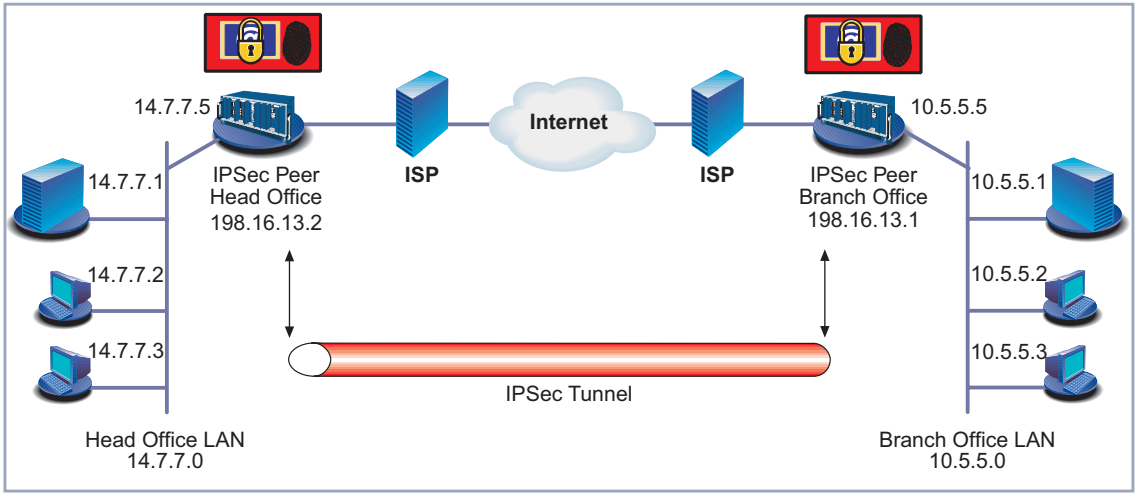


Figure B-1: IPSec LAN-to-LAN connection

Once both routers (peers) have been configured to use IPSec, hosts in either LAN can securely exchange data with the hosts of the other LAN. All traffic (or

such traffic as has been specified) is routed through an IPSec tunnel and hence secured. Traffic inside either of the LANs (from host to host or from host to router within one of the LANs), however, is still unprotected and in plain text.

The configuration described later must be performed on each side of the WAN. Make sure that settings specific to one peer (like IDs and certificates) are made specifically for each peer, i.e. that what is the local ID of one router needs be configured as peer ID on the other and so on.

The following chapters comprise descriptions of the following:

- configuration prerequisites (section B, chapter 1.2, page 133)
- IPSec Wizard configuration (section B, chapter 1.3, page 135)
- reviewing and adjusting the IPSec Wizard configuration (section B, chapter 1.4, page 150)
- DynIPSec configuration (section B, chapter 1.5, page 161).

1.2 Prerequisites

IPSec software and license

For the use of IPSec you will need a license and an IPSec enabled version of the system software (you will receive the latter upon purchasing the license, or you can download it from www.bintec.net). For information on how to enter a license and install a new software image, see the **User's Guide** of your router. The most recent information on licensing mechanisms and software update can be found on our webserver, too.

IPSec supporting devices

Make sure that you either have a BinTec Router at each side of the intended tunnel, or make sure that any third party device used complies with the IPSec standards.

Static and dynamic IP addresses

As long as you do not supplement your IPSec configuration with an DynDNS service and adjust your configuration accordingly (see section B, chapter 1.5, page 161), at least one VPN partner must have a statically configured, official IP address.

- Both sides have a statically configured IP address.
  Assuming both sides have static IP addresses, the VPN connection can be established by both sites.
- If one peer gets its IP address dynamically assigned by its ISP, the IPSec connection can only be established by that peer, not by the peer with the statically configured, official IP address.

User's Guide and Software Reference

For the basic and advanced configuration of your BinTec Router (Internet connection or WAN partner configuration), consult the **User's Guide** of your router or the **Software Reference**. In this document the IPSec relevant configuration is described only.

Prerequisite Configuration Steps

Before you start with the IPSec configuration proper, there are two prerequisite configuration settings required for the connection.

Routing settings:

In your routing settings a default route to the Internet Service Provider (including the remote peer network to connect to) is required. Verify the settings in the Setup Tool menu ***IP*** ➧ ***ROUTING*** ➧ **ADD/EDIT**. For detailed information on how to configure a default route, consult your **User's Guide**.

NAT settings:

If you have activated Network Address Translation (NAT) on any interface (e.g. to enable Internet access), you have to adjust the NAT settings (for detailed information on how to configure NAT, consult your **User's Guide** and the **Software Reference**).

If you choose to use the IPSec Wizard, it will adjust your NAT settings automatically if this is necessary. If you need to or want to do this manually, create NAT entries as follows:

NAT settings for sessions requested from outside

- To enable a phase-1 exchange you need to allow IKE traffic from the outside (UDP port 500). Create an entry with these settings:
  - **Service**: *user defined*
  - **Protocol**: *udp*
  - **External Port**: *500*
  - **Internal Port**: *500*

- Since the IP headers of IPSec packets are modified and need to be processed by IPSec to discover the recipient's IP address, an entry for each of the IPSec protocols (AH and ESP) is mandatory:
  - **Service**: *user defined*
  - **Potocol**: *ah* or *esp* respectively

You need not make or change any other entries in any of the other fields of the menu.

NAT settings for sessions requested from inside

Here you need to specify only one static port mapping (the IPSec protocols are not bound to specific ports). Create an entry with these settings:

- **Service**: *user defined*
- **Protocol**: *udp*
- **External Port**: *500*
- **Internal Port**: *500*

Again, you need not make or change any other settings.

1.3 Configuration – IPSec Wizard

Once you have completed all preliminary configuration steps, you can make use of the IPSec Wizard for a quick and easy way of setting up IPSec. The IPSec Wizard allows for a basic configuration which is sufficient for our scenario, since only one peer has to be configured and a single peer traffic list entry is enough to protect all TCP traffic between the peers. After completing the IPSec Wizard you will have a functional IPSec configuration and you will be able to protect the most common kind of traffic between the peers. You can then adjust the settings made according to your specific needs.

Starting the Wizard

If you have not made any IPSec settings so far, the IPSec Wizard will be automatically triggered when you first enter the ***IPSEC*** menu. If there already is an IPSec configuration on your router, two events can possibly take place: Either the configuration is complete in that it contains all settings the Wizard can make. In this case you are taken to the ***IPSEC*** main menu immediately. Or the configuration is incomplete in that there are still settings to be made that actually can be made using the IPSec Wizard. In this case you will be prompted to decide if

you want to finish the configuration using the Wizard or if you want to access the ***IPSEC*** main menu.

The prompt looks like this:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC]: IPSec Configuration - Main Menu                        MyRouter


       There are still some prerequisite configuration steps to do.
          Do you want to use the wizard?

                          Yes                 No
```

If you start the Wizard for the first time, all steps described in section A, chapter 3.1, page 48 need to be completed. If you are finishing an already existing configuration, you can skip past all steps previously completed (alternatively, you can make changes, too).

The following chapters describe each step of the IPSec Wizard where you are prompted for input. As described in section A, chapter 3.1, page 48, the IPSec Wizard completes a number of steps without prompting (like, e.g., adjusting your NAT settings if necessary). We will assume that you want to configure certificate based security, since this requires the most configuration steps.

1.3.1 Authentication Method

The first decision you have to make when using the IPSec Wizard is which authentication method you want to employ.

The menu window will look like this:

```
BinTec Router Setup Tool                          BinTec Communications AG
 [IPSEC][WIZARD]: IPSec Configuration - Wizard Menu              MyRouter

   IPSec 1st step configurations wizard

   Configuration History:
                DES3/SHA1,      CAST/SHA1, DES/SHA1                    ^
     - for AH:   none/SHA1,      none/MD5                              |
   + Check IPSEC default proposals ...                                 |
     created:                                                          |
     - for ESP:  NULL Rijndael Twofish Blowfish CAST DES DES3          |
                 MD5 SHA1 NOMAC                                        |
     - for AH:   SHA1 MD5                                              |
   + Check IPSEC Default Authentication Method ...                     |
     Currently unconfigured                                            =

==> Use which Default IPSEC Authentication Method ?     RSA Signatures
                                                      (<Space>  to choose)
                                                      (<Return> to select)
                                Exit
```

The only setting you can make here is the one for the field **Use which Default IPSEC Authentication Method?**

- Choose the authentication method you wish to use, either *Pre Shared Keys*, *DSA Sigantures*, *RSA Signatures* or *RSA Encryption*.
  For our example, choose ***RSA Signatures***.
- Confirm your choice by pressing **ENTER**.

  The Wizard stores the setting and proceeds to the next step. In this case it will check if any public key pairs are already installed on you router. If it does not find any key, it will create a standard 1024 bit RSA key.
- Proceed to section B, chapter 1.3.2, page 137.

1.3.2 Certificate Enrollment

Once the IPSec Wizard has either created a keypair or has found one on the router, it checks whether an own certificate is available. If no certificate is found, it prompts you whether to start a certificate enrollment.

The prompt looks like this:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][WIZARD]: IPSec Configuration - Wizard Menu              MyRouter

   IPsec 1st step configurations wizard

   Configuration History:
      - for ESP:  NULL Rijndael Twofish Blowfish CAST DES DES3          ^
                  MD5 SHA1 NOMAC                                        |
      - for AH:   SHA1 MD5                                              |
   + Check IPSEC Default Authentication Method ...                      |
     Currently set to "RSA Signatures"                                  |
   + Check for public key pair ...                                      |
     created Key RSA 1024 e=65537                                       |
   + Check for own Certificate ...                                      =

==> Request own certificate (initiate enrollment) ?     start
                                                       (<Space>  to choose)
                                                       (<Return> to select)
                              Exit
```

If you do not already have a certificate that you know you can download from a server or paste into the Setup Tool (see the next step), you may want to enroll for a certificate now. In order to do that you need some information. You are prompted to enter this information once the IPSec Wizard has taken you to the ***CERTIFICATE ENROLLMENT*** menu.

The menu window looks like this (see section A, chapter 3.9.1, page 92 for more information about the menu):

```
BinTec Router Setup Tool                      BinTec Communications AG
[IPSEC][WIZARD][ENROLL]: IPSec Configuration -
                         Certificate Enrollment              MyRouter

     Key to enroll:          1 (automatic key RSA 1024 (e 65537))

     Subject Name:

     Subject Alternative Names (optional):
       Type   Value

       IP     198.16.13.2
       DNS    Head_Router
       NONE


     Signing algorithm to use:   sha1WithRSAEncryption
     Server:
     Filename:                                                base64

                    Start                              Exit
```

You now must enter the data the IPSec Wizard needs to successfully send a certificate request to a CA. If you do have to request a certificate in this way, you may have to contact your prospective CA for details. Proceed as follows:

Key to enroll

- Choose the key for which you need a certificate. If there is only one key stored, it will be automatically chosen and you cannot make any changes to the selection.
  In our example, choose the key the IPSec Wizard has created for you: ***1 (automatic key RSA 1024 (e 65537))***.

Subject Name

- Enter a X.509 compliant subject name. See section A, chapter 2.4, page 36 for a detailed description of the X.509 syntax.
  An example for a X.509 name would be: ***CN=Head_Office, OU=Department, O=YourCompany, C=DE***. You need to enter the name as shown above, i.e. separated by commas.

Subject Alternative Names (optional)

Here you can optionally enter alternative descriptions by which your router can be identified, See table A-26, page 96 for information about the options you have here.

The router will assume its DNS name and its IP address as values for two of the three instances available.

Signing Algorithm to use

➤ Choose one of the algorithms available for your keypair, for a RSA key (such as is generated by the IPSec Wizard) there are two possibilities, *md5WithRSAEncryption* and *sha1WithRSAEncryption*.
For our example we will choose ***sha1WithRSAEncryption***.

Server

➤ Enter IP address or hostname of the TFTP server for certificates.The certificate request will be uploaded to this server.

Filename

➤ Enter a filename for your certificate request.
An example filename could look like this: ***request.pem***.

base64/binary

➤ Choose the coding for the request you are about to send.
Make sure to comply with your CA's standards. In general, base64 requests are the rule.

➤ When you have entered all the required details (only the Subject Alternative Names are optional in this menu), you send the request by highlighting **START** and hitting the **Return** key.

If the request was successfully sent to the TFTP server, a success message will be printed in the Setup Tool. Likewise an error message will show, if there have been problems sending the request.

➤ You can return to the IPSec Wizard main window by highlighting **EXIT** and hitting **Return**.

The IPSec Wizard now proceeds by prompting for an own certificate.

➤ Proceed to section B, chapter 1.3.3, page 140.

1.3.3 Import Own Certificate

Once you have received either the certificate you have requested as a file (again, the rule is a base 64 encoded file), you can import this certificate.

If you choose to do so, the IPSec Wizard takes you to the ***GET CERTIFICATE*** menu for own certificates:

```
BinTec Router Setup Tool                    BinTec Communications AG
[IPSEC][WIZARD][GETCERT]: IPSec Configuration -
                          Get Certificate                    MyRouter

     Import a Certificate/CRL using:  TFTP

      Type of certificate: Own Certificate


     Server:
     Name:                                                    auto

                    START                                   EXIT
```

Proceed as follows to import your own certificate:

Import a Certificate/CRL using

- First, you need to decide if you want to copy and paste the contents of your certificate directly into the Setup Tool, or if you want to download the certificate from a TFTP server.
  If you have received your certificate as a file and are not running a TFTP server of your own, choose *Direct Input*.
  If you are running a TFTP server you can copy the certificate to an export folder of the server and download it from there. In this case choose *TFTP*.

Please enter certificate data

This prompt and the space where you can paste the contents of the certificate is visible only if you have chosen *Direct Input* before.

- Copy the content of your own certificate into the clipboard of your computer and paste it into the Setup Tool.

You can open a base64 coded certificate in any text editor. It will look like this:


```
-----BEGIN CERTIFICATE-----
MIIENTCCA56gAwIBAgIBATANBgkqhkiG9w0BAQQFADCBvDELMAkGA1UEBhMCREUx
EDAOBgNVBAgTB0hhbWJ1cmcxEDAOBgNVBAcTB0hhbWJ1cmcxOjA4BgNVBAoTMVRD
IFRydXN0Q2VudGVyIGZvciBTZWN1cml0eSBpbiBEYXRhIE5ldHdvcmtzIEdtYkgx
IjAgBgNVBAsTGVRDIFRydXN0Q2VudGVyIENsYXNzIDAgQ0ExKTAnBgkqhkiG9w0B
CQEWGmNlcnRpZmljYXRlQHRydXN0Y2VudGVyLmRlMB4XDTk4MDMwOTEzNTQ0OFoX
DTA1MTIzMTEzNTQ0OFowgbwxCzAJBgNVBAYTAkRFMRAwDgYDVQQIEwdIYW1idXJn
MRAwDgYDVQQHEwdIYW1idXJnMTowOAYDVQQKEzFUQyBUcnVzdENlbnRlciBmb3Ig
U2VjdXJpdHkgaW4gRGF0YSBOZXR3b3JrcyBHbWJIMSIwIAYDVQQLExlUQyBUcnVz
dENlbnRlciBDbGFzcyAwIENBMSkwJwYJKoZIhvcNAQkBFhpjZXJ0aWZpY2F0ZUB0
cnVzdGNlbnRlci5kZTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA333mvr/V
8C9tTg7R4I0LfztU6IrisJ8oxYrGubMzJ/UnyhpMVBJrtLJGsx1Ls/QhC0sCLqHC
NJyFoMR4EdvbaycrCSoYTkDMn3EZZ5l0onw/wdiLI8hjO4ohq1zeHvSN3LQYwwVz
9Gq0ofoBCCsBD203W6o4hmc51+Vf+uR+zKMCAwEAAaOCAUMwggE/MEAGCWCGSAGG
+EIBAwQzFjFodHRwczovL3d3dy50cnVzdGNlbnRlci5kZS9jZ2ktYmluL2NoZWNr
LXJldi5jZ2k/MEAGCWCGSAGG+EIBBAQzFjFodHRwczovL3d3dy50cnVzdGNlbnRl
ci5kZS9jZ2ktYmluL2NoZWNrLXJldi5jZ2k/MDwGCWCGSAGG+EIBBwQvFi1odHRw
czovL3d3dy50cnVzdGNlbnRlci5kZS9jZ2ktYmluL1JlbmV3LmNnaT8wPgYJYIZI
AYb4QgEIBDEWL2h0dHA6Ly93d3cudHJ1c3RjZW50ZXIuZGUvZ3VpZGVsaW5lcy9p
bmRleC5odG1sMCgGCWCGSAGG+EIBDQQbFhlUQyBUcnVzdENlbnRlciBDbGFzcyAw
IENBMBEGCWCGSAGG+EIBAQQEAwIABzANBgkqhkiG9w0BAQQFAAOBgQBNB39fCTAZ
kqoFR3qUdVQqrs/82AxC4UU4KySVssqHynnEw5eQXmIYxsk4YUxoNdNMFBHrxM2h
qdjFnmgnMgc1RQT4XyGgYB4cAEgEWNLFy65tMm49d5WMhcflrlCddUp7/wsneepN
pFn/7FrqJqU5g6TReM6nqX683SvKEpMDSg==
-----END CERTIFICATE-----
```


Figure B-2: A base64 coded certificate

Server This field is visible only if you have chosen to import the certificate through a TFTP server.

- Enter the IP address or the resolvable hostname of the TFTP server you can download the certificate from. Note that you must not enter the scheme (i.e. tftp://) before the IP address or the hostname.

Name

- If you have imported the certificate by Direct Input, specify under which name the certificate should be stored on your router. An example name could be: ***own.pem***.
  If you intend to import the certificate from a TFTP server, specify the name, under which it is stored there.
- You can now start the import by highlighting **START** and hitting **Return**.

The IPSec Wizard now displays the certificate in a Certificate Review window. It may look, e.g., like this:

```
BinTec Router Setup Tool                      BinTec Communications AG
[IPSEC][WIZARD][GETCERT]: IPSec Configuration -
                          Review Certificate                  MyRouter

 Please Review retrieved Certificate:   [own.cer]

 Certificate =                                                          =
   SerialNumber = 1013591521                                            |
   SubjectName = <CN=Head_Office, OU=Department, O=YourCompany, C=DE    |
   IssuerName = <CN=CA, OU=Certification, O= CAName C=DE>               |
   Validity =                                                           |
     NotBefore = 2002 Feb 13th, 00:00:00 GMT                            |
     NotAfter  = 2002 Apr  1st, 00:00:00 GMT                            |
   PublicKeyInfo =                                                      |
     Algorithm name (X.509) : rsaEncryption                             |
     Modulus n  (1024 bits) :                                           |
       121179862766711621974009096377964165704639367311084553253160    |
       655517488847150073456622832102019191288071967602443814186358    v

                    IMPORT                              CANCEL
```

You can scroll through the certificate contents, the screenshot above only shows what can be seen in a single Setup Tool window.

- Review the certificate and check if all details are correct. If you are certain that the certificate is in order, you can finally store it on your router by highlighting **IMPORT** and hitting **Return**.

  The IPSec Wizard now takes you back to the main Wizard window and proceeds by prompting for a CA certificate.

- Proceed to section B, chapter 1.3.4, page 143.

1.3.4 Import New CA Certificate

A CA certificate is imported in the same way as an own certificate:

- Follow the instructions given above for the import of an own certificate.

Make sure to choose the filename properly (e.g. ***CA.pem***) when downloading from a TFTP server or to paste the correct certificate contents when using *Direct Input*. The IPSec Wizard cannot distinguish a peer certificate from a CA certificate, since they have the same logical structure.

After you have reviewed and stored the CA certificate on your router, the IPSec Wizard takes you back to the Wizard main window and proceeds by checking the availability of a CRL server.

➤ Proceed to section B, chapter 1.3.5, page 144.

1.3.5 Get Certificate Server for Retrieval of CRLs

A CRL (Certificate Revocation List) is essential for an IPSec configuration that makes use of certificates. This list is issued by most CAs on a regular basis. If you do not either statically store a CRL on your router or specify a server for dynamically checking CRLs, there is no way of knowing if a certain certificate is really valid or not.

Usually a CRL distribution point is contained within the CA certificate you have imported in the last step. If, however, this is not the case, you are prompted to specify a server from which the router can download CRLs.

To specify a server, the IPSec Wizard takes you to the ***CERTIFICATE SERVER*** menu:

```
BinTec Router Setup Tool                      BinTec Communications AG
[IPSEC][WIZARD][ADD]: IPSec Configuration - Wizard Menu       MyRouter

     Description:
     Url:
     Preference:    0


                    SAVE                                CANCEL
```

Proceed as follows to specify a certificate server:

Description

➤ Enter a convenient description for the server you want to add.

Url

➤ Specify the URL of the certificate server.

Preference

If you configure more than one certificate server, the router will check for CRLs beginning with the server that has the lowest preference number assigned to it. It will check the servers until it finds a CRL that covers the certificate in question.

➤ If your CA certificate specifies a CRL distribution point or you have CRLs statically stored on your router or you have specified a LDAP server, proceed to section B, chapter 1.3.7, page 146.
Otherwise proceed to section B, chapter 1.3.6, page 145.

If you entirely skip the configuration of CRL servers and CRLs, you are creating a severe security problem: Certificates will remain valid for your router, even if they have been revoked in the meantime. Thus, if, e.g., certificates are known to have been compromised and have been revoked, your router will still accept these certificates as long as is specified by the period of validity of the certificate in question.

If you choose to authenticate your phase-1 exchange by certificates, make sure to configure some sort of CRL.

1.3.6 Import New Peer Certificate

This prompt will only show if you have chosen RSA Encryption for authentication, but do not have configured a LDAP server, or if the peer certificates are not received during IKE negotiation. It is not possible to skip this step if it is required.

A peer certificate is imported in the same way as an own certificate:

➤ Follow the instructions given above for the import of an own certificate.

After you have reviewed and stored the peer certificate on your router, the IPSec Wizard takes you back to the Wizard main window.

There is an additional option for peer certificates: You can force the router to trust the certificate you have just stored.

➤ To do this, check the **Force Trusted** field in the peer certificate download menu: Highlight the checkbox and check the option using the side arrows.

Activating **Force Trusted** has the effect that your router does not require a CA certificate for the peer certificate.

➤ You can now proceed to section B, chapter 1.3.7, page 146.

1.3.7 Configure Peer

Configuring a peer is mandatory, i.e. you cannot skip this step during IPSec Wizard configuration. Since the IPSec Wizard only allows to configure a single IPSec peer, you may want to adjust the peer list configuration later (see section B, chapter 1.4, page 150).

The IPSec Wizard now takes you to the ***CONFIGURE PEER LIST*** menu:

```
BinTec Router Setup Tool                          BinTec Communications AG
[IPSEC][PEER][ADD]: IPSec Configuration - Configure Peer List MyRouter

     Description:
     Peer Address:
     Peer IDs:


                            SAVE                CANCEL
```

Proceed as follows:

Description

➤ Enter a convenient description for the peer you are about to configure. In our example, you would choose, e.g., ***Branch_Office***.

Peer Address

➤ Enter the IP address of the peer ***Branch_Office***, in our example ***198.16.13.1***.

If the peer you want to configure (unlike the one in our example) has the IP address dynamically assigned, leave the field blank. Note, that under this circumstances certain restrictions apply.They are explained in "Static and dynamic IP addresses", page 133.

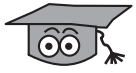
Peer IDs

➤ Enter the ID by which your router will identify the peer. Since our example assumes certificate based authentication, you would enter the X.509 name contained in the peer's own certificate, e.g. ***CN=Branch_Office, OU=Department, O=YourCompany, C=DE***.
See "IDs in IPSec", page 66 for important information on the choice of Peer IDs.

➤ You have now configured the basic peer parameters. Confirm your configuration with **SAVE**.

The IPSec Wizard takes you back to the main Wizard window and proceeds by checking for any already configured traffic lists. If there are none available (this will be the case if you are using the IPSec Wizard for the first time), it will prompt you to create one.

➤ Proceed to chapter section B, chapter 1.3.8, page 148.



The IPSec Wizard does not allow to specify the proposals to be used in Phase 1 and Phase 2. The default settings the router assumes are "Blowfish and MD5" for Phase 1 and "(ESP (Blowfish/MD5) no Comp)" for Phase 2.

These settings have the following meaning:

Proposal	Meaning
Blowfish/MD5	In Phase 1 the initiator suggests a single proposal that specifies a combination of encryption and hash algorithms. The responding router checks if it supports the suggested combination, and only if it agrees the exchange proceeds. *Blowfish/MD5* means that if your router initiates a Phase 1 exchange, it will suggest to use Blowfish for encryption and MD5 for authentication. This is a combination that should be supported by most third party routers.

Proposal	Meaning
(ESP (Blowfish/MD5) no Comp)	In Phase 2, the responder determines which of the proposals offered by the initiator will be chosen. *(ESP (Blowfish/MD5) no Comp)* means that the router will require Blowfish for encryption and MD5 for authentication. IPComP is not accepted.

Table B-1: Default proposals as set by the IPSec Wizard

1.3.8 Configure Peer Traffic

In order to protect the traffic between your router and peer router you have just configured you need to make at least one entry into the peer traffic list. This is the only traffic list entry you must specify manually. The necessary generic settings that allow IKE traffic to pass IPSec unchanged and that allow non-IPSec traffic to pass after the application of IPSec are made automatically by the IPSec Wizard.

The IPSec Wizard takes you to the ***EDIT TRAFFIC ENTRY MENU***. For creating a new entry, it looks like this:

```
BinTec Router Setup Tool                    BinTec Communications AG
[IPSEC][WIZARD][TRAFFIC][ADD]: Edit Traffic Entry            MyRouter

     Description:

     Protocol:      dont-verify

     Local:
          Type: net   Ip:                / 0

     Remote:
          Type: net   Ip:                / 0

     Action:        protect


                    SAVE                                CANCEL
```

Proceed as follows:

Description

➤ Enter a convenient description for this traffic entry; if you choose to protect all traffic between your and the peer router e.g. ***peer_traffic***.

Protocol

➤ If you choose to protect all traffic between your router and the peer, choose ***dont-verify***.
You can choose from specific protocols if you want to shape your IPSec traffic more precisely. If you want to protect e.g. your HTTP traffic, you will choose ***TCP***.

Local/Remote Type

➤ To protect traffic from your local network to the peer's remote network as in our example, choose ***net*** for both **Local** and **Remote Type**.

Local /Remote IP

Next specify the network addresses and the corresponding netmasks of the two networks:

➤ For **Local IP**, specify your own network's address, i.e. ***14.7.7.0/24*** in our example.

➤ For **Remote IP**, specify the branch office's network address, i.e. ***10.5.5.0/24*** in our example.

Local/Remote Port

This field only appears if for **Protocol** you have selected one of a number of protocols that are used for various services, namely TCP or UDP.

➤ If you have chosen a protocol that can connect to different ports, specify the port the traffic you want to protect will be sent over. For, e.g., HTTP traffic, this is ***TCP*** port ***80***.

Action

As long as you are using the IPSec Wizard the value for this field is set to *protect*, and you cannot change this setting here.

➤ When you have made the settings to specify the traffic you want to protect, confirm with **SAVE**.

The IPSec Wizard takes you back to the main Wizard window. You have now finished the IPSec Wizard configuration and are presented with a last choice: To dump the messages that have been printed to the console during configuration to the syslog host of your router or to clear the configuration (in which case you would have to start from scratch).

➤ If you do not want to do either, leave the IPSec Wizard with **EXIT**.

You are now taken to the ***IPSEC*** main menu. If you do not want to adjust the settings made by the IPSec Wizard, you should now save the configuration

as boot configuration. Otherwise you will loose it after with next reboot of your router.

➤ Leave the ***IPSEC*** menu with **SAVE**, then go to ***EXIT*** and choose **Save as boot configuration and exit**.

1.4 Reviewing and Adjusting the IPSec Wizard Configuration

With the IPSec Wizard completed the two peers can now securely exchange data (depending on the traffic entry you have made). There may be two more steps to take in order to ensure your configuration is sound. You may want to review the configuration to obtain a clear picture of which settings have been made, and you may want to adjust certain settings where the IPSec Wizard has assumed certain generic default values.

1.4.1 Reviewing the IPSec Wizard Configuration

Once you have completed the IPSec Wizard, you are taken to the IPSec main menu. From here you can access all the menus the IPSec Wizard has guided you through. To see which settings the Wizard has ultimately made, we will go through all of the menus to which changes have been made and identify the settings made.

Pre IPSec Rules

The Pre IPSec Rules menu window should now look like this:

```
BinTec Router Setup Tool                      BinTec Communications AG
[IPSEC][PRE IPSEC TRAFFIC]: IPSec Configuration -
                            Configure Traffic List            MyRouter

  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




   APPEND             DELETE              SAVE               CANCEL
```

The entry was automatically created by the IPSec Wizard. It is necessary to let all IKE traffic pass IPSec unchanged. If this is not ensured, the phase-1 exchange between your router and the peer cannot take place.

The entry can be read as follows: Traffic from any IP address in the LAN (**Local Address**=*0.0.0.0*, **M/R**=*M0*) using UDP port 500 (**Port**=*500*, **Proto**=*udp*) to any IP address in the WAN (**Remote Address**=*0.0.0.0*, **M/R**=*M0*) with the destination port 500 (**Port**=*500*) has to be passed in plain text (**A**=*PA*). You can ignore the setting (*default*) for **Proposal**, since no encryption or authentication takes place while the Pre IPSec rules are applied.

Configure Peers

The ***CONFIGURE PEERS*** ➧ **EDIT** menu now has the peer entry you made:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][PEERS][EDIT]: IPSec Configuration -
                      Configure Peer List                       MyRouter


  Description:   branch
  Peer Address:  198.16.13.1
  Peer IDs:      CN=Branch_Office, OU=Department, O=YourCompany, C=DE

  Special Settings >
Traffic List: Highlight an entry and type 'i' to insert new entry below
         'u'/'d' to move up/down, 'a' to select as active traffic list
          <another bit of help>

Local Address  M/R Port Proto Remote Address M/R Port A   Proposal
*14.7.7.0      M24   -  all   10.5.5.0       M24   -  PR  default



      APPEND             DELETE              SAVE              CANCEL
```

The settings can be read as follows: You have configured a peer called *Branch_Office*; the peer's ID is the subject name of the certificate he or she uses for authentication (the Setup Tool shows an extract from that name: *CN=Branch_Office, OU=Department, O=YourCompany, C=DE*); the peer's router is at IP address *198.16.13.1*.

To verify the peer traffic list entry you have created during IPSec Wizard configuration, check the lower half of the menu window. There the entry is displayed. It reads like this: All traffic (**Port**=-, **Proto**=*all*) from the local network at *14.7.7.0* (containing the IP addresses specified by the netmask (**M/R**) *24*) to the network at *10.5.5.0* (containing the IP addresses specified by netmask **M/R** *24*) is protected using the *default* **Proposal** for Phase 1. You can check the settings for the default proposal later in ***IKE (PHASE 1) DEFAULTS***.

Post IPSec Rules

In the Post IPSec menu, there are no complex settings to observe: The IPSec Wizard has set the **What to do with anything that didn't match** field to *let pass*. This ensures that all traffic that has not matched either the Pre IPSec rule

or the peer traffic list is allowed to pass instead of dropped. Note that, therefore, the router will still send unsecured traffic to other hosts and networks, and that only the peer traffic you have specified is protected.

IKE (Phase 1) Defaults

The settings in this menu have been automatically created by the IPSec Wizard, either as a consequence of other settings made by you or as generic default settings:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IPSEC][PHASE 1]: IPSec Configuration -
                  Phase 1 (IKE) Settings                        MyRouter

   Proposal              :  1 (Blowfish/MD5)
   Lifetime              :  900 Sec/0 Kb (def)
   Group                 :  2 (1024 bit MODP)
   Authentication Method :  RSA Signatures
   Mode                  :  id_protect
   Local ID              :
   Local Certificate     :  1 (own.cer)

   Edit Proposals >
   Edit Lifetimes >


                         SAVE                          CANCEL
```

The settings in this menu are not peer specific, and hence cannot be read in a single context as the above ones. Here is a table to explain the settings:

Setting	Explanation
Proposal: *1 (Blowfish/MD5)*	The router is set to suggest the use of Blowfish for encryption and MD5 for authentication when triggering a phase-1 exchange. This setting is made automatically.
Lifetime: *900 Sec/0 Kb (def)*	The keys negotiated in Phase 1 are renewed after 900 seconds. The amount of data processed does not play a role in determining the moment of rekeying. This setting is made automatically.

Setting	Explanation
Group: *2 (1024 bit MODP)*	The key length used for calculating new keying material is set to 1024 bit. This setting should offer a good balance of security and speed. This setting is made automatically.
Authentication Method: *RSA Signatures*	RSA Signatures is used for the initial authentication during Phase 1. This is the setting offering the highest security, but it also poses the most restriction (like, e.g., storing a peer certificate when not specifying a CRL or certificate server). You have chosen the authentication method during IPSec Wizard configuration.
Mode: *id_protect*	The IPSec Wizard set the IPSec mode to *id_protect* per default. This setting offers higher security than aggressive mode, but it is not possible with dynamic IP addresses and pre shared keys. This setting is made automatically.
Local ID: -	After IPSec Wizard configuration, this field is empty. This does not mean that there is no **Local ID** available; it means that the router will take the **Local ID** from the your own certificate if you have chosen certificate authentication as in our example. This setting is made automatically.
Local Certificate: 1 *(own.cer)*	The router displays the certificate you have entered as own certificate during IPSec Wizard configuration. This setting is made automatically, but if you have stored more than one own certificate, you can choose among them.

Table B-2: Phase-1 settings after IPSec Wizard configuration

IPSec (Phase 2) Defaults

Like the settings of the ***IKE (PHASE 1) DEFAULTS*** menu, the settings of this menu are peer independent.

The following table explains the settings made by the IPSec Wizard:

Setting	Explanation
Proposal: *1 (ESP (Blowfish/MD5) no Comp)*	In Phase 2, the router will require Blowfish for encryption and MD5 for authentication. IPComP is not accepted. This setting is made automatically.
Lifetime: *900 Sec/0 Kb (def)*	The keys negotiated in Phase 2 are renewed after 900 seconds. The amount of data processed does not play a role in determining the moment of rekeying. This setting is made automatically.
Use PFS: *no*	PFS (Perfect Forward Secrecy) is disabled. This means that the router will not perform a complete Phase 1 exchange to create new keying material, but the material created during the initial Phase 1 is reused to generate new keys for Phase 2. This setting is made automatically.

Table B-3: Phase-2 settings after IPSec Wizard configuration

Certificate and Key Management

This menu comprises all settings made for keys and certificates. There are five submenus, containing the settings for your keys, own certificates, CA certificates, peer certificates, CRLs and certificate servers. They all equally show a list of configured items when you enter them.

Key Management

When entering the ***KEY MANAGEMENT*** menu, you will see the most basic information about the key the IPSec Wizard has created for you. In our example the settings are:

- **Description** of the key (***automatic key RSA 1024 (e 65537)***)

- **Algortihm** used (***rsa***)
- **Key length** (***001024=1024 bit***)

Own Certificates

The menu ***OWN CERTIFICATES*** lists the basic information about the own certificate you have imported during IPSec Wizard configuration:

- **Description**: ***own.cer***
- **Flags** that might be set: ***O*** (= own)
- the serial number of the certificate
- **Subject Names**: you have specified at least a subject name when requesting the certificate, in our example it looks ilke this: ***CN=Head_Office, OU=Department, O= YourCompany C=DE***.

CA Certificates

Analogically, the ***CA CERTIFICATES*** menu displays information about the CA certificates. The details are the same as in the ***OWN CERTIFICATE*** menu; in our example they might read:

- **Description**: ***CA.cer***
- **Flags**:***CA, N, T*** (=Certificate Authority, No CRLs, Force Trusted)
- the serial number of the certificate
- **Subject Names**: ***CN=CA, OU=Certification, O= CAName C=DE***.

Peer Certificates

In our example there are no entries in the ***PEER CERTIFICATE*** menu. If you have to import a peer certificate, the same details are shown as in the other certificate menus.

Certificate Revocation Lists

According to our example configuration with the IPSec Wizard this menu will not have an entry either, since there are no CRLs statically stored on the router.

Certificate Servers

The last submenu, ***CERTIFICATE SERVERS***, has a single entry for the certificate server you have specified during IPSec Wizard configuration. The following details are displayed:

- **Description**: the description you have entered when specifying the Certificate server
- **URL**: the address of the server, in our example: ***ldap://ldapservice.yourCA.com***

- **Pref**: the preference you have assigned to the server, in our example ***0***

These are all the settings that are made during IPSec Wizard configuration. The remaining menus are not touched by this process and need not be described here. Especially the settings in the ***ADVANCED SETTINGS*** menu should only be changed if problems with the current configuration arise. For detailed information about the settings see section A, chapter 3.10, page 103.

1.4.2 Adjusting the IPSec Wizard Configuration

Even though the configuration by the IPSec Wizard is sufficient to protect all or the most of the important traffic between the head and the branch office, you may want to adjust the settings where the IPSec Wizard does not offer a choice. This may, above all, pertain to the following settings:

- peer configuration - you may want to add another peer with the same security settings (e.g. another branch office)
- peer traffic lists - you may not want to protect the entire traffic between two peers, but likewise do not want to protect only a single kind of traffic
- phase-1 and phase-2 proposals - you may want to choose different proposals, either specifically for certain peers, or in general

These adjustments are covered in brief in this chapter.

Adding Another Peer

If you want to add another peer with the same security settings as the one you have created during IPSec Wizard configuration, proceed as follows:

➤ Go to ***IPSEC*** ➧ ***PEER CONFIGURATION*** ➧ **APPEND** and enter the specifics of the new peer as described in section B, chapter 1.3.7, page 146, e.g.:
  – **Description**: ***Branch_Office_2***
  – **Peer Address**: ***198.16.13.3***
  – **Peer ID**: ***CN=Branch_Office_2, OU=Department, O=YourCompany, C=DE***

➤ Confirm with **SAVE** and enter the ***PEER CONFIGURATION*** ➧ **EDIT**

➤ Enter the **APPEND** menu from the bottom of the **EDIT** menu window to create a traffic list entry for the new peer.
Use the same values as in section B, chapter 1.3.8, page 148, but make sure to use the new peer's LAN address for the **Remote Type** settings, e.g. ***16.8.8.0***.

You have now added another peer who is treated in the same way as the peer you have configured during IPSec Wizard configuration.

Refining the Traffic Lists

During IPSec Wizard Configuration, you have either chosen to protect all traffic between the peers, or to protect only a certain kind of traffic. If you do not want to protect all traffic indiscriminately, but need to protect several kinds of traffic, you need to adjust the peer traffic lists.

Let us assume you want to protect certain kinds of traffic directed at the Branch Office:

- SMTP traffic for secure sending of e-mails
- FTP traffic for secured file transfers
- TELNET for a secure login to hosts in the remote WAN.

The kinds of traffic you want to protect require only little configuration: Basically, you need to create a traffic list entry for each of them in which you specify the protocol and the port used for the respective kind of service. All other settings, Local and Remote Type as well as the IP addresses and netmasks, can be copied from the entry you have created before.

The specific settings you need are these:

- SMTP:
  - **Protocol**: *TCP*
  - **Remote Port**: *25*
  - **Action**: *protect*
- FTP:
  - **Protocol**: *TCP*
  - **Remote Port**: *20*
  - **Action**: *protect*

- TELNET:
  - **Protocol**: *TCP*
  - **Remote Port**: *23*
  - **Action**: *protect*

To create an entry with the parameters described above, go to ***IPSec*** ➧ ***Configure Peers*** ➧ **EDIT** for the peer for which the traffic list entries should be created. Proceed as follows:

➤ Enter the **APPEND** menu at the bottom of the peer **EDIT** window and enter the settings detailed above, plus the address details which you know from IPSec Wizard configuration.

➤ Repeat the procedure for each of the services you want to protect, and for each of your configured peers. Then leave the IPSec menus with **SAVE** and **EXIT** until you return to the Maine Menu.
Choose ***Exit*** and in the next window **Save as boot configuration and exit** to permanently save your settings.

Adjusting Proposals

There are two ways in which you can adjust the proposals according to which traffic between your router and the peer router is protected:

- You can change the default settings in ***IPSec*** ➧ ***IKE (Phase 1) Defaults*** and ***IPSec*** ➧ ***IPSec (Phase 2) Defaults***. This means that the same settings will be used for every peer that does not have proposals specifically assigned.
  After IPSec Wizard configuration IKE and IPSec proposals are set to rather common values that allow for interoperability. If you change the default settings to less common values, you must make sure to check whether each of your peers supports the new settings. If any of your peers does not do so, you must configure security settings specifically for this peer.

- You can change the security settings for such peers you know support or require other settings than the defaults chosen by the IPSec Wizard (in ***IPSec*** ➧ ***Peer Configuration*** ➧ **EDIT** ➧ ***Special Settings*** ➧ ***Phase 1*** and ***Phase 2***). This option ensures that the faster and/or more secure settings are used with this peer while it retains the interoperability of all peers that use the default values.

Let us assume, e.g., to use the following settings with your peer ***Branch_Office***:

- IKE (Phase 1): ***Rijndael*** for encryption and ***Tiger 192*** for authentication
- IPSec (Phase 2): ***Rijndael*** for encryption and ***MD5*** for authentication with ***ESP*** for IPSec protocol.

You can choose either of the procedures described above:

Changing the defaults

If you decide to change the default settings for all peers:

- Go to ***IPSec*** ➧ ***IKE (Phase 1) Defaults***
- Choose the proposal you want to use for IKE in the field **Proposal**, for our example ***17 (Rijndael/Tiger192)***.
- Leave ***IPSec*** ➧ ***IKE (Phase 1) Defaults*** by confirming with **SAVE**.
- Go to ***IPSec*** ➧ ***IPSec (Phase 2) Defaults***.
- Choose the proposal you want to use for IPSec from the field **Proposal**, for our example***23 (ESP(Rijndael/MD5))***.
- Leave the menu by confirming with **SAVE**.
  If this is all the configuration you intend to do at this time, you should now save the new configuration as boot configuration.

Changing the proposals for a specific peer

If you decide to change the settings for a specific peer only:

- Go to ***IPSec*** ➧ ***Configure Peers*** ➧ **EDIT** ➧ ***Special Settings*** ➧ ***Phase 1***.
- Choose the proposal you want to for IKE use in the field **Proposal**, in our example ***17 (Rijndael/Tiger192)***.
- Leave ***IPSec*** ➧ ***IKE (Phase 1) Defaults*** by confirming with **SAVE**.
- Go to ***IPSec*** ➧ ***Configure Peers*** ➧ **EDIT** ➧ ***Special Settings*** ➧ ***Phase 2***.
- Choose the proposal you want to use for IPSec from the field **Proposal**, for our example***23 (ESP(Rijndael/MD5))***.
- Leave the menu by confirming with **SAVE**.
  If this is all the configuration you intend to do at this time, you should now save the new configuration as boot configuration.

There is another important modification of your IPSec configuration you may want to make use of: Dynamic IPSec. Dynamic IPSec allows you to create IPSec tunnels even if both peers involved use dynamically assigned IP addresses. Dynamic IPSec is described in general in section A, chapter 2.5, page 44 and in section A, chapter 4, page 113. Its configuration is described in the next chapters.

1.5 DynIPSec Configuration

As described in section A, chapter 2.5, page 44, it is possible to use IPSec even if peers have IP addresses assigned dynamically. There are two basic scenarios when you can make use of this:

Basic scenarios for Dynamic IPSec

- Both peers have their IP addresses assigned dynamically. In this case none of the peers can identify the other if Dynamic IPSec is not used. Identification of the peer is necessary, however, to choose the appropriate SAs.
- Only one of the peers has a static IP address, but it is desired that this peer can trigger IPSec tunnel creation with the "dynamic peer". In order for this to work, the IP address of the peer with a dynamically assigned IP address must be known.

Note that even though Dynamic IPSec makes it possible to use IPSec with dynamic IP addresses it does not obviate any restrictions that apply to IPSec with dynamic IP addresses, i.e. the use of preshared keys for authentication is only possible in Aggressive Mode.

Note, also, that if you do not use certificates for authentication, you need to configure IDs as described in "IDs in IPSec", page 66.

Remember: If only one of two peers uses a dynamically assigned IP address, and if it is not necessary that this peer can be the responder in a tunnel creation, then you need not use Dynamic IPsec.

1.5.1 Preparatory DynDNS Configuration

Let us assume that your peer, ***Branch_Office_2***, uses dynamically assigned IP addresses.

In order to use your routers with Dynamic IPSec, ***Branch_Office_2*** needs to configure the DynDNS service that is available on all routers of the X-Generation running System Software 6.2.2 or higher. For a general description of DynDNS and the menus that are relevant for configuring this service, see section A, chapter 4, page 113.

For our example, ***Branch_Office_2*** has registered the hostname ***dyn-peer.dyndns.org*** with dyndns.org. Registering a hostname is usually done through a web interface on a DynDNS provider's website.

DynDNS configuration for *Branch_Office_2*

Once ***Branch_Office_2*** has registered the hostname, they can start configuring the router for the use of DynDNS. These are the directions ***Branch_Office_2*** has to follow:

- Go to ***IP*** ➧ ***DynDNS*** and choose **ADD** in order to create a new service entry.
- Fill in or choose the desired values for the fields in this menu.

These are the settings for our example configuration:

Field	Value
Host Name	***dyn-peer.dyndns.org*** This is the hostname you have registered with your DynDNS provider.
Interface	***internet*** This is the interface through which the dynamic IP address of your router should be publicized.
User	***dyn-peer*** This is the username under which you have registered the DynDNS hostname. Depending on your DynDNS provider it may, but need not be the same as the first part of your hostname.

Field	Value
Password	***secret*** This is the password you have chosen when registering with your DynDNS provider.
Provider	***dyndns*** This is your DynDNS provider. There is a number of preconfigured providers, but you can also add further ones. See section A, chapter 4.1, page 113 for further information.
MX	(blank) This activates a mail exchanger for the machine you are running the DynDNS service on. This setting will usually not be relevant for Dynamic IPSec.
Wildcard	***off*** This enables the use of wildcards for additional DNS resolution. This setting will usually not be relevant for Dynamic IPSec.
Permission	***enabled*** This activates the DynDNS service.

Table B-4: Example values in ***IP*** ➧ ***DynDNS*** ➧ **ADD**

The configuration window now looks like this:

```
BinTec Router Setup Tool                        BinTec Communications AG
[IP][DYNDNS][ADD]: Dynamic DNS Service                           MyRouter

          Host Name                 dyn-peer.dyndns.org
          Interface                 internet
          User                      dyn-peer
          Password                  ******

          Provider                  dyndns
          MX
          Wildcard                  off
          Permission                enabled


                    SAVE                                CANCEL
```

You have completed the DynDNS service configuration and should save it:

- Choose **SAVE** to save the configuration and trigger a first publication of your IP address. The update takes place only if the interface the DynDNS service uses already has an IP address, i.e. if it is in an *up* state.
  You should now save the configuration as boot configuration by choosing **Save as boot configuration and exit** in the ***EXIT*** menu you can access from the Setup Tool main menu.

Once you have configured the DynDNS service, you have created the conditions for using Dynamic IPSec.

Note that each peer using dynamically assigned IP addresses must register a hostname and complete the configuration described above if they should be able to play the role of a responder in IPSec.

1.5.2 IPSec Wizard Configuration for Dynamic IPSec

As mentioned above, there are two possible basic scenarios for the use of Dynamic IPSec:

- Only one peer uses a dynamically assigned IP address, but it should be possible to reach this peer with a tunnel creation request.

- Both peers use dynamically assigned IP addresses. This means that at least one of the peers must configure DynDNS to make tunnel creation possible.

Configuration with one "Dynamic Peer"

Adjusting an existing configuration

If you have completed IPSec Wizard configuration, you only need to adjust a single setting to prepare the same configuration for the use with Dynamic IPSec (see section A, chapter 4.2, page 118 for a description of the relevant menus).

The example assumes that your peer (***Branch_Office_2***) uses a dynamically assigned IP address. This is the configuration ***Head_Office*** (the peer with the assumed static IP address) has to enter:

➤ Go to ***IPSEC*** ➧ ***CONFIGURE PEERS*** ➧ **EDIT**

➤ Enter the hostname ***Branch_Office_2*** has registered with their DynDNS provider as value for the **Peer Address** field.

The peer configuration now looks like this (the example assumes that authentication is done with certificates):

- **Description:** ***Branch_Office_2***
- **Address:** ***dyn-peer.dyndns.org***
- **Peer ID:** ***CN=Branch_Office_2, OU=Department, O=YourCompany, C=DE***

➤ Return to the Setup Tool main menu by leaving the IPSec menus with **SAVE** or **EXIT**.

➤ In the main menu, choose **EXIT** and save your configuration as boot configuration.

Branch_Office_2 does not have to change the IPSec configuration for their peer ***Head_Office***, since ***Head_Office*** uses a static IP address.

Creating a new Dynamic IPSec configuration

If you want to create a Dynamic IPSec configuration right from the start, you can use the IPSec Wizard. Again, this is the configuration ***Head_Office*** has to enter:

➤ Follow all the steps described in section B, chapter 1.3, page 135 until you reach the **Configure Peer** section.

➤ When filling in the required information for a new peer (see section B, chapter 1.3.7, page 146), enter the DynDNS hostname ***Branch_Office_2*** has registered with their DynDNS provider in the field **Peer Address**.

The configuration is the same as the one described above.

➤ Save the peer and thus return to the IPSec Wizard main menu.

Note that if not using certificates you must configure IDs as described in "IDs in IPSec", page 66.

➤ Continue configuration with the IPSec Wizard and save the new configuration as boot configuration.

Dynamic IPSec is now enabled and you are able to create secure tunnels when ***Branch_Office_2*** is using a dynamically assigned IP address.

Configuration with Two "Dynamic Peers"

If both peers (***Head_Office*** and ***Branch_Office_2***) use dynamically assigned IP addresses, at least the peer that is to respond to the tunnel creation request (e.g. ***Head_Office***) must configure DynDNS. Then it is, however, not possible that ***Head_Office*** triggers an IPSec tunnel creation with ***Branch_Office_2***. In this case it may be preferable that both peers configure DynDNS so that IPSec tunnels can be created in either direction.

The instructions you need to follow are the same as for only one "dynamic peer", but you must make sure to configure the **Peer Address** field appropriately.

The peer configuration ***Head_Office*** enters for ***Branch_Office_2*** as peer is the same as described above:

- **Description:** ***Branch_Office_2***
- **Address:** ***dyn-peer.dyndns.org***
- **Peer ID:** ***CN=Branch_Office_2, OU=Department, O=YourCompany, C=DE***

Assuming that ***Head_Office*** has registered the hostname ***dyn-head.dyndns.org***, ***Branch_Office_2*** must enter the following configuration for ***Head_Office*** as peer:

- **Description:** ***Head_Office***
- **Address:** ***dyn-peer.dyndns.org***
- **Peer ID:** ***CN=Head_Office, OU=Department, O=YourCompany, C=DE***

For information on how to choose IDs for IPSec, see "IDs in IPSec", page 66.

You have now configured DynIPSec for two peers with dynamically assigned IP addresses. Keep in mind that you need to save your configuration and should even save it as boot configuration in the ***EXIT*** menu accessible form the main menu.