NCP
SECURE COMMUNICATIONS

Funktionsbeschreibung und Konfiguration

high security remote access

Enterprise Client IPsec-Funktionalität

Copyright

Network
Communications
Products engineering GmbH

Dombühler Str.2
D-90449 Nürnberg
Tel.: 0911 / 99 68-0
Fax: 0911 / 99 68-299
internet http:// www.ncp-e.com
E-mail: info@ncp-e.com

IPsec-Funktionalität und Konfiguration

Im ersten Teil dieses Dokuments ist zunächst in allgemeiner Form die Funktionalität von IPsec skizziert, wobei Besonderheiten von NCP in ekkigen Klammern angemerkt sind.

Im zweiten Teil wird die Konfiguration von IPsec Tunneling mit NCP Clients behandelt.

IPsec-Funktionalität

IPSec ist ein Standard mit ausgezeichneten Sicherheitsmechanismen, der in VPN-Szenarien funktioniert, in denen mit festen IP-Adressen gearbeitet wird (z. B. B2B, Extranet). In diesen Fällen lassen sich auch VPN Gateways verschiedener Hersteller einsetzen. Hier sind feine, bis auf Port-Ebene reichende Sicherheitseinstellungen möglich. Allerdings kann IPsec nur für IP-Datenverkehr eingesetzt werden.

Die IPsec-Spezifikation umfasst nicht nur das (Layer 3-) Tunneling, sondern auch alle notwendigen Sicherheitsmechanismen, wie starke Authentisierung (XAUTH), Schlüsselaustausch und Verschlüsselung.

Mit den IPsec RFCs (2401 - 2409) lässt sich ein VPN mit vorgegebener Security für IP realisieren. Tunneling und Security sind für IPsec vollständig beschrieben, so dass ein komplettes Rahmenwerk für das VPN zur Verfügung steht. Prinzipiell ist es möglich, herstellerunabhängige veschiedene Komponenten zu nutzen. In Site to Site VPNs etwa könnten die VPN Gateways von veschiedenen Herstellern stammen, in End to Site VPNs könnten die Clients von einem anderen Hersteller als die Gateways sein. Der Verbindungsaufbau zum IPsec-Verkehr erfolgt auf Basis des Internet Key Exchange-Protokolls (IKE).

Der IPsec-Prozess

In jedem IP-Host (Client oder Gateway) der IPsec unterstüzt, gibt es ein IPsec-Modul, bzw. eine IPsec-Maschine. Dieses Modul untersucht jedes IP-Paket nach bestimmten Eigenschaften, um die jeweils entsprechende Security-Behandlung darauf anzuwenden.

Die Prüfung der vom IP Stack ausgehenden IP-Pakete erfolgt bezüglich einer Secure Policy Database (SPD). [NCP Clients und Gateways bauen die SPD intern dynamisch auf].

Die SPD besteht aus mehreren Einträgen (SPD Entries), die wiederum einen Filterteil beinhalten. Der Filterteil oder Selektor eines SPD-Eintrags besteht hauptsächlich aus IP-Adressen, UDP und TCP Ports sowie anderer IP Header-spezifischer Einträge. Wenn Werte eines IP-Pakets mit Werten aus dem Selektorteil des SPD-Eintrags übereinstimmen, wird aus den SPD-Einträgen weiter ermittelt, wie mit diesem IP-Paket zu verfahren ist. Das Paket kann einfach durchgelassen werden (permit), es kann abgelehnt bzw. weggeworfen werden (deny) oder bestimmte Security-Richtlinien des IPsec-Prozesses kommen an ihm zur Anwendung. Diese Security-Richtlinien stehen auch im SPD-Eintrag beschrieben.

Wird auf diese Weise festgestellt, dass ein IP-Paket mit einem SPD-Eintrag verknüpft ist, der einen IPsec-Prozess einleitet, so wird überprüft, ob bereits eine Sicherheits-Verknüpfung (Security Association, SA) für diesen SPD-Eintrag existiert. Existiert noch keine SA, wird vor dem Aushandeln einer SA zunächst eine Authentisierung und ein Schlüsselaustausch (siehe unten → SA-Verhandlung / Phase 1) vorgenommen.

Nach der SA-Verhandlung erfolgen in einem weiteren Schritt (siehe unten → SA-Verhandlung / Phase 2) die Verhandlungen für eine Verschlüsselung (ESP) und/oder Authentisierung (AH) der Datenpakete und ob im Tunnel- oder Transportmodus übertragen werden soll. [Aufgrund höherer Sicherheit lässt NCP nur den Tunnelmodus mit ESP zu.]

Die Implementierung von IPsec

Die SA beschreibt, welches Sicherheitsprotokoll verwendet werden soll (ESP oder AH). ESP (Encapsulating Security Payload) unterstützt die Verschlüsselung und die Authentisierung von IP-Paketen, AH (Authentication Header) unterstüzt nur die Authentisierung von IP-Paketen. Die SA beschreibt auch, in welcher Betriebsart das Sicherheitsprotokoll benutzt werden soll (Tunnel- oder Transportmodus). Im Tunnelmodus wird ein IP Header hinzugefügt, im Transportmodus wird der Original-Header verwendet. Weiter beschreibt die SA, welcher Algorithmus zur Authentisierung verwendet werden soll, welche Verschlüsselungsmethode (bei ESP) und welcher Schlüssel zur Anwendungen kommen sollen. Die Gegenstelle muss selbstverständlich nach der gleichen SA arbeiten.

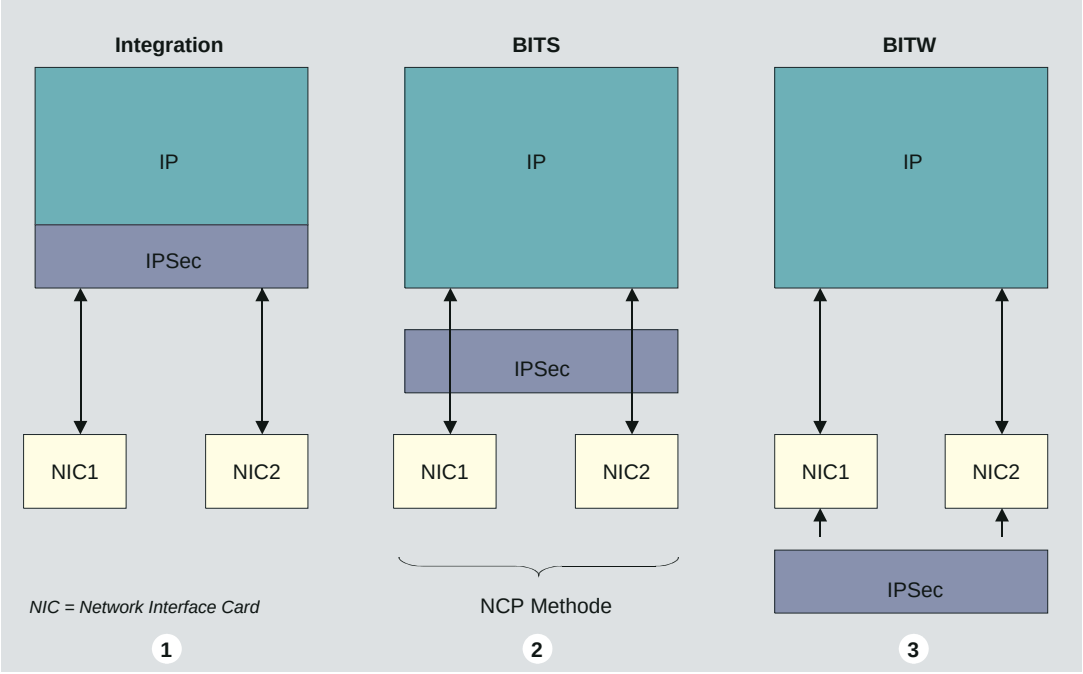
Ist die SA ausgehandelt, wird jedes Datenpaket gemäß Betriebsmodus (Tunnel oder Transport) und Protokoll (ESP oder AH) bearbeitet.

Die Implementierung von IPsec kann auf drei verschiedene Arten erfolgen (Abb. unten):

1. Intergration: Dabei wird IPsec vollständig in den IP Stack integriert. Dies ist jedoch nur möglich, wenn der IP Stack vom gleichen Hersteller entwikkelt wird wie IPsec.

2. BITS (Bump in the Stack): In diesem Fall wird IPsec durch zusätzliche Treiber zwischen Layer 2 und dem Netzwerkadapter implementiert. Dies ist die am weitesten verbreitete und auch von NCP angewendete Methode. Dabei stellt sich das IPsec-Modul von NCP als ein LAN-Adapter und Intermediate-Treiber für IPsec und Tunneling dar. Die IPsec-Implementierung von NCP ist RFC-konform und vollständig kompatibel zu Drittherstellern.

3. BITW (Bump in the Wire): Hierbei wird IPsec in die Hardware integriert.



IPsec-Dienste

IPsec bietet durch die Wahlmöglichkeit alternativer Sicherheitsprotokolle und Verschlüsselungsalgorithmen verschiedene Sicherheitsdienste. Bei den Sicherheitsprotokollen handelt es sich um ein Authentisierungsprotokoll, festgelegt durch den Header (Authentisierungs-Header / AH), und ein kombiniertes Verschlüsselungs- und Authentisierungsprotokoll, festgelegt durch das Format (Encapsulating Security Payload / ESP). Folgende Sicherheitsdienste werden durch IPsec bereitgestellt:

– Zugriffskontrolle (Access Control)
– Integrität (Integrity, ESP)
– Authentisierung der Datenherkunft (Data origin Authentication, ESP)
– Vertraulichkeit (Confidentiality, ESP)

IPsec-Richtlinie

Die IPsec-Richtlinie legt fest:

– wie mit ESP verschlüsselt oder mit AH der Hash-Wert zur Authentisierung gebildet werden soll (Transform / Authentisierung)

– ob zusätzlich in Phase 2 mit der SA-Verhandlung ein kompletter Schlüsselaustausch (PFS) nach Diffie-Hellman (DH-Gruppe) stattfinden soll

– nach welchen Kriterien die Dauer der Schlüsselgültigkeit bemessen wird (Dauer / KBytes)

– welches der beiden Sicherheitsprotokolle verwendet wird, AH oder ESP.

[In der IPsec-Konfiguration des Clients ist eine IPsec-Richtline mit ESP abgelegt. Der Einsatz des AH-Transportprotokolls ist von NCP nicht vorgesehen. In der Beschreibung **Secure Client Parameter** wird in den Konfigurationsfeldern **Security** und **IPsec-Einstellungen** darauf hingewiesen.]

AH und ESP im Transport- und Tunnelmodus

Beachten Sie zur folgenden Beschreibung die Abbildung auf der nächsten Seite.

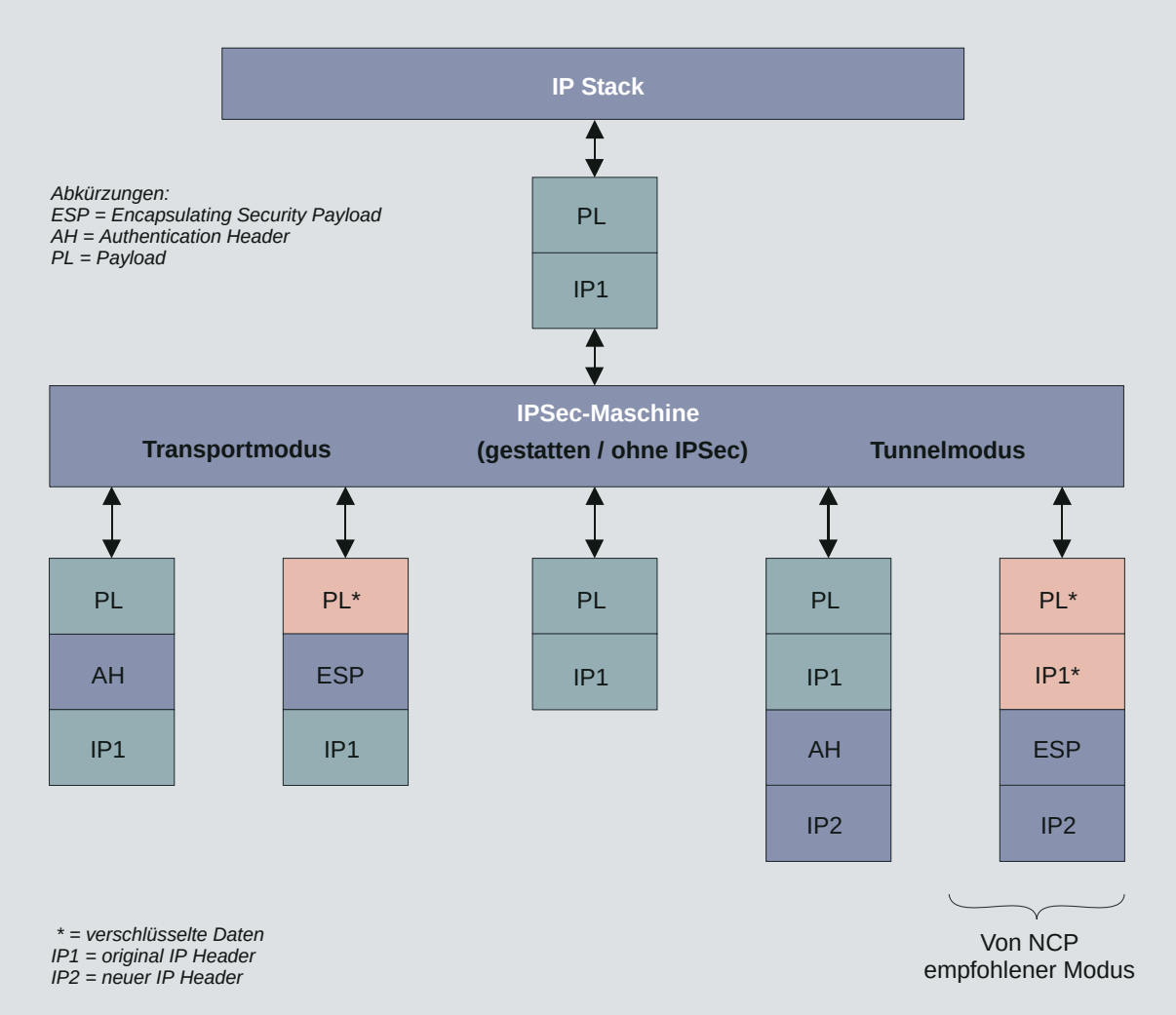
Beide IPsec-Sicherheitsprotokolle (AH und ESP) unterstützen zwei verschiedene Betriebsarten, den Transport- und den Tunnelmodus.

AH im Transportmodus authentifiziert die Nutzdaten des IP-Pakets (Payload) und ausgewählte Teile des IP Headers (IP1). ESP im Transportmodus verschlüsselt (und authentifiziert) die Nutzdaten (Payload) des IP-Pakets, nicht aber den IP Header (IP1). Im Transportmodus werden Ziel- und Quelladressen mit dem IP Header unverschlüsselt übertragen – Quell- und Zieladresse bleiben ungeschützt. Der Transportmodus eignet sich daher nur für eine direkte Kommunikation zwischen zwei Hosts mit festen IP-Adressen oder zwischen Arbeitsplatzrechnern im LAN. Außerdem wird er für L2TP over IPsec eingesetzt. [L2TP over IPsec kann auf NCP-Produkten nicht konfiguriert werden.] Der AH-Transportmodus ist für flexiblen Remote Access ungeeignet.

Im Tunnelmodus wird das gesamte IP-Paket, einschließlich des hinzugefügten AH- oder ESP-Feldes, eingekapselt und mit einem neuen IP Header (IP2) versehen. Das IP-Paket wird auf diese Weise durch einen Layer 3-Tunnel geschickt. Der innere IP Header mit Original-Adressen ist dabei versteckt und kann nicht eingesehen werden – nur die (Layer 3-) Tunnelendpunkte sind erkennbar. Rechner in Netzen hinter Firewalls oder Routern mit IPsec können in diesem Modus sicher miteinander kommunizieren. Der neue IP Header (IP2) kann völlig andere Quell- und Zieladressen beinhalten als der Original-Header aber er muss Informationen für die Gegenstelle bereithalten, die nötig sind, um das eingekapselte IP-Paket nach den Richtlinien der Sicherheitsverknüpfung (SA) anzunehmen und weiterzuleiten. [Dieser Modus ist für NCP-Produkte die Standard-Einstellung.)

Welches IPsec-Sicherheitsprotokoll mit welchem Verschlüsselungsalgorithmus und welcher Art der Authentisierung kombiniert wird, wird in den IPsec-Richtilinien (IPsec Policy) festgelegt. In der Secure Policy Database (SPD) wird auf diese IPsec-Richtlinie, d. h. das Sicherheitsprotokoll, wie auch auf den Betriebsmodus, d. h. Tunnel- oder Transportmodus, verwiesen.

Funktion der IPsec-Maschine



Die Abbildung (oben) zeigt wie ein IP-Datenpaket vom IP Stack zum IPsec-Modul gesendet wird. Der originale IP Header (IP1) mit seinem Payload (PL-Nutzdaten) wird bearbeitet. Der untere Teil des Bildes zeigt das Ergebnis des IPsec Prozesses.

Der Transportmodus ist nur für Host-zu-Host Kommunikation geeignet, der Tunnelmodus dagegen ermöglicht auch den Betrieb über ein VPN Gateway. Mit dem IP2 Header ist der Transfer von einem Client über das Internet zu einem Gateway möglich. Das VPN Gateway entfernt den IP2 Header, entschlüsselt und sendet das Paket weiter ins lokale LAN. [Für Remote Access und End to Site VPN setzt NCP generell nur den ESP-Tunnelmodus ein.]

Anwendungen

In beiden Betriebsmodi von IPsec erfolgen Authentisierung und Verschlüsselung IP-Adressen-orientiert (auf Layer 3). Daher kommt IPsec insbesondere dann zum Einsatz, wenn beide Kommunikationsendpunkte durch offizielle IP-Adressen gekennzeichnet sind, bzw. die Verbindung vordefiniert ist:

So lässt sich mit IPsec eine sichere Kommunikation zwischen Zweigstellen eines Unternehmens herstellen. Die Sicherheit dieser LAN-LAN-Kommunikation über ein öffentliches Netz kann auch ohne gemietete Standleitung gewährleistet werden. Ein Unternehmen kann zu diesem Zweck das Internet nutzen. Voraussetzung ist, dass eine Firewall oder ein Router mit IPsec-Funktionalität am Einwahlpunkt des jeweiligen LANs über eine feste offizielle IP-Adresse verfügt.

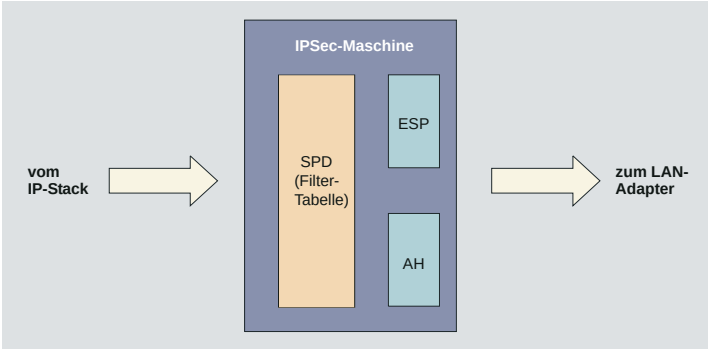
Ebenso lassen sich mit IPsec Extranet- und Internet-Verbindungen zu Partnern schützen, indem Authentisierung und Vertraulichkeit sichergestellt werden und ein Mechanismus für den Austausch von Schlüsseln festgelegt wird.

Weitaus schwieriger und nur mit Einschränkungen lassen sich Remote-Anbindungen mehrerer Telearbeiter an das zentrale Firmennetz ausschließlich mit IPsec sichern. Dies liegt daran, dass sich der Client am VPN Gateway durch seine IP-Adresse eindeutig identifizieren muss. Ein Client, der sich beim Provider einwählt, ist jedoch nicht durch die IP-Adresse zu erkennen, da er bei jeder Provider-Anwahl eine neue zugewiesen bekommt. Die IP-Adresse, die IPsec zur Authentisierung benötigt (in der vorigen Abb. IP1), steht nicht mehr zur Verfügung.

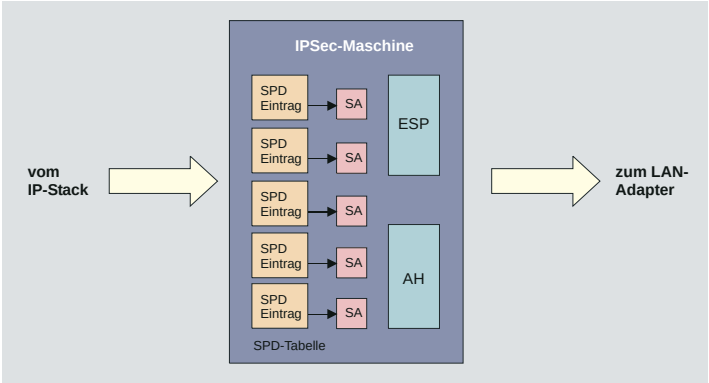
IPsec kann in dem letzten Fall nur mit ESP im Tunnelmodus zum Einsatz kommen. Zudem muss jeder Remote Client über eine eigene private IP-Adresse (eingetragen im Microsoft IP Stack) verfügen, die dem Ziel-Gateway bekannt ist – und für alle Remote Clients muss ein einziger Pre-shared Key gelten, was die Sicherheit für Remote Access-Anbindungen allerdings einschränkt.

Secure Policy Database

Ein wesentlicher Bestandteil von IPsec, bzw. der IPsec-Maschine, ist eine Datenbank, in der die Sicherheits-Richtlinien festgehalten sind, die Secure Policy Database (SPD). Siehe Abbildung unten.



Jeder der Einträge der SPD, die wie eine Filtertabelle aufgebaut ist, definiert einen Teil des IP-Verkehrs, sowie die Punkte einer Security Association (SA) dieses Verkehrs. Siehe Abbildung unten.



Zunächst entscheiden drei verschiedene Stati der SPD über den weiteren Umgang mit den IP-Paketen. Da in der IPsec-Maschine immer die Pakete definierter IP-Adressen bearbeitet werden, beziehen sich die Stati der SPD immer auch nur auf die in den Selektoren angegebenen Adressen oder Adressbereiche:

IPsec: Für die IP-Pakete mit Adressen aus dem definierten Bereich werden die IPsec-Sicherheitsdienste angewendet, die SPD-Filtertabelle kommt zum Einsatz.

gestatten (permit): Die IP-Pakete mit Adressen aus dem definierten Bereich werden durchgelassen, ohne dass die SPD zum Einsatz kommt.

sperren (deny): Alle IP-Pakete mit Adressen aus dem definierten Bereich werden weggeworfen.

inaktiv (disabled): Diese SPD wird ausgeschaltet und kommt für IPsec nicht zum Einsatz, ohne dass sie gelöscht werden muss.

Sicherheits-Verknüpfung (Security Association / SA)

Die Security Association bezeichnet eine Einwegbeziehung zwischen Sender und Empfänger von Daten, die die Sicherheitsdienste für den Datenaustausch definiert (und bereitstellt). Für sicheren Datenaustausch in einer bidirektionalen Peer-to-Peer-Verbindung sind zwei SAs erforderlich. Mit Hilfe der SPD wird dem IP-Verkehr eine bestimmte Sicherheitsverknüpfung (SA) zugeordnet. (Vergleiche Abbildung und Bildbeschreibung auf der folgenden Seite.)

Jeder SPD-Eintrag wird durch eine Gruppe von IP- und Oberschichtprotokoll-Parametern definiert, den Selektoren*. Mit ihnen wird der ausgehende Verkehr so gefiltert, dass er zu einer bestimmten SA passt.

Dabei wird jedes einzelne IP-Paket nach folgenden Kriterien untersucht:

1. Vergleiche die Selektorenfelder des IP-Pakets mit der SPD, um einen Eintrag zu finden, der auf eine SA verweist

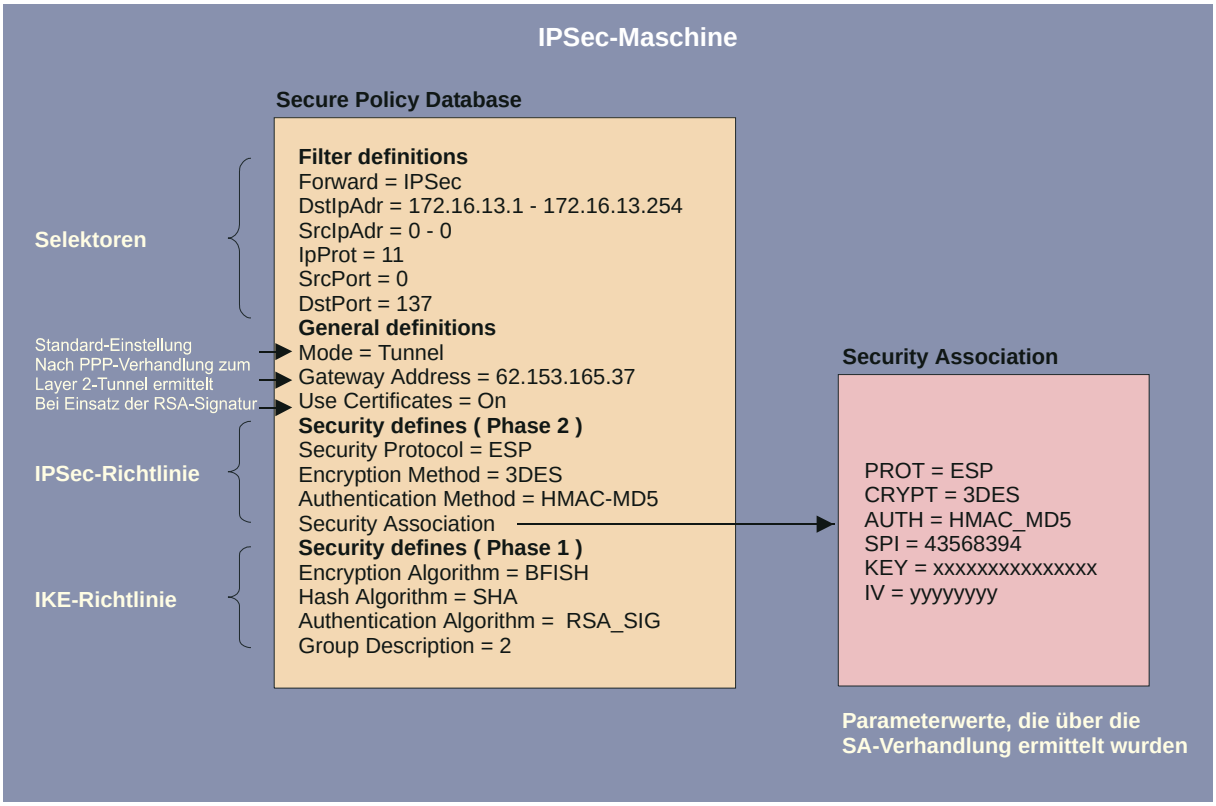
2. Selektiere eine passende SA nach dem Security Parameter Index (SPI)** im IP-Paket

3. Führe die entsprechenden IPsec-Anweisungen aus (z.B. AH oder ESP)

* Der Selektor oder Filterteil eines SPD-Eintrags besteht hauptsächlich aus IP-Adressen, UDP und TCP Ports sowie anderer IP Header-spezifischer Einträge. Wenn Werte eines IP-Pakets mit Werten aus dem Selektorteil des SPD-Eintrags übereinstimmen, wird aus den SPD-Einträgen weiter ermittelt, wie mit diesem IP-Paket zu verfahren ist.

** 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.

Beispiel einer Secure Policy Database von NCP



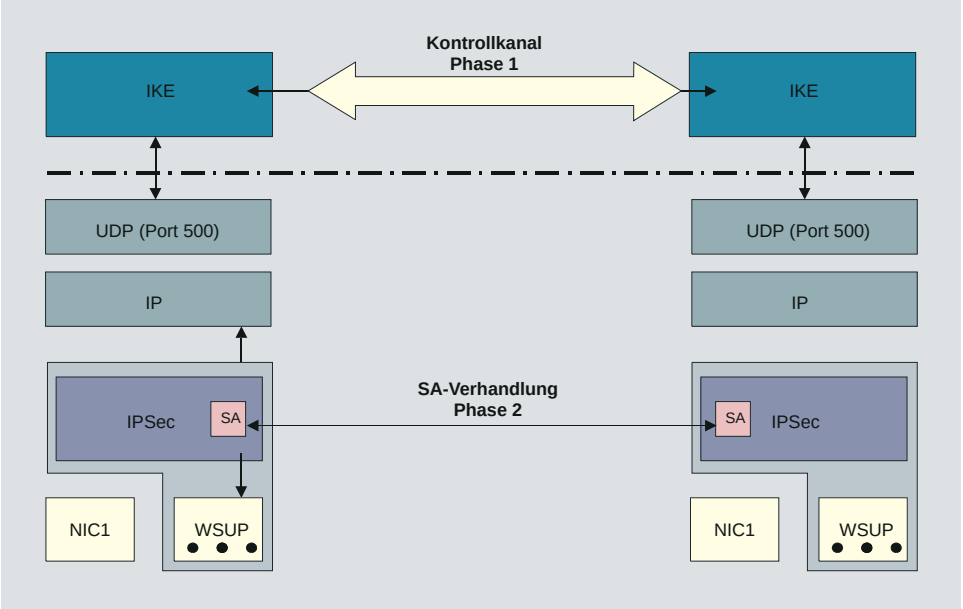
Die Prüfung der vom IP Stack ausgehenden IP-Pakete erfolgt bezüglich einer Secure Policy Database (SPD). Die SPD besteht aus mehreren Einträgen (SPD Entries), die wiederum einen Filterteil beinhalten. Der Filterteil oder Selektor eines SPD-Eintrags besteht hauptsächlich aus IP-Adressen, UDP und TCP Ports sowie anderen IP Header-spezifischen Einträgen. Wenn Werte eines IP-Pakets mit Werten aus dem Selektorteil des SPD-Eintrags übereinstimmen, wird aus den SPD-Einträgen weiter ermittelt, wie mit diesem IP-Paket zu verfahren ist. Das Paket kann einfach durchgelassen werden (permit), es kann abgelehnt bzw. weggeworfen werden (deny) oder bestimmte Security-Richtlinien des IPsec-Prozesses kommen an ihm zur Anwendung (IPsec). Diese Security-Richtlinien stehen auch im SPD-Eintrag beschrieben.

Wird auf diese Weise festgestellt, dass ein IP-Paket mit einem SPD-Eintrag verknüpft ist, der einen IPsec-Prozess einleitet, so wird überprüft, ob bereits eine Sicherheits-Verhandlung (Security Association, SA) für diesen SPD-Eintrag existiert. Die SA beschreibt, welches Sicherheitsprotokoll verwendet werden soll (ESP oder AH). ESP, Encapsulating Security Payload, unterstützt die Verschlüsselung und die Authentisierung von IP-Paketen, AH, Authentication Header, unterstüzt nur die Authentisierung von IP-Paketen. Die SA beschreibt auch, in welcher Betriebsart das Sicherheitsprotokoll benutzt werden soll (Tunnel- oder Transportmodus).

Im Tunnelmodus wird ein IP Header hinzugefügt, im Transportmodus wird der Original-Header verwendet. Weiter beschreibt die SA, welcher Algorithmus zur Authentisierung verwendet werden soll, welche Verschlüsselungsmethode (bei ESP) und welcher Schlüssel zur Anwendungen kommen sollen. Die Gegenstelle muss selbstverständlich nach der gleichen SA arbeiten.

SA-Verhandlung und Richtlinien / Policies

Damit der IPsec-(Filter-) Prozess in Gang kommen kann, muss vorher die SA verhandelt worden sein. Diese SA-Verhandlung (Bild links) findet pro SPD statt – die für verschiedene Ports, Adressen und Protokolle angelegt sein können. Für diese SA-Verhandlung wird ein Kontrollkanal benötigt.



Phase 1 (Parameter der IKE-Richtlinie)

Der Kontrollkanal wird im Tunnelmodus von IPsec über das IKE-Protokoll zur IP-Adresse des Secure Gateways aufgebaut, im Transportmodus direkt zur IP-Adresse der Gegenstelle.

Parameter zur Festlegung von Verschlüsselungs- und Authentisierungsart über das IKE-Protokoll definieren Sie in den IKE-Richtlinien. Dabei kann die Authentisierung über einen Pre-shared Key oder eine RSA-Signatur erfolgen. (In der Secure Policy Database wird unter Security auf diese IKE-Richtlinie verwiesen.)

Phase 2 (Parameter der IPsec-Richtlinie)

Die SA-Verhandlung wird über den Kontrollkanal abgewickelt. Von der IPsec-Maschine wird die SA an das IKE-Protokoll übergeben, das sie über den Kontrollkanal zur IPsec-Maschine der Gegenstelle überträgt.

Abb. oben: Kontrollkanal und SA-Verhandlung

Damit der IPsec-Prozess in Gang kommen kann, muss vorher die SA verhandelt worden sein. Diese SA-Verhandlung findet pro SPD – die für verschiedene Ports, Adressen und Protokolle angelegt sein können – einmal statt. Für diese SA-Verhandlung wird ein Kontrollkanal benötigt.

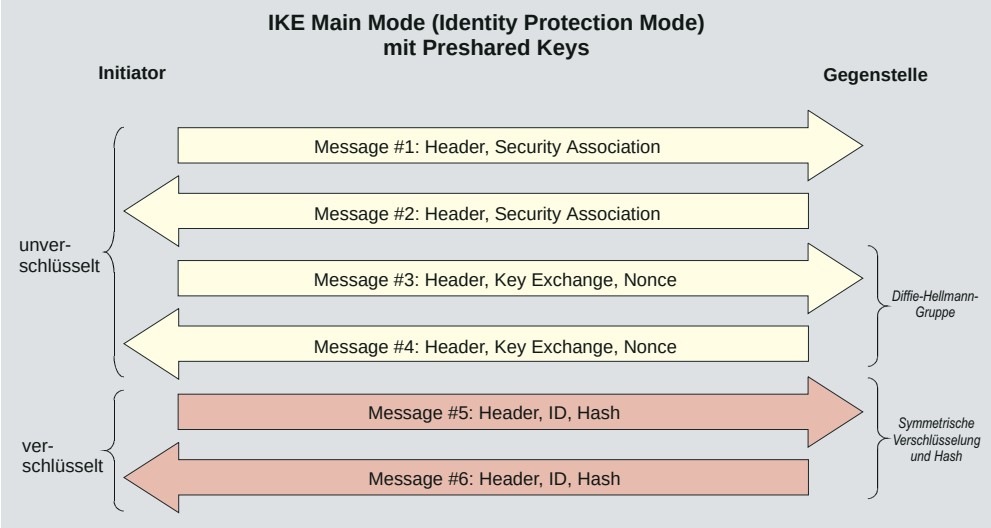
Im Client muss nun zunächst eine Layer 2-(PPP)-Verbindung zum Provider hergestellt werden. Dabei bekommt er (bei jeder Einwahl) eine neue IP-Adresse. Das IPsec-Modul im Client bekommt ein IP-Paket mit der Zieladresse der Firmenzentrale. Ein SPD-Eintrag für dieses IP-Paket wird gefunden aber es existiert noch keine SA. Das IPsec-Modul stellt die Anforderung an das IKE-Modul, eine SA auszuhandeln. Dabei werden auch die angeforderten Sicherheits-Richtlinien, wie sie im SPD-Eintrag vorhanden sind, an das IKE-Modul übergeben. Eine IPsec-SA auszuhandeln wird als Phase-2-Verhandlung bezeichnet. Bevor jedoch eine IPsec-SA mit der Gegenstelle (Secure Server) ausgehandelt werden kann, muss eine Art Kontrollkanal vom Client zum Secure Server existieren. Dieser Kontrollkanal wird über die Phase-1-Verhandlung hergestellt, deren Ergebnis eine IKE-SA ist. Die Phase-1-Verhandlung übernimmt somit die komplette Authentisierung vom Client gegenüber dem Secure Server (VPN Gateway) und erzeugt einen verschlüsselten Kontrollkanal. Über diesen Kontrollkanal kann dann rasch die Phase 2 (IPsec SA) durchgeführt werden. Die Phase-1-Verhandlung ist ein Handshake, über den auch der Austausch von Zertifikaten möglich ist und die den Schlüsselaustausch für den Kontrollkanal beinhaltet.

IKE-Modi

Im wesentlichen können zwei Arten der IKE-Richtlinien konfiguriert werden. Sie unterscheiden sich durch die Art der Authentisierung, entweder über Preshared Key oder über RSA-Signatur. Beide Arten des Internet Key Exchanges können in zwei unterschiedlichen Modi (Austausch-Modi / Exchange Modes) ausgeführt werden, dem Main Mode, auch Identity Protection Mode, oder dem Aggressive Mode. Die Modi unterscheiden sich durch die Anzahl der Messages und durch die Verschlüsselung.

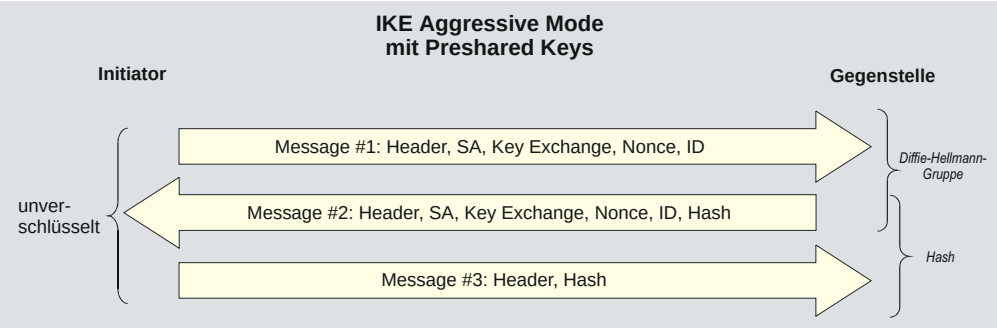
Wird die Pre-shared Key-Methode im Main Mode genutzt (Abb. unten), so muss der Client am Gateway durch seine IP-Adresse eindeutig identifizierbar sein, da der Pre-shared Key mit in die symmetrische Schlüsselberechnung einbezogen und verschlüsselt wird, bevor sonstige Informationen übertragen werden, die den Client identifizieren könnten. Ein Client, der sich beim Provider einwählt, ist jedoch nicht durch die IP-Adresse zu erkennen, da er bei jeder Provider-Anwahl eine neue zugewiesen bekommt. Letztlich kann im Main Mode an alle Clients nur derselbe Pre-shared Key vergeben werden, was allerdings die Authentisierung abschwächt.

Im Main Mode (Standard-Einstellung) werden sechs Meldungen über den Kontrollkanal geschickt, wobei die beiden letzten, welche die User ID, das Zertifikat, die Signatur und ggf. einen Hash-Wert beinhalten, verschlüsselt werden – daher auch Identity Protection Mode.



Eine Möglichkeit, einen allgmeinen Preshared Key zu vermeiden, wäre, den Aggressive Mode zu nutzen (Abb. unten), doch wird dabei die ID des Clients nicht verschlüsselt.

Im Aggressive Mode gehen nur drei Meldungen über den Kontrollkanal, wobei nichts verschlüsselt wird.



Den IKE-Modus für (die dynamisch erzeugte SPD), Main Mode oder Aggressive Mode, definieren Sie in den Konfigurationsfeldern **Security** am Enterprise Client.

Werden RSA-Signaturen eingesetzt, so bedeutet dies, dass Zertfikate zum Einsatz kommen, womit die Vorkonfiguration jedweder "Secrets" überflüssig wird.

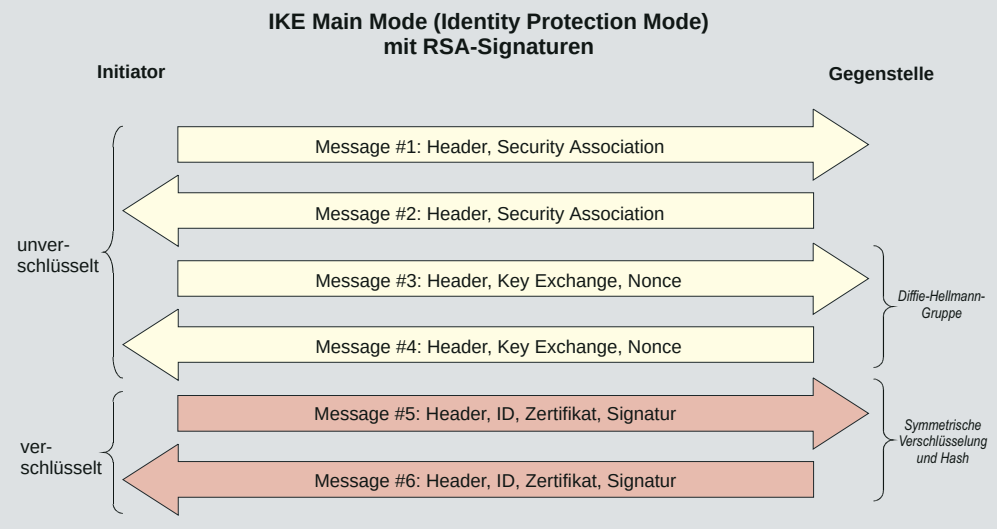


Abb. rechts:
IKE Main Mode mit RSA-Signaturen

Abb. rechts:
IKE Aggresive Mode mit RSA-Signaturen

Konfiguration von IPsec Tunneling mit NCP Clients

IPsec Tunneling entspricht dem standardisierten IPsec-Protokoll (native IPsec), das auch gegenüber IPsec Gateways zum Einsatz kommen kann, die von anderen Herstellern als NCP stammen.

Eine Tunnelverbindung vom Enterprise Client zum Gateway kann über L2TP (Layer 2-Tunnel) oder über IPsec Tunneling (Layer 3-Tunnel) oder über beide (IPsec over L2TP) hergestellt werden.

Um eine Tunnelverbindung mit native IPsec herstellen zu können, muss in den Profil-Einstellungen des Enterprise Clients im Konfigurationsfeld **Tunnel-Parameter** das VPN-Protokoll “IPsec Tunneling” (Layer 3) selektiert werden.

Die Kompatibilität mit den IPsec-Modi der anderen Hersteller beruht auf der Konformität mit folgenden RFCs und Drafts zu IPsec:

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)

Algorithmen für Phase 1 und 2

Folgende Algorithmen sind am Client implementiert zur Unterstützung für:

Authentisierung für Phase 1 (IKE-Richtlinie)
– RSA-Signatur
– PSK (Pre-shared Key)

Symmetrische Verschlüsselung (Phase 1 + 2)

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

Asymmetrische Verschlüsselung (Phase 1 + 2)
– DH 1,2,5 (Diffie-Hellman)
– RSA

Hash-Bestimmung
– MD5
– SHA-1

Zusätzliche Unterstützung für Phase 2
– PFS (Perfect Forward Secrecy)
– IPsec-Kompression (LZS, Deflate)
– Seamless re-keying

Wird am Secure Client ein Profil mit “IPsec-Tunneling” konfiguriert, so werden zunächst einige Standards gesetzt:

IKE Phase 1 Richtlinie = Von Gegenstelle bestimmt
IKE Phase 2 Richtlinie = Von Gegenstelle bestimmt
IKE Phase 1 Modus RSA = Main Mode
IKE Phase 1 Modus PSK = Aggressive Mode

Die automatisch gesetzten Richtlinien und Verhandlungsmodi sind konfigurierbar gehalten, sodass sie anderslautenden Verbindungsanforderungen entsprechend über die **IPsec-Konfiguration** modifiziert werden können.

Standard IKE-Vorschläge

Ohne Eintrag eines Pre-shared Keys in der Client-Konfiguration

Bleibt das Feld für “Pre-shared Key” leer, wenn die Einstellung “von Gegenstelle bestimmt” vorgenommen wurde, so wird vom Client (IPsec-Initiator) automatisch eine Liste von Vorschlägen für die IKE-Richtlinie verschickt, wobei die Authentisierung immer mit Zertifikat erfolgt (vgl. oben IKE-Modi mit RSA-Signatur).

Das Gateway prüft die Liste und sucht nach seiner Priorität die stärkste Sicherheits-Kombination heraus. Passt kein Vorschlag des Clients zur Liste des Gateways, wird die Verbindung nicht aufgebaut.

Vorschlagsliste für IKE-Richtlinie

```
EA    = Encryption Algorithm (Verschlüsselung)
HASH  = Hash Algorithm (Hash)
AUTH  = Authentication Method (Authentisie-
rung)
GROUP = Diffie-Hellman Group Number (DH-Grup-
pe)
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

Wird ein spezifischer IKE-Vorschlag in der IPsec-Konfiguration des Client eingestellt, so wird immer auch automatisch der gleiche Vorschlag zusätzlich mit Extended Authentication generiert und an die Gegenstelle geschickt.

Mit Eintrag eines Pre-shared Keys in der Client-Konfiguration

Wird in das Feld für “Pre-shared Key” ein String eingetragen, so werden an das Gateway der Gegenstelle automatisch vom Client (IPsec-Initiator) folgende Vorschläge für die IKE-Richtlinie versendet, wobei die Authentisierung immer ohne Zertifikat erfolgt (vgl. oben IKE-Modi mit Pre-shared Key).

Das Gateway prüft die Liste und sucht nach seiner Priorität die stärkste Sicherheits-Kombination mit Pre-shared Key heraus. Passt kein Vorschlag des Clients zur Liste des Gateways, wird die Verbindung nicht aufgebaut.

Vorschlagsliste für IKE-Richtlinie

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

Standard IPsec-Vorschläge

In Phase 2 schickt der Client zur Aushandlung der IPsec-Richtlinie in der Standardeinstellung ebenfalls eine Liste von Vorschlägen, von welcher ein Vorschlag zur IPsec-Richtlinie der Gegenstelle passen muss.

Das Gateway prüft die Liste und sucht nach seiner Priorität den passenden Vorschlag heraus. Passt kein Vorschlag des Clients zur Liste des Gateways, wird die Verbindung nicht aufgebaut.

Vorschlagsliste für IPsec-Richtinie

```
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-Parameter

Im folgenden finden Sie die wichtigsten Einstellungen für die IPsec-Konfiguration. Mit einem Mausklick auf die fettgedruckten roten Begriffe öffnet sich das Dokument Secure Client-Parameter an der entsprechenden Stelle.

IPsec Tunneling

Am Enterprise Client wird im Konfigurationsfeld **Tunnel-Paramter** das VPN-Protokoll IPsec-Tunneling selektiert. Damit wird die native IPsec-Verbindung ohne einen Layer 2-Tunnel (L2TP) hergestellt.

Mit der Erzeugung eines IPsec-Profils werden (am Enterprise Client unter **Tunnel-Parameter**) folgende Einstellungen automatisch gesetzt:

IKE-Richtlinie = von Gegenstelle bestimmt
IPsec-Richtlinie = von Gegenstelle bestimmt

(Bei dieser Richtlinien-Einstellung wählt das IPsec Gateway die passende Richtlinie aus einer Liste von Standard-Vorschlägen aus, wie oben beschrieben).

Austausch-Modus

Die Standard-Einstellung ist Main Mode und sollte nur in Absprache mit dem Systemadministrator geändert werden. (Unter **Security**.)

IKE ID-Typ und IKE ID

Diese Parameter befinden sich am Enterprise Client unter **Security** und können nur in Absprache mit dem Systemadministrator korrekt gesetzt werden.

Pre-shared Key oder RSA Signatur

Entsprechend der Vorgaben durch die Gegenstelle kann als IKE-Richtlinie die automatisch vorgenommene Einstellung “von Gegenstelle bestimmt” auf “Pre-shared Key” oder “RSA-Signatur” (Zertifikat) abgeändert werden.

Erwartet die Gegenstelle “Pre-shared Key”, so muss der Schlüssel in das Feld eingetragen werden. Er muss mit dem Pre-shared Key für diesen Benutzer am Gateway übereinstimmen.

Ebenso kann in Absprache mit der zentralen Gegenstelle die IPsec-Richtlinie nach deren Vorgaben geändert werden. Dies erfolgt unter **Security**.

Sollen Details der Richtlinien editiert werden, so kann auch dies nur in Absprache mit dem Systemadministrator erfolgen. Dazu muss am Client die **IPsec-Konfiguration** geöffnet werden.

IP-Adressen und DNS Server

IP-Adressen und DNS Server werden für den Enterprise Client standardmäßig über das Protokoll IKE-Config Mode (Draft 2) zugewiesen (kompatibel derzeit nur gegen Cisco).

Die Einstellungen können nach Absprache mit dem Systemadministrator in der **IPsec-Adresszweisung** geändert werden.

Für die NAS-Einwahl können alle bisherigen WAN-Schnittstellen verwendet werden.

Authentisierung

Wenn die Authentisierung über das XAUTH Protokoll (Draft 6) erfolgt (Standard-Einstellung) müssen folgende Parameter, womit sich der Benutzer am Gateway authentisiert, gesetzt sein:

am Enterprise Client unter **Tunnel-Parameter**
– VPN-Benutzername
– VPN-Passwort
– Zugangsdaten aus Zertifikatsfeld ...
(optional bei Einsatz eines Zertifikats)

Wie die Authentisierung zu erfolgen hat, legt die Gegenstelle fest.

DPD und NAT-T

Bei IPsec Tunneling wird im Hintergrund automatisch DPD (Dead Peer Detection) und NAT-T (NAT Traversal) ausgeführt, falls dies von der Gegenstelle unterstützt wird. Mit DPD prüft der IPsec Client in bestimmten Abständen, ob die Gegenstelle noch aktiv ist. Bei inaktiver Gegenstelle erfolgt ein automatischer Verbindungsabbau. DPD kann im Konfigurationsfeld **Erweiterte IPsec-Optionen** deaktiviert werden.

Der Einsatz von NAT Traversal erfolgt beim IPsec Client automatisch und ist immer nötig, wenn auf dem weg zum Zielsystem ein Gerät mit Network Address Translation zum Einsatz kommt.

PFS / DH-Gruppe

Am Enterprise Client kann die Diffie-Hellman-Gruppe für den Schlüsselaustausch (Perfect For-

ward Secrecy) pro IPsec-Richtlinien-Vorschlag in der **IPsec-Konfiguration** selektiert werden.

Standard-Einstellung ist “keine”. Eine Änderung der Einstellung ist nur nach Absprache mit dem Administrator sinnvoll, da die Vorgabe der Gegenstelle erfüllt werden muss.

IPsec-Kompression

Der Enterprise Client unterstützt die Kompressionsverfahren LZS und Deflate.

Pro IPsec-Richtlinie kann in der **IPsec-Konfiguration** zwischen beiden Verfahren differenziert werden.

Das IPsec Gatewas wählt das Kompressionsverfahren aus, das es unterstützt. Ist die Kompression am Client aktiv und das Gateway unterstützt keine Kompression, kommt keine Verbbindung zustande.

IPsec für Remote Access – IPSec over L2TP

Wie lässt sich IPsec in uneingeschränktem Funktionsumfang für Remote Access nutzen, ohne dass Sicherheitslücken entstehen, d. h. wie kann trotz sich ändernder IP-Adressen das Prinzip der IP-Adressen-Orientierung von IPsec beibehalten werden, ohne dass die oben beschriebenen Einschränkungen vorgenommen werden müssen?

Wie in RFC 2888 beschrieben und von verschiedenen IPsec-Experten empfohlen, kann dies bewerkstelligt werden, indem zunächst ein Layer 2-Tunnel über das Internet zwischen Remote Access Client und Zentralsystem aufgebaut wird, so dass die anschließende IPsec-Verhandlung bereits in einem VPN (Virtual Private Network) getunnelt stattfindet.

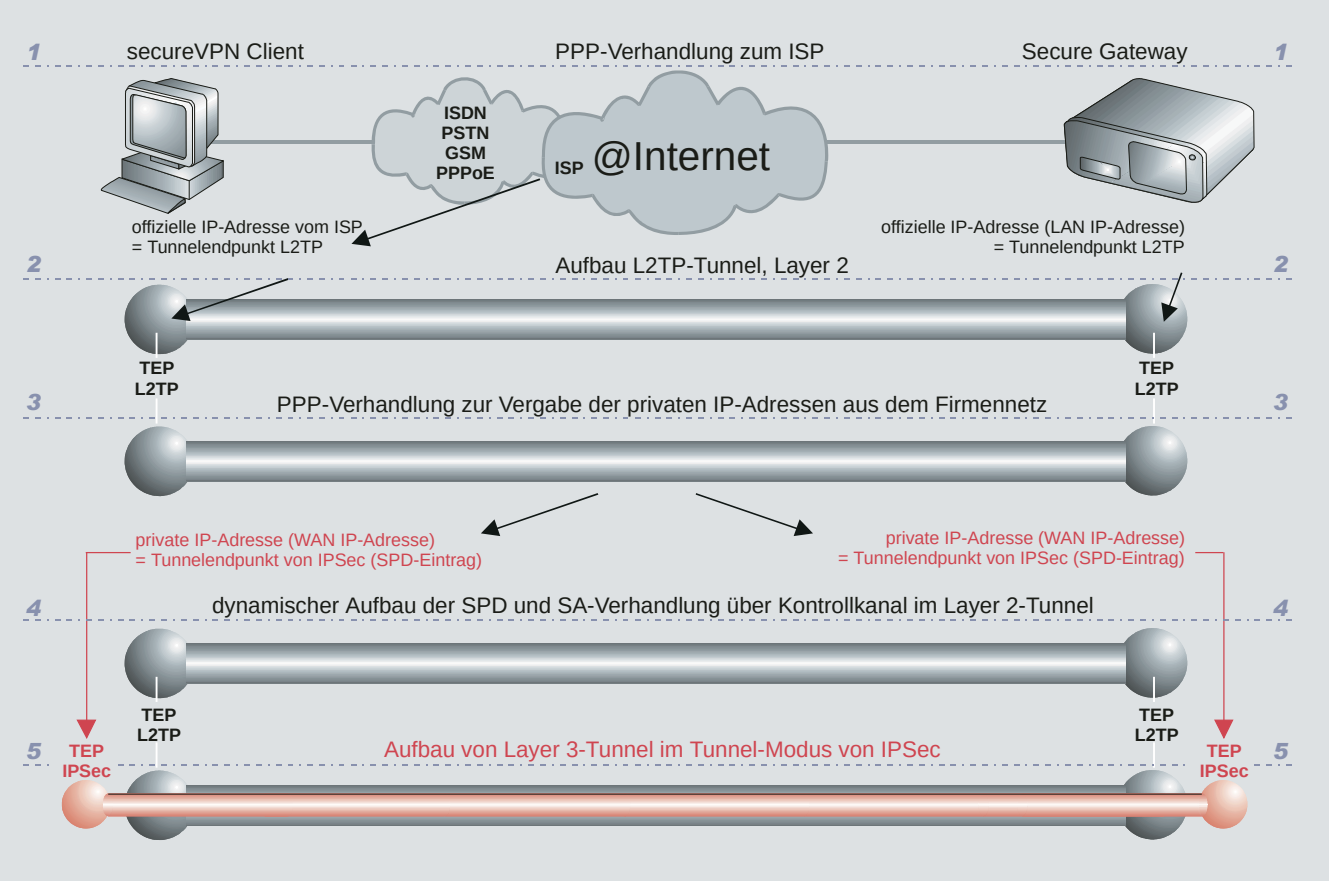
Der Tunnelaufbau wird durch eine benutzerorientierte Authentisierung (Layer 2) gesichert. Danach kann eine IP-Adresse aus dem Firmennetz vergeben werden, die für den daraufhin einsetzenden IPsec-Prozess verwendet werden kann.

Mit IPsec over L2TP (am Enterprise Client zu konfigurieren mit **VPN-Protokoll L2TP** und **Security-Modus IPsec**) werden alle Nachteile von IPsec im Remote Access-Bereich wett gemacht. Jeder handelsübliche Router, der IP Network Address Translation unterstützt, kann eingebunden werden. Zudem besteht die Möglichkeit, über standardi-sierte Schnittstellen zusätzliche Sicherheitsmechanismen einer Public Key Infrastucture zu nutzen. Um die Sicherheit von IPsec over L2TP auf ganzer Strecke gewährleisten zu können, empfiehlt NCP das Secure Gateway hinter dem Access Server und der Firewall in der Demilitarisierten Zone (DMZ) zu installieren. Damit befinden sich alle Parameter der sicheren Datenübertragung im Einflussbereich des Unternehmens:

- ☑ Endpunkte des Layer 2-Tunnels (Secure Server, VPN Gateway, Remote Client)
- ☑ Tunnelingverfahren
- ☑ Schlüsselalgorithmus
- ☑ Netzwerkprotokoll
- ☑ Datenkompression
- ☑ Übertragungsmedium
- ☑ IP-Adresse aus dem Firmennetz
- ☑ IPsec-Parameter

Eine Funktionsdarstellung befindet sich auf der folgenden Seite.

IPsec over L2TP mit dynamischer SPD



1. Standard-PPP-Verhandlung über Benutzer / Passwort (User ID / Password) und Authentisierung vom Client gegenüber Internet Service Provider (ISP), wonach der Client eine offizielle IP-Adresse vom ISP erhält. Anschließend baut der Client eine Verbindung zum Secure Server via Internet auf. Die dazu nötigen Parameter befinden sich in den Profil-Einstellungen des Clients unter “Grundeinstellungen” und “Netzeinwahl”. Der “Gateway (Tunnel-Endpunkt)”, eingetragen im Konfigurationsfeld “Tunnelparameter”, entspricht der offiziellen IP-Adresse des Secure Servers.

2. Nach Prüfung des “Tunnelsecret” werden die Tunnel-Parameter verhandelt und der L2TP-Tunnel im Layer 2 aufgebaut. Tunnelendpunkte sind die offizielle IP-Adresse, die der Client vom ISP erhalten hat und die offizielle IP-Adresse des Secure Servers, “Gateway (Tunnel-Endpunkt)”.(1* (*2

3. Nach einer weiteren PPP-Verhandlung und Prüfung von “Benutzer” und “Passwort”, erfolgt die Vergabe der privaten IP-Adressen aus dem Firmennetz. Diese Adressen können aus einem Pool des Secure Servers stammen. Der Remote Client ist damit – unabhängig von seinem Standort – immer eindeutig anhand seiner IP-Adresse identifizierbar.

4. Über den Kontrollkanal im Layer 2-Tunnel findet die SA-Verhandlung statt. Die Strong Authentication erfolgt gemäß der IKE-Richtlinien (IKE Policy), die für dieses Link-Profil festgelegt wurden (Profil-Einstellungen: Security).

5. Der Layer 3-Tunnel wird nach Vorgabe des IPsec-Betriebsmodus (Profil-Einstellungen: Security, IPsec-Richtlinie) aufgebaut. Tunnel-Endpunkte sind die IP-Adressen aus dem Firmennetz.

(*1 Nach IETF muss das Tunnelende immer im geschützten privaten Bereich des VPN-Betreibers, hinter der Firewall in der DMZ liegen.
(*2 Bei L2Sec erfolgt hier die SSL-Verhandlung.