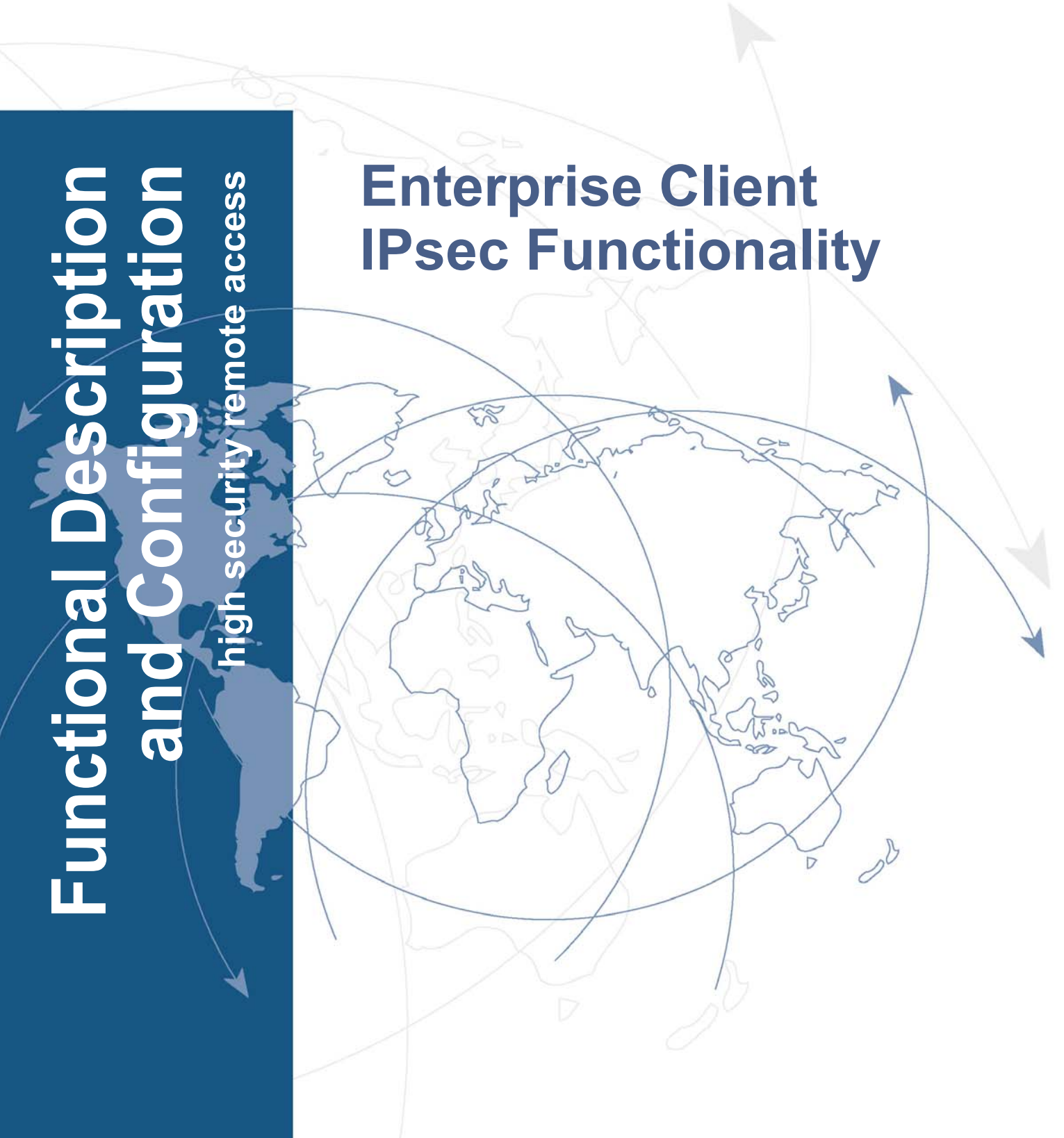


Functional Description and Configuration

high security remote access

Enterprise Client IPsec Functionality





Copyright

Considerable care has been taken in the preparation and publication of this manual, errors in content, typographical or otherwise may occur. If you have any comments or recommendations concerning the accuracy, then please contact NCP as desired.

NCP makes no representations or warranties with respect to the contents or use of this manual, and explicitly disclaims all expressed or implied warranties of merchantability or use for any particular purpose.

Furthermore NCP reserves the right to revise this publication and to make amendments to the content, at any time, without obligation to notify any person or entity of such revisions and changes. This manual is the sole property of NCP and may not be copied for resale, commercial distribution or translated to another language without the express written permission of NCP engineering GmbH.

All trademarks or registered trademarks appearing in this manual belong to their respective owners.

© NCP engineering GmbH,
February 2010

Network
Communications
Products engineering GmbH

GERMANY
Headquarters:
Dombühler Straße 2
D-90449 Nürnberg
Tel.: +49-911-99680
Fax: +49 - 911 - 9968 299
internet
<http://www.ncp-e.com/en>
E-mail: info@ncp-e.com

IPsec Functionality and Configuration



The first section of this document describes generally the **Functionality** of IPsec.

The second section describes the **Configuration of IPsec Tunneling with NCP Clients**. The differences between Entry- and Enterprise Client are shown.

IPsec Functionality

IPsec is a standard with superb security mechanisms which functions in certain VPN scenarios when it is implemented with permanent IP addresses such as B2B, or Extranet. In these cases VPN gateways from different suppliers can be implemented. Highresolution security settings up to the port level are possible in these cases. However IPsec can only be implemented for IP data traffic.

The IPsec specification includes not only Layer 3 tunneling but also includes all necessary security mechanisms like strong authentication, key exchange and encryption.

The IPsec RFC's (2401-2409) permit the development of a VPN with specified IP security. IPsec tunneling and security are thoroughly described making a complete VPN framework available. In principle it is possible to use vendor-independent components. For site-to-site VPN's the gateways may be supplied by different manufacturers, for end- to-site gateways the clients may be supplied by another manufacturer. The establishment of a connection to IPsec traffic is based on the Internet Key Exchange Protocol (IKE).

The IPsec Process

In every IP host (client or gateway) that supports IPsec there is an IPsec module i.e. an IPsec engine. This module examines each packet for certain characteristics in order to apply the appropriate security negotiation to it.

Testing of the outgoing IP packets from the IP stack occurs relative to a Secure Policy database (SPD). With this all configured SPDs will be processed. First the static SPD's listed in the IPsec branch of the configuration tree and then if no agreement is found then the dynamic SPD's are processed.

The SPD consists of multiple entries (SPD entries), which in turn contain a filter portion. The filter portion or Selector of an SPD entry consists primarily of IP addresses, UDP, and TCP ports as well as other IP header-specific entries. If the values of an IP packet agree with the values from the SPD entry Selector portion, then further determination as to what should be done with this IP packet is made from the SPD Entries. The packet can simply be allowed through (permitted), or discarded, or certain security policies of the IPsec process can be imposed on the packet. These security policies are also described in the SPD entry.

If, in this manner, it is determined that an IP packet is linked with an SPD entry that triggers an IPsec process, then it will be examined to see whether a security association (SA) exists for this SPD entry. If an SA does not yet exist then first an authentication and a key exchange will take place before the negotiation of an SA (see below → "IPsec Negotiation Phase 1")

After the SA negotiation, negotiations follow for data packet encryption (ESP) and/or authentication (AH) and also to determine whether transmission should be in Transport or Tunnel mode.

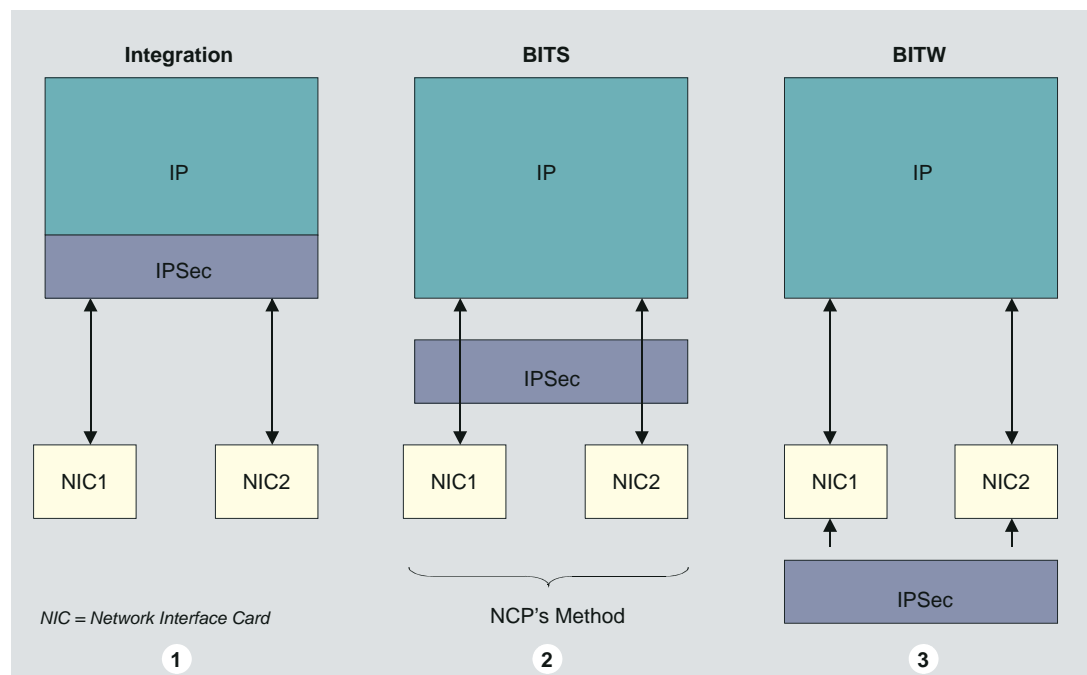
IPsec Implementation

The SA describes which security protocol should be used (ESP or AH). ESP (Encapsulating Security Payload) supports the encryption and authentication of IP packets. AH (Authentication Header) supports only the authentication of IP packets. The SA also describes the operating mode in which the security protocol should be used either Tunnel or Transport mode. In Tunnel mode an IP header is inserted, in Transport mode the original header is used. Additionally the SA describes which algorithm will be used for authentication, which encryption method (for ESP) and which key should be used. Of course the other side should work according to the same SA.

If the SA is negotiated, then each packet will be processed according to the operating mode and protocol, either Tunnel or Transport, and either ESP or AH respectively.

There are three different types of IPsec Implementation:

1. Integration – in this case IPsec is completely integrated within the IP stack. However this is only possible if the same manufacturer developed the IP stack and the IPsec.
2. BITS (Bump in the Stack) – in this case IPsec is implemented through additional drivers between Layer 2 and the network adapter. This is the most widely used method and is also the method used by NCP. The NCP IPsec module presents itself as a LAN adapter and intermediate driver for IPsec and tunneling. The NCP IPsec implementation conforms to RFC and is completely compatible with third-party manufacturers.
3. BITW (Bump in the Wire) – with this type of implementation IPsec is integrated in the hardware.



IPsec Services

IPsec offers different security services through the selection of alternative security protocols and encryption algorithms. Regarding security protocols, an authentication protocol is determined by the header (authentication header /AH), and a combined encryption and authentication protocol is determined by the format (Encapsulating Security Payload /ESP). The following security services are made available through IPsec:

- Access Control
- Integrity, AH/ESP
- Data origin Authentication, AH/ESP
- Confidentiality, ESP

IPsec Policy

The IPsec Policy determines:

- how authentication is to be formed, that is with ESP encrypted or with Hash values (Transform / Authentication)
- whether a complete Diffie Hellmann, (DH Group), key exchange (PFS) should occur in Phase 2 in addition to the SA negotiation
- which criteria will govern the duration of the key validity. (Duration / Validity)
- which security protocol is to be used, AH or ESP

[In the IPsec configuration of the Client a IPsec policy with ESP is stored. The usage of the AH protocol is not intended by NCP. See the sections **Security** and **IPsec Settings** in the description **Secure Client Parameters**.]



AH and ESP in Transport and Tunnel Mode

Note for the following description the graphic on the next page.

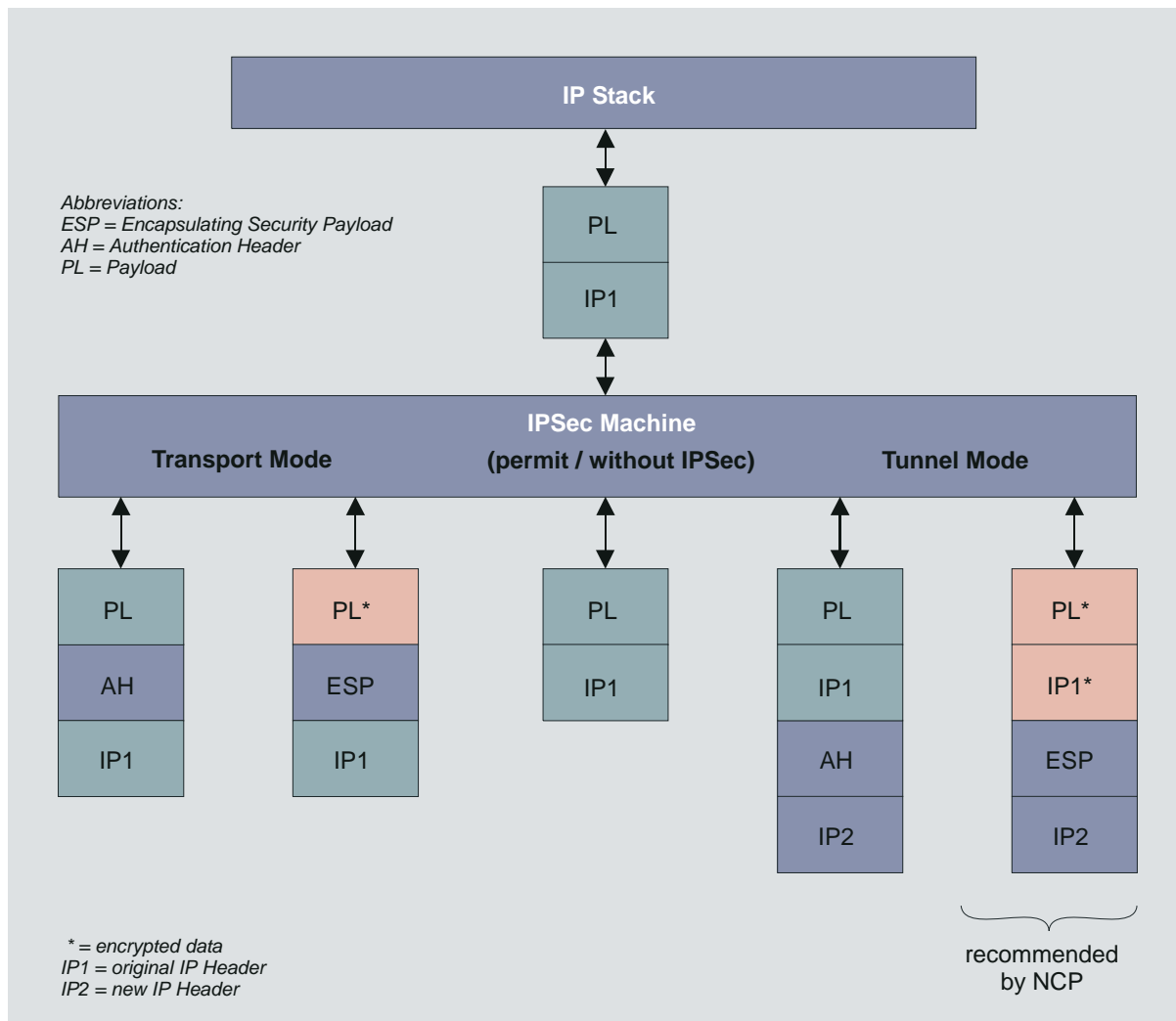
Each of the IPsec security protocols, AH and ESP, supports two different operating modes, Transport and Tunnel modes.

AH in Transport mode authenticates the payload of the IP packet as well as selected parts of the IP header (IP1). ESP in Transport mode encrypts and authenticates the payload of the IP packet but not the header (IP1). In Transport mode destination and source address are transmitted unencrypted with the IP header. In other words source and destination addresses remain unprotected. Transport mode is therefore suitable only for direct communication between two hosts with permanent IP addresses or between LAN workstation computers. This mode is totally unsuitable for flexible remote access.

In tunnel mode the entire IP packet, including the inserted AH or ESP field, is encapsulated and provided with a new IP header (IP2). In this manner the IP packet is sent through a Layer 3 tunnel. The inner IP header with original address is accordingly hidden and cannot be viewed – only the Layer 3 tunnel end points can be identified. Networked computers behind firewalls or routers with IPsec can communicate securely with each other in this mode. The new IP header (IP2) can contain completely different source and destination addresses than the original header but it must hold necessary information ready for the corresponding station that enables it to accept and forward the encapsulated packet according to the SA guidelines of the security link. This mode is the standard setting for the Secure Server.

The questions of which IPsec security protocol should be combined with which encryption algorithm, and with which authentication type, are determined in the IPsec guidelines (IPsec policy). In the SPD there is reference made to these guidelines, i.e. to the security protocol as well as to the operating mode whether tunnel or transport.

Function of the IPsec Maschine



The above graphic shows how an IPsec data frame is sent from the IP stack to the IPsec module. The original IP header (IP1) is processed with its payload. The lower portion of the graphic shows the result of the IPsec process.

Transport Mode is only suitable for host-to-host communication. Tunnel mode, on the other hand, also enables operation over a VPN /GW. The IP header enables transfer from a client over the Internet via a gateway. The VPN /GW removes the IP2 header then encrypts, and sends the frame further on to a local LAN. Generally you should only consider Tunnel Mode for remote access and end-to-site VPN's.

Applications

Layer 3, IP oriented authentication and encryption occur in both IPsec operation modes. Thus IPsec is particularly well suited for implementations in which both communication end points are identified by official IP addresses, or in other words, when the connection has been predefined.

IPsec also assures that a secure communication between branch offices of an enterprise. The security of this LAN-to-LAN communication over a public network can also be assured without a leased line. An enterprise can use the Internet for this purpose. The requirement however is that a firewall or router, with IPsec functionality at the dial-in point must also be provided with a permanent official IP address.

Similarly Extranet and Internet connections to partners can be protected when authentication and confidentiality are guaranteed and a key exchange mechanism has been determined.

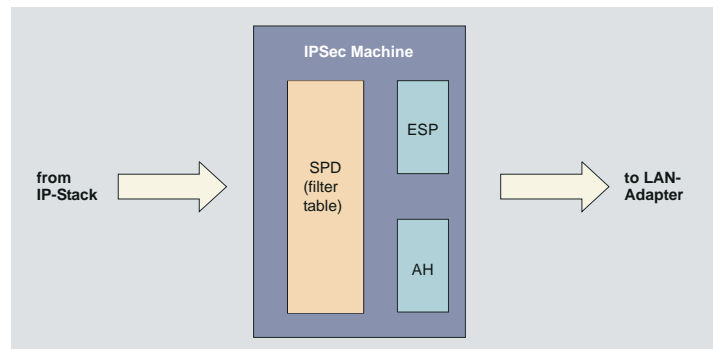
However remote connection of multiple telecommuters to the central corporate network exclusively with IPsec can be assured only with much more difficulty and only with limitations. This is due to the fact that the client must clearly identify himself by his IP address at the VPN gateway. However a client dialing-in to a provider cannot be identified by his IP address as he receives a new one each time he dials in and the destination address that IPsec needs for authentication, (see → graphic above IP1), is no longer available.



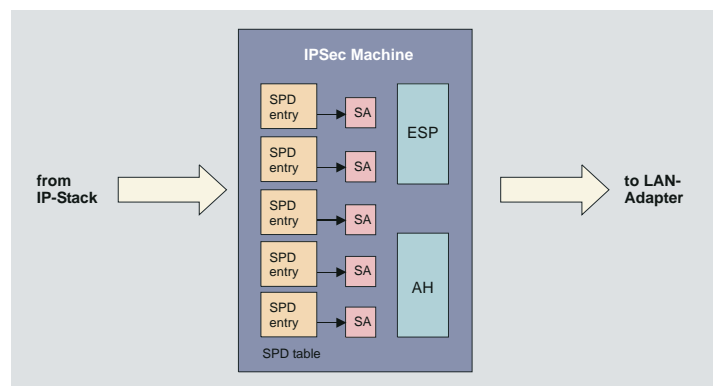
In this case IPsec can only be implemented in Tunnel mode. In addition each remote client must have a private IP address, entered in the Microsoft IP stack, that is known to the destination gateway – and for all remote clients only a single pre-shared key is valid which limits the security for remote access connections.

Secure Policy Database

An essential component of IPsec, or rather of the IPsec machine, is a database that maintains the security policies. This is the Secure Policy Database (SPD) (see graphic below).



The SPD is constructed like a filter table. Each of the SPD entries defines a portion of the IP traffic as well as the security association (SA) points of this traffic (see graphic below).



First three different status conditions of the SPD determine further activity of the IP packets, (see → “Selectors”, “Status”). Due to the fact that packets of defined IP addresses are processed in the IP machine, the SPD status conditions always reference only the addresses or address range specified in the selector:

IPsec: Is used for IP packets with addresses from the defined range; the SPD filter table is implemented.

permit: IP packets with addresses from the defined range are allowed through without implementing the SPD.

deny: All IP packets with addresses from the defined range will be discarded.

disabled: This SPD is turned off and is not implemented for IPsec; it is not necessary to delete it.

Security Association / SA

The Security Association designates a one-way relationship between data sender and data recipient that defines and provides the security services for the exchange of data. Two SA's are necessary for the secure exchange of data in a bidirectional, peer-to-peer connection. The SPD helps by allocating a certain SA to the IP traffic.

The Selectors define each SPD entry; these are a group of IP and upper layer protocol parameters. They filter the outgoing traffic in such a way that it fits a certain SA.

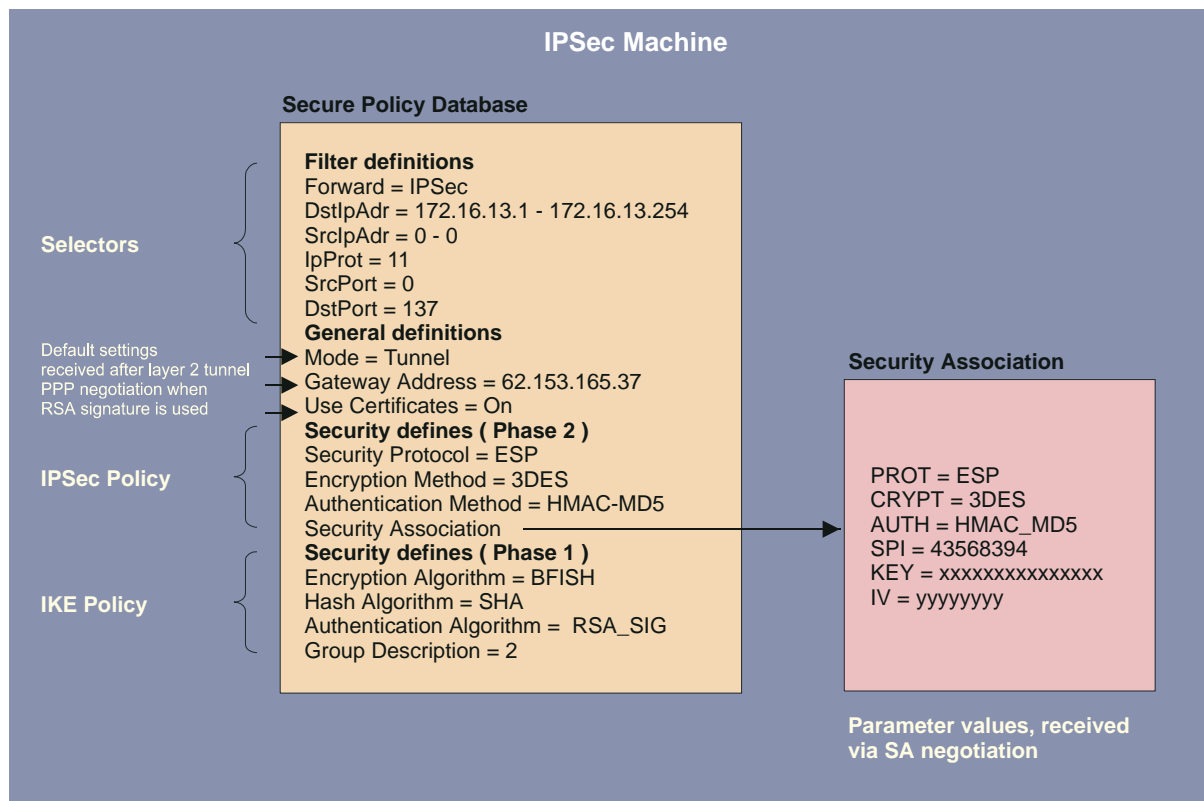
Thus each individual IP packet is examined for the following criteria:

1. Comparison of the IP packet Selector field with the SPD in order to find an entry that references a certain SA.
2. Selection of an appropriate SA according to the Security Parameter Index (SPI)* in the IP packet.
3. Execution of the appropriate IPsec instructions (for example: AH or ESP)

* The SPI is a bit string and will be entered in the AH or ESP header of the IP packet so that the other side can recognize the affiliated SA.

** Der SPI (Security Parameters Index) ist ein Bitstring und wird in den AH- oder ESP-Header des IP-Pakets eingetragen, damit die Gegenstelle die zugehörige SA erkennen kann.

Example of a Secure Policy Database from NCP

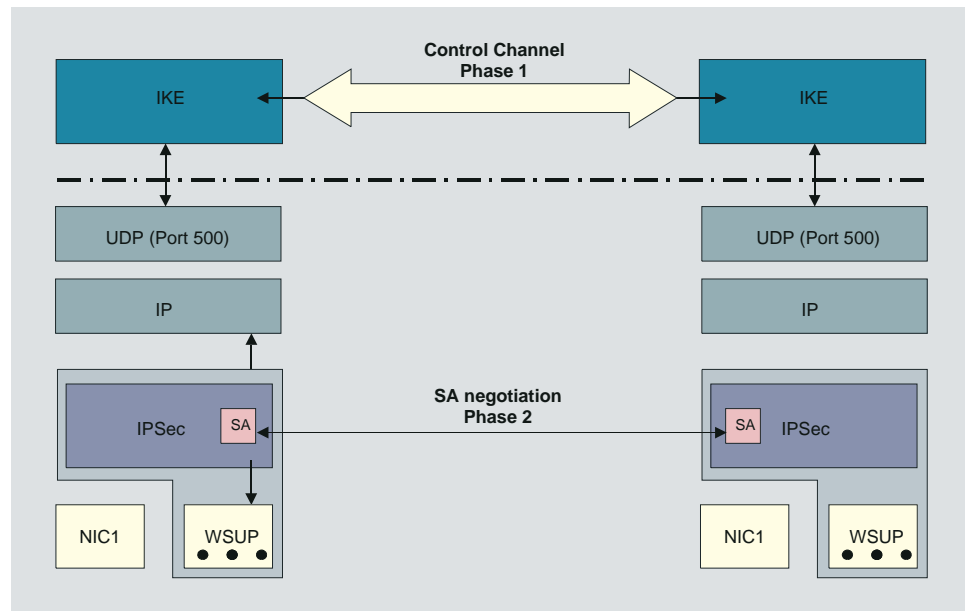


A Secure Policy Database (SPD) checks outgoing frames from the IP stack. The SPD consists of multiple SPD entries that in turn contain a filter portion or Selector. The Selector of an SPD entry is made up mainly of IP addresses, UDP, and TCP ports as well as other IP header-specific entries. If values of an IP frame agree with values from the Selector portion then the SPD entries determine how to proceed with this frame. The frame can simply be permitted, or it can be denied, or certain IPsec process security policies will be applied to it. These security policies are also described in the SPD entry.

If in this manner it is determined that an IP packet is linked with an SPD entry that triggers an IPsec process, then it will be verified whether a security association (SA) already exists for this SPD entry. The SA describes which security protocol should be used either ESP or AH. ESP (Encapsulating Security Payload) supports encryption and authentication of IP frames. AH (Authentication Header) supports only the authentication of IP frames. The SA also specifies in which mode the Security protocol should be used, either Tunnel Mode or Transport Mode. Tunnel mode inserts an IP header, in Transport Mode the original header is used. In addition the SA designates which algorithm will be used for authentication, which encryption method (for ESP) and which key will be applied. The other side of course must work according to the same SA.

SA Negotiation and Policies

In order to initiate the IPsec filter process the SA must first have been negotiated. This SA negotiation takes place once per SPD and can be set for different ports, addresses, and protocols. A Control Channel is required for this SA negotiation.



Phase 1 (IKE Policy)

IPsec establishes the control channel in tunnel mode over the IKE protocol to the IP address of the secure gateway. In Transport mode it is established directly to the IP Address of the other side. (Tunnel- or Transport mode is set under Secure Policy Database, Tunnel).

You define parameters to determine encryption and authentication type over the IKE protocol in the IKE Policies. Thus an authentication can be achieved via a pre-shared key or RSA signature. In the Secure Policy Database these IKE guidelines are referenced under Security.

Phase 2 (IPsec Policy)

The SA negotiation is concluded over the control channel. From the IPsec engine the SA is handed-off to the IKE protocol that it transmits over the control channel to the IPsec engine.

Graphic above: Control Channel and SA Negotiation

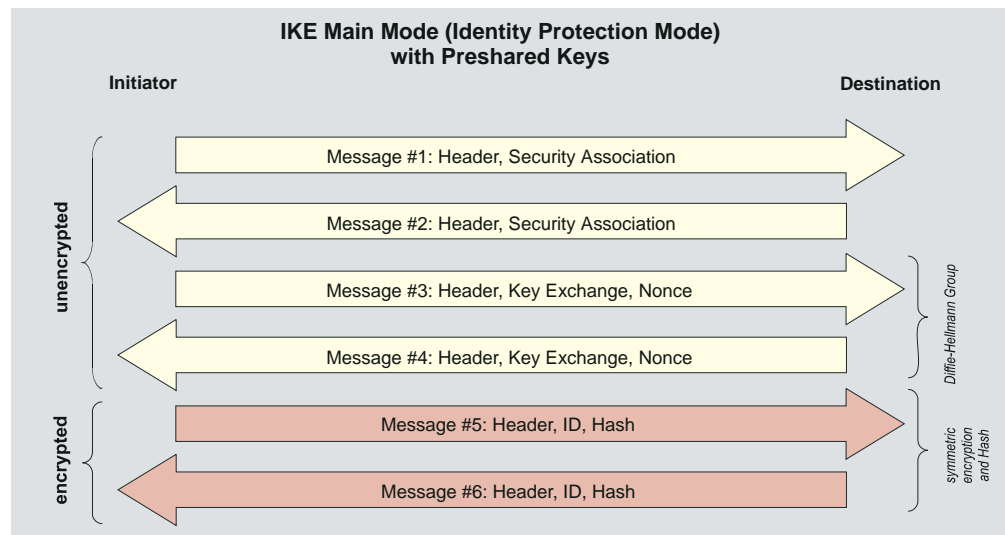
The SA must first have been negotiated in order for the IPsec process to start. This SA negotiation takes place once per SPD (which can be created for different ports, addresses, and protocols). This SA negotiation requires a control channel.

First the client must create a Layer 2 (PPP) link to the provider. With this link the client is assigned a new IP address each time he dials in. The IPsec module in the client receives an IP frame with the destination address of the corporate network. An SPD entry for this IP frame will be found but no SA exists at this time. The IPsec module then issues a request to the IKE module to negotiate an SA. Thus the requested security policies as present in the SPD entry are handed off to the IKE module. Negotiating an IPsec-Security Association (IPsec-SA) is considered a Phase 2 negotiation. However before an IPsec-SA can be negotiated with the other side (Secure Server) a kind of control channel from the client to the Secure Server (VPN) gateway must first exist. This control channel is established via the Phase 1 negotiation whose result is an IKE- Security Association (IKE-SA). Thus the Phase 1 negotiation undertakes the complete authentication of the client relative to the Secure Server and generates an encrypted control channel. Then the Phase 2 negotiation (IPsec-SA) can immediately take place over this control channel. The Phase 1 negotiation is a handshake over which the exchange of certificates is possible and it contains key exchange for the control channel.

IKE Modes

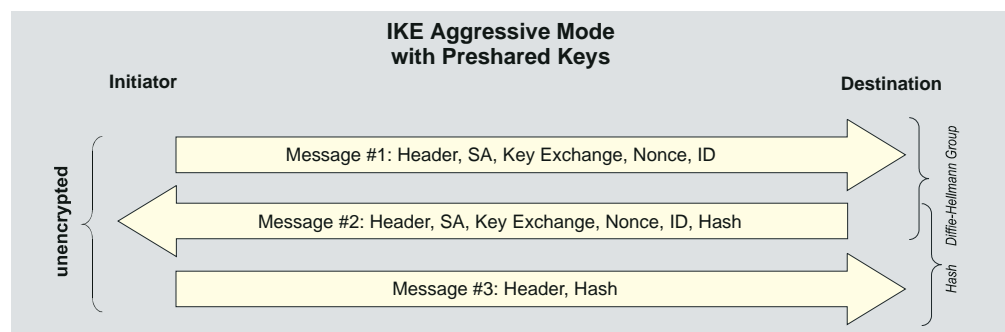
Essentially two types of IKE policies can be configured. They differ according to the type of authentication, which can be either over Pre-shared Key or RSA signature. Each of the two types of Internet Key Exchange can be executed in two different modes. These are; Main Mode also referred to as Identity Protection Mode or Aggressive Mode. These modes are differentiated by the number of messages and by the encryption.

In Main Mode (standard setting) six messages are sent over the Control Channel and the last two messages are encrypted. The last two messages contain the user ID, the signature, the certificate and, if required, a hash value. This is why it is also known as Identity Protection Mode.



One possibility to avoid a general pre-shared key would be to use the Aggressive Mode (see below graphic), however in this case the client ID is not encrypted.

In Aggressive Mode only three messages are sent over the Control Channel and nothing is encrypted.

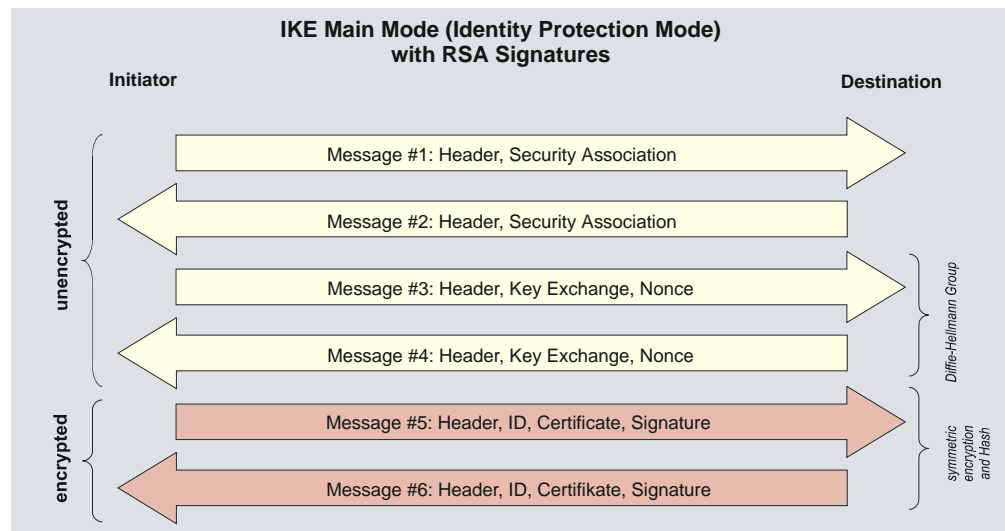


You determine the IKE mode (Exchange Mode), Main Mode or Aggressive Mode in the configuration fields **Security** (Enterprise Client).

If RSA signatures have been set (Graphic above and below), then this means that certificates will be used and thus pre-configuration of all “secrets” is no longer relevant.

Graphics on the right:

IKE Main Mode with RSA Signatures



IKE Aggressive Mode with RSA Signatures



Configuring IPsec Tunneling with NCP Clients

IPsec tunneling conforms to the standard IPsec protocol (native IPsec), which can be used with IPsec gateways of other manufacturers.

A tunnel connection from an Enterprise Client to the gateway can be established via L2TP (layer 2 tunnel) or via IPsec tunneling (layer 3 tunnel) or via both tunnels (IPsec over L2TP).



To establish the tunnel via native IPsec, the VPN protocol “IPsec Tunneling” (Layer 3) has to be selected in the configuration field **VPN Tunneling** of the Enterprise Clients’s profile settings.

The compatibility with other manufactures relies on the ability to conform to the IPsec RFCs and to some drafts (official or not):

- RFC 2104 - Keyed-Hashing for Message Authentication
- RFC 2401 - Security Architecture for the Internet Protocol
- RFC 2403 - The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404 - The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2406 - IP Encapsulating Security Payload (ESP)
- RFC 2407 - The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 - The Internet Key Exchange (IKE)
- DRAFT - draft-beaulieu-ike-xauth-05 (XAUTH)
- DRAFT - draft-dukes-ike-mode-cfg-02 (IKECFG)
- DRAFT - draft-ietf-ipsec-dpd-01 (DPD)
- DRAFT - draft-ietf-ipsec-nat-t-ike-01 (NAT-T)
- DRAFT - draft-ietf-ipsec-nat-t-ike-02 (NAT-T)
- DRAFT - draft-ietf-ipsec-nat-t-ike-03 (NAT-T)
- DRAFT - draft-ietf-ipsec-nat-t-ike-05 (NAT-T)
- DRAFT - draft-ietf-ipsec-udp-encaps-06 (UDP-ENCAP)



Algorithms for Phase 1 and 2

Following algorithms are implemented on the client to support:

Authentication Methods (IKE Policy, Phase 1)

- RSA-Signatur
- PSK (Pre-shared Key)

Symmetric Encryption (Phase 1 & 2)

- DES
- 3DES
- AES-128, AES-192, AES-256

Asymmetric Encryption (Phase 1 & 2)

- DH 1,2,5 (Diffie-Hellman)
- RSA

Hash Algorithms

- MD5
- SHA-1

Additional Phase 2 Support

- PFS (Perfect Forward Secrecy)
- IPsec-Kompression (LZS, Deflate)
- Seamless re-keying

When a profile setting with IPsec tunneling is defined the client falls back to some defaults:

IKE Phase 1 Policy = automatic Mode
 IKE Phase 2 Policy = automatic Mode
 IKE Phase 1 Mode RSA = Main Mode
 IKE Phase 1 Mode PSK = Aggressive Mode

These policies and negotiation modes are set automatically but, alternatively they can be configured manually in **IPsec Configuration**. They can therefore be modified if necessary for other requirements.

Default IKE Proposals

Without entry of a pre-shared keys in the configuration of the client

With the setting “automatic Mode” and the “Pre-shared Key” field left empty, the following proposals for the IKE policy will be sent from the client (IPsec initiator) to the destination by default and a certificate will be used for authentication (refer to “IKE Mode with RSA Signature” above).

The gateway checks the list und looks for the strongest security combination according to its own priority. If no proposal of the client matches to the list of the gateway, the connection will not be established.

List of Proposals for IKE Policy

EA = Encryption Algorithm (Verschlüsselung)
 HASH = Hash Algorithm (Hash)
 AUTH = Authentication Method (Authentisierung)
 GROUP = Diffie-Hellman Group Number (DH-Gruppe)
 LT = Life Type (Dauer)
 LS = Life Seconds (Dauer)
 KL = Key Length (Schlüssellänge)

EA	HASH	AUTH	GROUP	LT	LS	KL
AES_CBC	SHA	XAUTH_RSA	DH5	SECONDS	28800	256
AES_CBC	MD5	XAUTH_RSA	DH5	SECONDS	28800	256
AES_CBC	SHA	RSA	DH5	SECONDS	28800	256
AES_CBC	MD5	RSA	DH5	SECONDS	28800	256
AES_CBC	SHA	XAUTH_RSA	DH2	SECONDS	28800	256
AES_CBC	MD5	XAUTH_RSA	DH2	SECONDS	28800	256
AES_CBC	SHA	RSA	DH2	SECONDS	28800	256
AES_CBC	MD5	RSA	DH2	SECONDS	28800	256
AES_CBC	SHA	XAUTH_RSA	DH5	SECONDS	28800	192
AES_CBC	MD5	XAUTH_RSA	DH5	SECONDS	28800	192
AES_CBC	SHA	RSA	DH5	SECONDS	28800	192
AES_CBC	MD5	RSA	DH5	SECONDS	28800	192
AES_CBC	SHA	XAUTH_RSA	DH5	SECONDS	28800	128
AES_CBC	MD5	XAUTH_RSA	DH5	SECONDS	28800	128
AES_CBC	SHA	RSA	DH5	SECONDS	28800	128
AES_CBC	MD5	RSA	DH5	SECONDS	28800	128
AES_CBC	SHA	XAUTH_RSA	DH2	SECONDS	28800	128
AES_CBC	MD5	XAUTH_RSA	DH2	SECONDS	28800	128
AES_CBC	SHA	RSA	DH2	SECONDS	28800	128
AES_CBC	MD5	RSA	DH2	SECONDS	28800	128
DES3	SHA	XAUTH_RSA	DH5	SECONDS	28800	0
DES3	MD5	XAUTH_RSA	DH5	SECONDS	28800	0
DES3	SHA	RSA	DH5	SECONDS	28800	0
DES3	MD5	RSA	DH5	SECONDS	28800	0
DES3	SHA	XAUTH_RSA	DH2	SECONDS	28800	0

If a specific IKE proposal is entered in the IPsec configuration of the Client profile settings, the same proposal will automatically be generated with Extended Authentication and sent.

With entry of a pre-shared keys in the configuration of the client

Entering a string in the field for “Pre-shared Key” ein String eingetragen, the following proposals for IKE policies will be sent from the client (IPsec initiator) to the destination gateway by default. The authentication will be always without certificate (refer to “IKE Mode with Pre-shared Key” above).

The gateway checks the list und looks for the strongest security combination with pre-shared key according to its own priority. If no proposal of the client matches to the list of the gateway, the connection will not be established.

List of Proposals for IKE Policy

EA	HASH	AUTH	GROUP	LT	LS	KL
AES_CBC	SHA	XAUTH_PSK	DH5	SECONDS	28800	256
AES_CBC	MD5	XAUTH_PSK	DH5	SECONDS	28800	256
AES_CBC	SHA	PSK	DH5	SECONDS	28800	256
AES_CBC	MD5	PSK	DH5	SECONDS	28800	256
AES_CBC	SHA	XAUTH_PSK	DH2	SECONDS	28800	256
AES_CBC	MD5	XAUTH_PSK	DH2	SECONDS	28800	256
AES_CBC	SHA	PSK	DH2	SECONDS	28800	256
AES_CBC	MD5	PSK	DH2	SECONDS	28800	256
AES_CBC	SHA	XAUTH_PSK	DH5	SECONDS	28800	192
AES_CBC	MD5	XAUTH_PSK	DH5	SECONDS	28800	192
AES_CBC	SHA	PSK	DH5	SECONDS	28800	192
AES_CBC	MD5	PSK	DH5	SECONDS	28800	192
AES_CBC	SHA	XAUTH_PSK	DH5	SECONDS	28800	128
AES_CBC	MD5	XAUTH_PSK	DH5	SECONDS	28800	128
AES_CBC	SHA	PSK	DH5	SECONDS	28800	128
AES_CBC	MD5	PSK	DH5	SECONDS	28800	128
AES_CBC	SHA	XAUTH_PSK	DH2	SECONDS	28800	128
AES_CBC	MD5	XAUTH_PSK	DH2	SECONDS	28800	128
AES_CBC	SHA	PSK	DH2	SECONDS	28800	128
AES_CBC	MD5	PSK	DH2	SECONDS	28800	128
DES3	SHA	XAUTH_PSK	DH5	SECONDS	28800	0
DES3	MD5	XAUTH_PSK	DH5	SECONDS	28800	0
DES3	SHA	PSK	DH5	SECONDS	28800	0
DES3	MD5	PSK	DH5	SECONDS	28800	0
DES3	SHA	XAUTH_PSK	DH2	SECONDS	28800	0
DES3	MD5	XAUTH_PSK	DH2	SECONDS	28800	0
DES3	SHA	PSK	DH2	SECONDS	28800	0
DES3	MD5	PSK	DH2	SECONDS	28800	0

Default IPsec Proposals

In phase 2 the client sends by default the following list of proposals to negotiate the IPsec policy. One entry of this list must match to a proposal of the remote side.

The gateway checks the list und looks for the strongest security combination according to its own priority. If no proposal of the client matches to the list of the gateway, the connection will not be established.

List of Proposals for IPsec Policy

```
PROTO - Protocol (Protokoll)
TRANS - Transform (Transformation (ESP))
LT      - Life Type (Dauer)
LS      - Life Seconds (Dauer)
KL      - Key Length (Schlüssellänge)
COMP    - IP Compression (Transformation (Comp))
```

PROTO	TRANS	AUTH	LT	LS	KL	COMP	LZS
ESP	AES	MD5	SECONDS	28800	128	Yes	Yes
ESP	AES	SHA	SECONDS	28800	128	Yes	Yes
ESP	AES	MD5	SECONDS	28800	128	No	No
ESP	AES	SHA	SECONDS	28800	128	No	No
ESP	AES	MD5	SECONDS	28800	192	Yes	Yes
ESP	AES	SHA	SECONDS	28800	192	Yes	Yes
ESP	AES	MD5	SECONDS	28800	192	No	No
ESP	AES	SHA	SECONDS	28800	192	No	No
ESP	AES	MD5	SECONDS	28800	256	Yes	Yes
ESP	AES	SHA	SECONDS	28800	256	Yes	Yes
ESP	AES	MD5	SECONDS	28800	256	No	No
ESP	AES	SHA	SECONDS	28800	256	No	No
ESP	DES3	MD5	SECONDS	28800	0	Yes	Yes
ESP	DES3	MD5	SECONDS	28800	0	No	No

IPsec Tunneling Parameters



In the following section you will find the most important settings of the IPsec configuration. Click on the terms depicted in bold red font, and you will navigate directly to the relevant section in the document Secure Client Parameters.

IPsec Tunneling

In the profile settings of the Enterprise Client the VPN protocol IPsec Tunneling has to be selected in the configuration field **VPN Tunneling**. With this protocol the native IPsec connection without layer 2 tunnel (L2TP) will be established.

By creating an IPsec profile under **VPN Tunneling** on the Enterprise Client) following settings will be done automatically:

IKE Policy = automatic Mode
IPsec Policy = automatic Mode

(Using this setting the IPsec gateway looks for the matching policy, how described above).

Exchange Mode

Default setting is Main Mode. If you want to modify this setting you should enter into an agreement with your system administrator. (Under **Security**)

IKE ID Type and IKE ID

This parameter is located under **Security**. It can only be set correctly in coordination with your system administrator.

Pre-shared Key or RSA Signature

According to the requirement of the remote gateway the “automatic mode” of the IKE policy can be set either to “Pre-shared Key” or “RSA Signature” (Certificate).

If the gateway requires “Pre-shared Key”, the key has to entered into the field. It has to agree with the pre-shared key of this user on the gateway.

In the same manner you can modify the IPsec policy by coordinating with the requirements of the central gateway. This can be done under **Security**.

To modify details of the policies you have to enter into an agreement with your system administrator.

The details can be configured in the **IPsec Configuration** of the client.

IP Addresses and DNS Server

IP addresses and DNS server are assigned to the Enterprise Client by default with the protocol IKE Config Mode (Draft 2, actually compatible only with Cisco).

In coordination with your system administrator these settings can be modified under **IPsec Address Assignment**.

For the NAS dial-up all regular WAN interfaces can be used.

Authentication

Using the XAUTH protocol (Draft 6) for authentication (default for the Enterprise Client) the following parameter have to be configured:

on the Enterprise Client under **VPN Tunneling**

- VPN User ID
- VPN Password
- Access Data from Certificate ...
(optionally when using Certificates)

The manner of authentication is designated by the gateway.

DPD und NAT-T

DPD (Dead Peer Detection) and NAT-T (NAT Traversal) are automatically executed in the background for “IPsec Tunneling” when supported by the destination. The IPsec client uses DPD to check, in regular intervals, whether the other side is still active. If the other side is inactive, then an automatic connection-disconnect occurs. DPD can be deactivated in the configuration filed **Advanced IPsec Options**.

Using NAT Traversal is automatic with the IPsec client and is always necessary if network address translation is used on the side of the destination system device.

PFS / DH-Gruppe

On the Enterprise Client the Diffie Hellman group can be selected for the code exchange (Perfect For-

ward Secrecy) per IPsec policy suggestion in the **IPsec Configuration**.

The standard setting is “none”. If you want to modify this setting you should enter into an agreement with your system administrator.

IPsec Compression

The Enterprise Client supports the Compression via LZS and deflate.

You differ the compression for each IPsec policy in the **IPsec Configuration**.

The remote station specifies which IPsec compression is used. When the compression is activated at the client and the gateway does not support compression no connection will be established.

IPsec for Remote Access – IPsec over L2TP

How then indeed can IPsec be used with unlimited functionality for remote access without giving rise to security loopholes? Or how can the principle of IP address orientation be maintained in spite of changing IP addresses without having to deal with the limitations described above?



On the next page you will find a functional description.

As specified in RFC 2888 and as recommended by different IPsec experts, this can be achieved by first establishing a Layer 2 Tunnel over the Internet between the remote access client and the central system so that the ensuing IPsec negotiation already occurs in a tunneled manner in a VPN (Virtual Private Network).

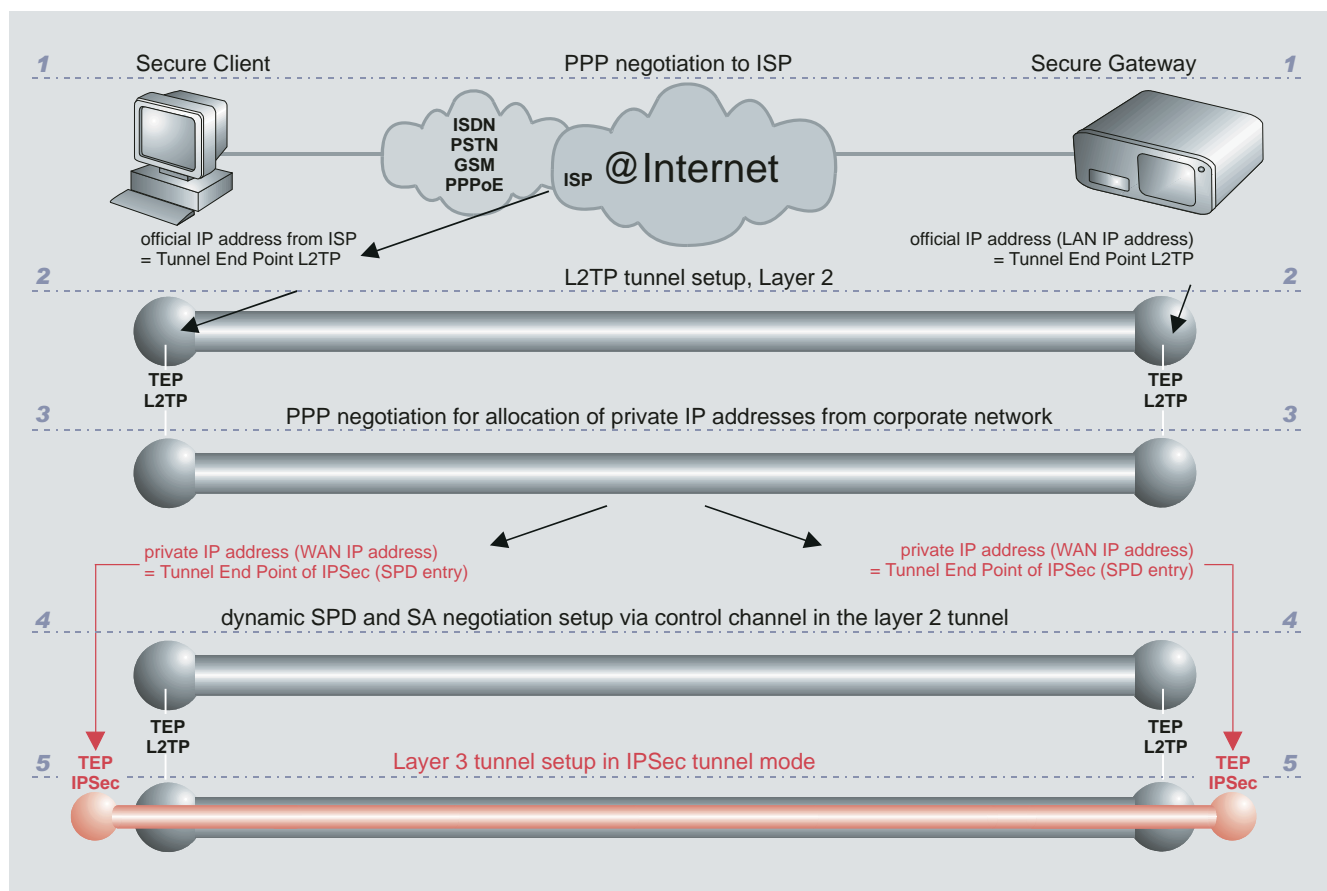
Establishment of the Tunnel is insured through user-oriented authentication (Layer 2). Afterwards an IP address can be assigned from the corporate network that can be used for the following IPsec process.



All the disadvantages of IPsec in remote access environments are eliminated with IPsec over L2TP. (It can be configured on the Enterprise Client with the **VPN Protocol L2TP** and the **Security Mode IPsec**). Any decent router that supports IP network address translation can be linked. In addition it is possible to use the supplemental security mechanisms of a public key infrastructure over standard interfaces. In order to assure the security of IPsec over L2TP over entire segments NCP recommends that the Secure Gateway be installed in the DMZ behind the Access Server and the firewall. Thus all parameters of secure data transmission are under the control of the enterprise:

- ☒ Endpoints of the Layer 2 tunnel (secure gateway, remote client)
- ☒ Tunneling protocol
- ☒ Key algorithm
- ☒ Network protocol
- ☒ Data compression
- ☒ Transmission medium
- ☒ IP address from the corporate network
- ☒ IPsec parameters

IPsec over L2TP with dynamic SPD



1. Standard User/Password (User ID) and authentication PPP negotiations relative to the Internet service provider (ISP) in which the client receives an official IP address from the ISP. Afterwards the client establishes a connection to the secure server over the Internet. The parameters required for this are located in the client Phonebook under "Destination System" and "Network Dial-in". The "Tunnel IP Address (Source)" entered in the "Phonebook" under "Tunnel Parameters" corresponds to the official IP address of the secure server.

2. After checking the "Tunnelsecret" the tunnel parameters are negotiated and the L2TP Tunnel is established in Layer 2. Tunnel end points are the official IP address that the client received from the ISP and the official IP address of the secure server that is entered in the client's Phonebook as "Tunnel IP Address (destination)".(*1)(*2)

3. After a further PPP negotiation and user and password check the private IP address from the corporate network is allocated. These addresses can originate from a pool. The remote client is thus clearly identifiable based on its IP address independent of its location.

4. The SA negotiation takes place over the Control Channel in Layer 2 Tunnels. The strong authentication occurs according to the IKE Policy that has been determined for this link profile (Profile Settings: Security).

5. The Layer 3 Tunnel is established according to the default of the IPsec operating mode. Tunnel end points are the IP addresses from the corporate network.

(1* According to IETF the tunnel end must always be in the protected private area of the VPN operator, behind the firewall in the DMZ.

(2* For L2SEC this is where the SSL negotiations are located.