

ELSA LANCOM™ VPN Option

© 2001 ELSA AG, Aachen (Germany)

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. ELSA haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist.

Weitergabe und Vervielfältigung der zu diesem Produkt gehörenden Dokumentation und Software und die Verwendung ihres Inhalts sind nur mit schriftlicher Erlaubnis von ELSA gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

ELSA ist DIN-EN-ISO-9001-zertifiziert. Mit der Urkunde vom 15.06.1998 bescheinigt die akkreditierte Zertifizierungsstelle TÜV-CERT die Konformität mit der weltweit anerkannten Norm DIN EN ISO 9001. Die an ELSA vergebene Zertifikatsnummer lautet 09 100 5069.

Alle Erklärungen und Urkunden zur Zulassung der Produkte finden Sie im Anhang dieser Dokumentation, sofern sie zum Zeitpunkt der Drucklegung vorlagen.

Marken

Windows[®], Windows NT[®] und Microsoft[®] sind eingetragene Marken von Microsoft, Corp.

Cisco ist eine eingetragene Marke von Cisco Systems, Inc.

SSH Secure Shell, SSH IPSEC Express, SSH NAT Traversal, SSH Sentinel und SSH Certifier sind Marken von SSH Communications Security.

ELSA LANCOM VPN-Produkte werden hergestellt unter Lizenz von SSH Communications Security. Für Produktbestandteile von SSH gilt: © 2000 SSH Communications Security. Alle Rechte vorbehalten.

Das ELSA-Logo ist eine eingetragene Marke der ELSA AG. Alle übrigen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein.

ELSA behält sich vor, die genannten Daten ohne Ankündigung zu ändern, und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

ELSA AG
Sonnenweg 11
52070 Aachen
Deutschland

www.elsa.de

Aachen, Juli 2001

Ein Wort vorab

Vielen Dank für Ihr Vertrauen!

Mit *LANCOM VPN Option* erweitern Sie einen *ELSA LANCOM* um die Fähigkeit, sogenannte virtuelle private Netzwerke aufzubauen. Damit wird es Ihnen möglich, kostengünstige Netzwerkkoppelungen über das Internet aufzubauen, ohne auf die gewohnt hohe Datensicherheit direkter Verbindungen verzichten zu müssen.

Eine besondere Eigenschaft von *LANCOM VPN* ist *LANCOM Dynamic VPN*, eine von ELSA zum Patent angemeldete Technologie. Während VPN üblicherweise statische IP-Adressen voraussetzt, ermöglicht das *LANCOM Dynamic VPN* den Aufbau von VPN-Verbindungen auch mit dynamischen IP-Adressen. Dadurch können Sie *LANCOM VPN* mit jeder Internetanbindung verwenden.

An der Erstellung dieser Dokumentation haben mehrere Mitarbeiter/innen aus verschiedenen Teilen des Unternehmens mitgewirkt, um Ihnen die bestmögliche Unterstützung bei der Nutzung Ihres ELSA-Produktes anzubieten.

Sollten Sie dennoch einen Fehler finden, oder einfach nur Kritik oder Anregung zu dieser Dokumentation äußern wollen, senden Sie bitte eine E-Mail direkt an:

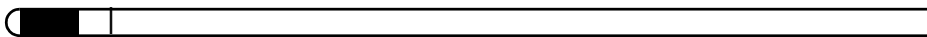


editorial@elsa.de.

Sollten Sie zu den in diesem Handbuch besprochenen Themen noch Fragen haben oder zusätzliche Hilfe benötigen, steht Ihnen unser Internet-Server www.elsa.de rund um die Uhr zur Verfügung. Hier finden Sie im Dateibereich 'Support' unter 'Know-how' viele Antworten auf „häufig gestellte Fragen“. Darüber hinaus bietet Ihnen die Wissensdatenbank (KnowledgeBase) einen großen Pool an Informationen. Aktuelle Treiber, Firmware, Tools und Handbücher stehen Ihnen jederzeit zum Download bereit.

Inhalt

1 Einführung	7
1.1 Lieferumfang der <i>ELSA LANCOM VPN Option</i>	7
1.2 Welchen Nutzen bietet VPN?	7
1.2.1 Private IP-Adressen im Internet?	10
1.2.2 Sicherheit des Datenverkehrs im Internet?	11
1.2.3 VPN nur für Internet-Verbindungen?	12
1.3 VPN-Verbindungen im Detail	13
1.3.1 LAN-LAN-Kopplung	13
1.3.2 Einwahlzugänge (Remote Access Service)	14
1.4 Was ist <i>ELSA LANCOM Dynamic VPN</i> ?	14
1.4.1 Ein Blick auf die IP-Adressierung	15
1.4.2 So funktioniert <i>ELSA LANCOM Dynamic VPN</i>	16
1.5 <i>ELSA LANCOM VPN</i> im Überblick	19
1.6 So geht es weiter	20
2 Die Installation der VPN-Option	21
2.1 Installations-Voraussetzungen	21
2.1.1 Unterstützte <i>ELSA LANCOM</i>	21
2.1.2 Lieferumfang	21
2.1.3 Zugriff auf das Gerät und <i>ELSA LANconfig</i>	22
2.1.4 Version von <i>ELSA LANconfig</i> überprüfen	22
2.1.5 Version der Firmware überprüfen	22
2.1.6 Firmware aktualisieren	23
2.2 Online-Registrierung	24
2.3 Freischalten der VPN-Option	25
2.4 Überprüfen der Freischaltung	26
3 Einrichtung der VPN-Verbindung	27
3.1 Der <i>ELSA LANconfig</i> -Assistent für VPN	27
3.2 Welche Fragen stellt der Assistent?	28
3.2.1 Die Konfigurationseinträge in der Übersicht	28
3.2.2 Bedeutung der Konfigurationseinträge	30
3.3 Beispiele für VPN-Konfigurationen	35
3.3.1 VPN über direkte Verbindung	35
3.3.2 VPN über das Internet	37



3.4	Einrichten der Basisverbindung	40
3.4.1	Direkte Verbindungen	40
3.4.2	Verbindungen über Internet	41
3.5	Vor Eingabe der VPN-Verbindungsdaten	41
3.6	Eingabe der Daten und Test der VPN-Verbindung	41

4	Die Technik hinter VPN	43
4.1	Wie funktioniert VPN?	43
4.1.1	IPSec – Die Basis für <i>ELSA LANCOM VPN</i>	43
4.1.2	Alternativen zu IPSec	44
4.2	Die Standards hinter IPSec	46
4.2.1	Module von IPSec und ihre Aufgaben	46
4.2.2	Security Associations – nummerierte Tunnel	47
4.2.3	Die Authentifizierung – das AH-Protokoll	47
4.2.4	Verschlüsselung der Pakete – das ESP-Protokoll	50
4.2.5	Management der Schlüssel – IKE	52

1

Einführung

Dieses Kapitel gibt Antworten auf die drei folgenden Fragen:

- Was gehört zum Lieferumfang der *ELSA LANCOM VPN Option*?
- Welchen Nutzen hat VPN?
- Welche Fähigkeiten und Eigenschaften hat *ELSA LANCOM VPN*?

1.1

Lieferumfang der *ELSA LANCOM VPN Option*

Prüfen Sie bitte zunächst, ob dem Paket *ELSA LANCOM VPN Option* neben dem vorliegenden Handbuch auch die folgenden Komponenten enthält:

- *ELSA LANCOM VPN Option*-CD
- Lizenznachweis (gelber Aufkleber)

1.2

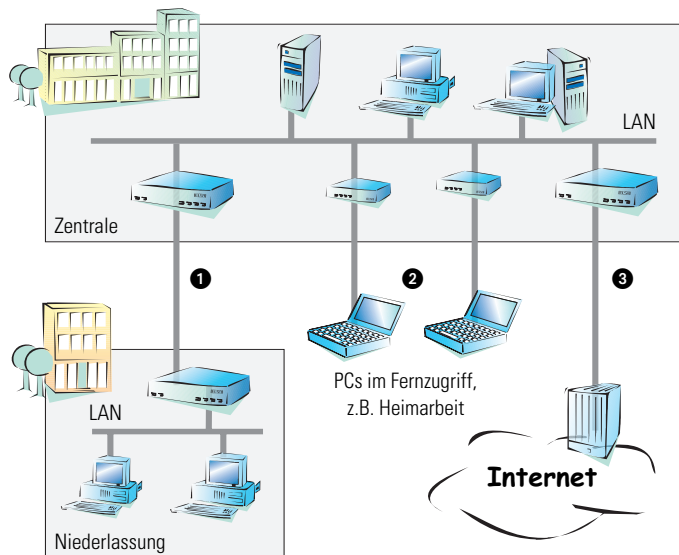
Welchen Nutzen bietet VPN?

Mit einem VPN (**V**irtual **P**rivate **N**etwork) können sichere Datenverkehrsverbindungen über kostengünstige, öffentliche IP-Netze aufgebaut werden, beispielsweise über das Netz der Netze: das Internet.

Was sich zunächst unspektakulär anhört hat in der Praxis enorme Auswirkungen. Zur Verdeutlichung schauen wir uns zunächst ein typisches Unternehmensnetzwerk ohne VPN-Technik an. Im zweiten Schritt werden wir dann sehen, wie sich dieses Netzwerk durch den Einsatz von VPN optimieren lässt.

Herkömmliche Netzwerkstruktur

Blicken wir zunächst auf eine typische Netzwerkstruktur, die in dieser Form oder ähnlich in vielen Unternehmen anzutreffen ist:



Das Unternehmensnetz basiert auf einem internen Netzwerk (LAN) in der Zentrale. Dieses LAN ist auf drei Wegen mit der Außenwelt verbunden:

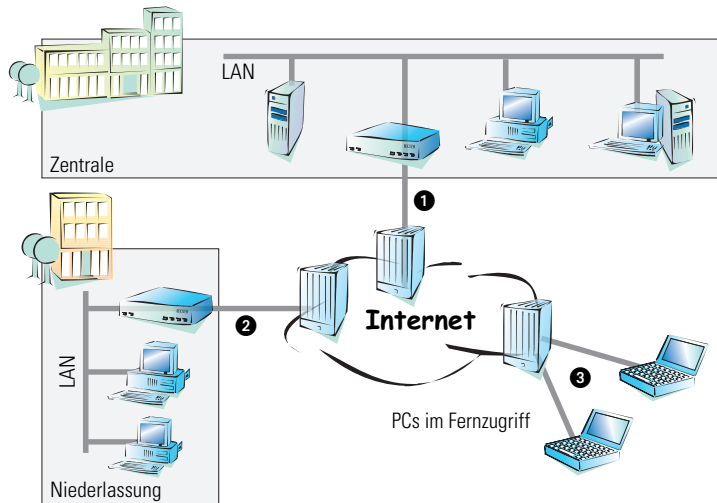
- ❶ Eine Niederlassung ist (typischerweise über eine Standleitung) angeschlossen.
- ❷ PCs wählen sich über ISDN oder Modem ins zentrale Netzwerk ein (Remote Access – RAS).
- ❸ Es existiert eine Verbindung ins Internet, um den Benutzern des zentralen LAN den Zugriff auf das Web und die Möglichkeit zum Versand und Empfang von E-Mails zu geben.

Alle Verbindungen zur Außenwelt basieren auf dedizierten Leitungen, d.h. Wähl- oder Standleitungen. Dedizierte Leitungen sind sehr zuverlässig und sicher. Andererseits erzeugen sie hohe Kosten. Die Kosten für dedizierte Leitungen sind in aller Regel von der Entfernung abhängig. So hat es gerade bei Verbindungen über weite Strecken Sinn, nach preisgünstigeren Alternativen Ausschau zu halten.

In der Zentrale muss für jeden verwendeten Zugangs- und Verbindungsweg (analoge Wählverbindung, ISDN, Standleitungen) entsprechende Hardware betrieben werden. Neben den Investitionskosten für diese Ausrüstung fallen auch kontinuierliche Administrations- und Wartungskosten an.

Vernetzung über Internet

Bei Nutzung des Internet (oder eines anderen öffentlichen Netzes auf IP-Basis) anstelle direkter Verbindungen ergibt sich folgende Struktur:



Alle Teilnehmer sind (fest oder per Einwahl) mit dem Internet verbunden. Es gibt keine teuren dedizierten Leitungen zwischen den Teilnehmern mehr.

- ❶ Nur noch die Internet-Verbindung des LANs der Zentrale ist notwendig. Spezielle Einwahlgeräte oder Router für dedizierte Leitungen zu einzelnen Teilnehmern entfallen.
- ❷ Die Niederlassung ist ebenfalls mit einer eigenen Verbindung ans Internet angeschlossen.
- ❸ Die RAS-PCs wählen sich über das Internet in das LAN der Zentrale ein.

Das Internet hat eine enorme Verbreitung und zeichnet sich durch geringe Zugangskosten aus. Insbesondere bei Verbindungen über weite Strecken sind gegenüber herkömmlichen Wähl- oder Standverbindungen deutliche Einsparungen zu erzielen.

Die physikalischen Verbindungen bestehen nicht mehr direkt zwischen zwei Teilnehmern, sondern jeder Teilnehmer hat selber nur einen Zugang ins Internet. Die Zugangstechnologie spielt dabei keine Rolle: Es kann sich um eine herkömmliche digitale ISDN-Verbindung handeln. Ebenso sind aber auch

Breitbandtechnologien wie DSL, Kabelmodem oder 2-Mbit-Festverbindungen möglich.

Die Technologien der einzelnen Teilnehmern müssen nicht kompatibel zueinander sein, wie das bei herkömmlichen Direktverbindungen erforderlich ist. Über einen einzigen Internet-Zugang können mehrere gleichzeitige logische Verbindungen zu verschiedenen Gegenstellen aufgebaut werden.

Die Kostenersparnis und die hohe Flexibilität machen das Internet (oder jedes andere IP-Netzwerk) zu einem hervorragenden Backbone für das Unternehmensnetzwerk.

Zwei technische Eigenschaften des IP-Standards stehen allerdings der Nutzung des Internets als Teil von Unternehmensnetzwerken entgegen:

- Die Notwendigkeit öffentlicher IP-Adressen für Teilnehmer des Internet
- Fehlende Datensicherheit durch ungeschützte Datenübertragung

1.2.1

Private IP-Adressen im Internet?

Der IP-Standard definiert zwei Arten von IP-Adressen: öffentliche und private. Eine öffentliche IP-Adresse hat weltweite Gültigkeit, während eine private IP-Adresse nur in einem abgeschotteten LAN gilt.

Öffentliche IP-Adressen müssen weltweit eindeutig und daher einmalig sein. Private IP-Adressen dürfen weltweit beliebig häufig vorkommen, innerhalb ihres abgeschotteten Netzwerkes jedoch nur einmal.

Normalerweise haben PCs im LAN lediglich private IP-Adressen, nur der Router ins Internet verfügt auch über eine öffentliche IP-Adresse. Nur solche Router sind innerhalb des Internet von anderen Rechnern (mit öffentlicher IP-Adresse) ansprechbar. PCs im LAN, die ausschließlich über private IP-Adressen verfügen, sind aus dem Internet heraus nicht ansprechbar.

Routing auf IP-Ebene mit VPN

Soll das Internet zur Kopplung von Netzwerken eingesetzt werden, müssen deshalb IP-Strecken zwischen Routern mit jeweils öffentlicher IP-Adresse eingerichtet werden. Diese Router stellen die Verbindung zwischen mehreren Teilnetzen her. Schickt ein Rechner ein Paket an eine private IP-Adresse in einem entfernten Netzwerksegment, dann setzt der eigene Router dieses Paket über das Internet an den Router des entfernten Netzwerksegments ab.

Die Umwandlung zwischen privaten und öffentlichen IP-Adressen übernimmt VPN. Ohne VPN können Rechner ohne eigene öffentliche IP-Adresse nicht über das Internet miteinander kommunizieren.

1.2.2

Sicherheit des Datenverkehrs im Internet?

Es existiert Skepsis gegenüber der Idee, Teile der Unternehmenskommunikation über das Internet abzuwickeln. Der Grund für die Skepsis ist die Tatsache, dass sich das Internet dem Einflussbereich des Unternehmens entzieht. Anders als bei dedizierten Verbindungen laufen die Daten durch fremde Netzstrukturen, deren Eigentümer dem Unternehmen häufig unbekannt ist.

Das Internet basiert außerdem nur auf einer simplen Form der Datenübertragung in Form unverschlüsselter Datenpakete. Dritte, durch deren Netze diese Pakete laufen, können sie mitlesen und möglicherweise sogar manipulieren. Der Zugang zum Internet ist für jedermann möglich. Dadurch ergibt sich die Gefahr, dass sich auch Dritte unbefugt Zugang zu den übertragenen Daten verschaffen.

VPN – Sicherheit durch Verschlüsselung

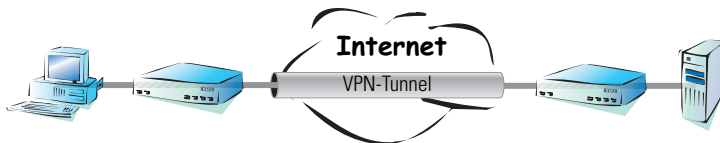
VPN wurde zur Lösung dieses Sicherheitsproblems entwickelt. Es verschlüsselt auf Wunsch den gesamten Datenverkehr zwischen zwei Teilnehmern. Für Dritte sind die Pakete unlesbar. Für VPN können die modernsten und sichersten Verschlüsselungstechniken verwendet werden. Damit wird ein sehr hohes Sicherheitsniveau erreicht. VPN-geschützter Datenverkehr über das Internet bietet eine Sicherheit, die dem Niveau dedizierter Leitungen zumindest entspricht.

Zur Datenverschlüsselung werden Codes zwischen den Teilnehmern vereinbart, die man üblicherweise als „Schlüssel“ bezeichnet. Diese Schlüssel kennen nur die Beteiligten im VPN. Ohne gültigen Schlüssel können Datenpakete nicht entschlüsselt werden. Die Daten bleiben Dritten unzugänglich, sie bleiben „privat“.

Schicken Sie Ihre Daten in den Tunnel – zur Sicherheit

Jetzt wird auch klar, warum mit VPN ein virtuelles privates Netz aufgebaut wird: Es entsteht zu keinem Zeitpunkt eine feste, physikalische Verbindung zwischen den Geräten, wie sie bei direkten Verbindungen notwendig ist. Dritte können mit entsprechendem technischen Aufwand die Daten während der Übertragung sogar verfolgen und aufzeichnen. Da die Pakete durch VPN

verschlüsselt sind, ist der eigentliche Inhalt der Pakete unzugänglich. Experten vergleichen diesen Zustand mit einem Tunnel: Offen nur am Anfang und am Ende, dazwischen perfekt abgeschirmt. Die sicheren Verbindungen innerhalb eines öffentlichen IP-Netzes werden deshalb auch „Tunnel“ genannt.



Damit ist das Ziel moderner Netzwerkstrukturen erreicht: Sichere Verbindungen durch kostengünstige IP-Netze. Die Tunnel machen's möglich.

1.2.3

VPN nur für Internet-Verbindungen?

Das Konzept VPN wurde speziell für den Aufbau von virtuellen Netzwerkstrukturen über öffentliche IP-Netze (insbesondere das Internet) entwickelt.

Sicherheitsbedenken existieren nicht nur gegenüber dem Internet. Auch private und abgeriegelte Netze für Direktverbindungen, wie etwa das Telefonnetz oder ISDN, bieten Möglichkeiten zum Abhören und Manipulieren übertragener Daten. Über das tatsächliche Ausmaß des Missbrauchs wird heftig diskutiert. Ein Bestehen eines Risikos wird aber kaum noch bestritten.

Grund genug, auch die Kommunikation über dedizierte Leitungen zusätzlich abzusichern. VPN bietet sich als Sicherheitskonzept an, auch wenn die eingesetzte Netzstruktur bei dedizierten Leitungen nicht virtuell sondern real ist.

ELSA LANCOM VPN kann sowohl auf Internet-Verbindungen als auch auf dedizierte Verbindungen aufgesetzt werden. Als dedizierte Verbindungen werden ISDN-Wählverbindungen, ISDN-Standleitungen und 2-Mbit-Standleitungen unterstützt.



Alle folgenden Erklärungen und Beispiele verwenden aus Gründen der Übersichtlichkeit immer das Internet als Grundlage für VPNs. Das Internet vertritt andere Verbindungsmöglichkeiten. An Stelle des Internet können daher immer auch private IP-Netze oder direkte Verbindungen eingesetzt werden.

1.3

VPN-Verbindungen im Detail

Es existieren zwei Arten von VPN-Verbindungen:

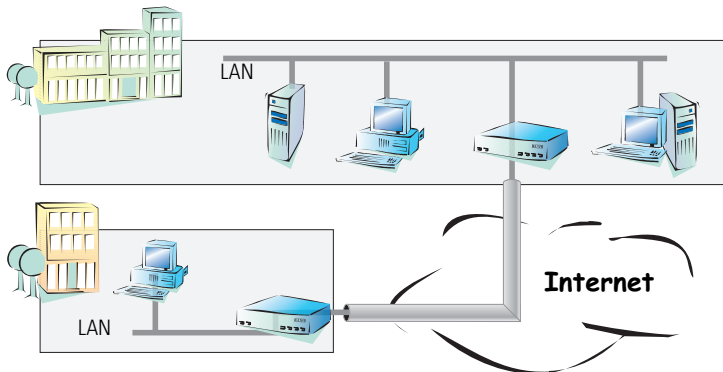
- VPN-Verbindungen zur Kopplung zweier lokaler Netzwerke. Diese Verbindungsart wird auch „LAN-LAN-Kopplung“ genannt.
- Den Anschluss eines einzelnen Rechners mit einem Netzwerk, in der Regel über Einwahlzugänge (RAS).

1.3.1

LAN-LAN-Kopplung

Als „LAN-LAN-Kopplung“ wird die Verbindung von zwei entfernten Netzen bezeichnet. Besteht eine solche Verbindung, dann können die Geräte in dem einen LAN auf Geräte des jeweils entfernten LANs zugreifen (sofern sie die notwendigen Rechte besitzen).

LAN-LAN-Kopplungen werden in der Praxis häufig zwischen Firmenzentrale und -niederlassungen oder zu Partnerunternehmen aufgebaut.



Auf jeder Seite des Tunnels befindet sich ein VPN-fähiger Router (VPN-Gateway). Die Konfiguration beider VPN-Gateways muss aufeinander abgestimmt sein.

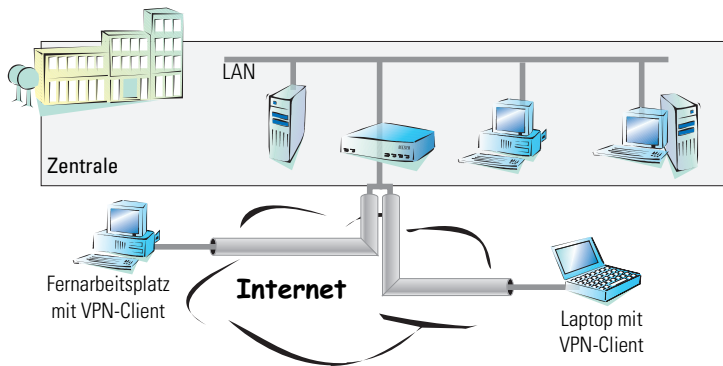
Für die Rechner und sonstigen Geräte in den lokalen Netzwerken ist die Verbindung transparent, d. h., sie erscheint ihnen wie eine gewöhnliche direkte Verbindung. Nur die beiden Gateways müssen für die Benutzung der VPN-Verbindung konfiguriert werden.

1.3.2

Einwahlzugänge (Remote Access Service)

Über Einwahlzugänge erhalten einzelne entfernte Rechner (Hosts) Zugriff auf die Ressourcen eines LANs. Beispiele in der Praxis sind Heimarbeitsplätze oder Außendienstmitarbeiter, die sich in das Firmennetzwerk einwählen.

Soll die Einwahl eines einzelnen PC in ein LAN über VPN erfolgen, dann wählt sich der einzelne PC ins Internet ein. Eine spezielle VPN-Client-Software baut dann auf Basis dieser Internetverbindung einen Tunnel zum VPN-Gateway im LAN auf.



Das VPN-Gateway im LAN muss den Aufbau von VPN-Tunneln mit der VPN-Client-Software des entfernten PC unterstützen. *ELSA LANCOM VPN* unterstützt derzeit keine Einwahl von VPN-Client-Software. Möglich ist nur der Aufbau von LAN-LAN-Kopplungen zwischen zwei VPN-Gateways. Eine Unterstützung von VPN-Client-Software ist in Vorbereitung.

Wir empfehlen aus Sicherheitsgründen, auch einzelne PCs stets über einen eigenen *ELSA LANCOM* anzubinden.

1.4

Was ist *ELSA LANCOM Dynamic VPN*?

ELSA LANCOM Dynamic VPN ist eine von ELSA zum Patent angemeldete Technik, die den Aufbau von VPN-Tunneln auch zu solchen Gegenstellen ermöglicht, die keine statische, sondern nur eine dynamische IP-Adresse besitzen. *ELSA LANCOM Dynamic VPN* ist fester Bestandteil der *ELSA LANCOM VPN Option*.

Wer benötigt *ELSA LANCOM Dynamic VPN* und wie funktioniert es? Die Antwort erfolgt in zwei Schritten: Zunächst zeigt ein Blick auf die Grundlagen der

IP-Adressierung das Problem statischer IP-Adressen. Der zweite Schritt zeigt die Lösung durch *ELSA LANCOM Dynamic VPN*.

1.4.1

Ein Blick auf die IP-Adressierung

Im Internet benötigt jeder Teilnehmer eine eigene IP-Adresse. Er benötigt sogar eine besondere Art von IP-Adresse, nämlich eine öffentliche IP-Adresse. Die öffentlichen IP-Adressen werden von zentralen Stellen im Internet verwaltet. Jede öffentliche IP-Adresse darf im gesamten Internet nur ein einziges Mal existieren.

Innerhalb lokaler Netzwerke auf IP-Basis werden keine öffentlichen, sondern private IP-Adressen verwendet. Für diesen Zweck wurden einige Nummernbereiche des gesamten IP-Adressraums als private IP-Adressen reserviert.

Einem Rechner, der sowohl an ein lokales Netzwerk als auch direkt an das Internet angeschlossen ist, sind deshalb zwei IP-Adressen zugeordnet: Eine öffentliche für die Kommunikation mit dem Rest des Internet und eine private, unter der er im lokalen Netzwerk erreichbar ist.

Statische und dynamische IP-Adressen

Öffentliche IP-Adressen müssen beantragt und verwaltet werden, was mit Kosten verbunden ist. Es gibt auch nur einen begrenzten Vorrat an öffentlichen IP-Adressen. Aus diesem Grund verfügt auch nicht jeder Internet-Benutzer über eine eigene feste (statische) IP-Adresse.

Die Alternative zu statischen IP-Adressen sind die sogenannten dynamischen IP-Adressen. Eine dynamische IP-Adresse wird dem Internet-Benutzer von seinem Internet Service Provider (ISP) bei der Einwahl für die Dauer der Verbindung zugewiesen. Der ISP verwendet dabei eine beliebige unbenutzte Adresse aus seinem IP-Adress-Pool. Die zugewiesene IP-Adresse ist dem Benutzer nur temporär zugewiesen, nämlich für die Dauer der aktuellen Verbindung. Wird die Verbindung gelöst, so wird die zugewiesene IP-Adresse wieder freigegeben, und der ISP kann sie für den nächsten Benutzer verwenden.

Vor- und Nachteile dynamischer IP-Adressen

Dieses Verfahren hat für den ISP einen wichtigen Vorteil: Er benötigt nur einen relativ kleinen IP-Adress-Pool. Auch für den Benutzer sind dynamische IP-Adressen günstig: Er muss nicht zuerst eine statische IP-Adresse beantragen, sondern kann sich sofort ins Internet einwählen. Auch die Verwaltung

der IP-Adresse entfällt. Dadurch erspart er sich Mühe und Gebühren. Die Kehrseite der Medaille: Ein Benutzer ohne statische IP-Adresse lässt sich aus dem Internet heraus nicht direkt adressieren.

Für den Aufbau von VPNs ergibt sich daraus ein erhebliches Problem. Möchte beispielsweise Rechner A einen VPN-Tunnel zu Rechner B über das Internet aufbauen, so benötigt er dessen IP-Adresse. Besitzt B nur eine dynamische IP-Adresse, so kennt A sie nicht, er kann B deshalb nicht ansprechen.

Hier bietet die Technik von *ELSA LANCOM Dynamic VPN* die Patentlösung.

1.4.2

So funktioniert *ELSA LANCOM Dynamic VPN*

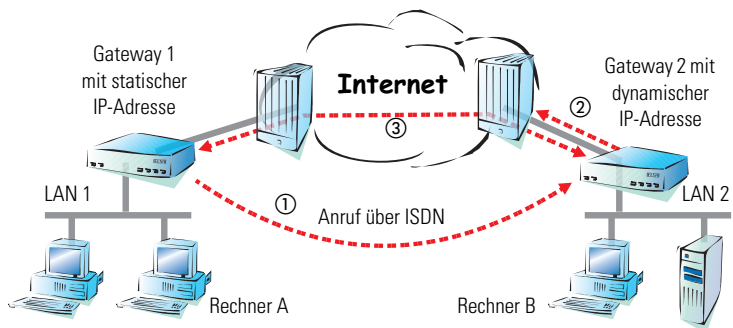
Verdeutlichen wir die Funktionsweise von *ELSA LANCOM Dynamic VPN* an Hand zweier Beispiele (Bezeichnungen beziehen sich auf IP-Adressart der beiden VPN-Gateways):

- statisch – dynamisch
- dynamisch – dynamisch

Statisch – dynamisch

Möchte ein Benutzer an Rechner A im LAN 1 eine Verbindung zu Rechner B im LAN 2 aufbauen, dann erhält Gateway 1 die Anfrage und versucht einen VPN-Tunnel zu Gateway 2 aufzubauen. Gateway 2 verfügt nur über eine dynamische IP-Adresse und kann daher nicht direkt über das Internet angesprochen werden.

Mit Hilfe von *ELSA LANCOM Dynamic VPN* kann der VPN-Tunnel trotzdem aufgebaut werden. Dieser Aufbau geschieht in drei Schritten:



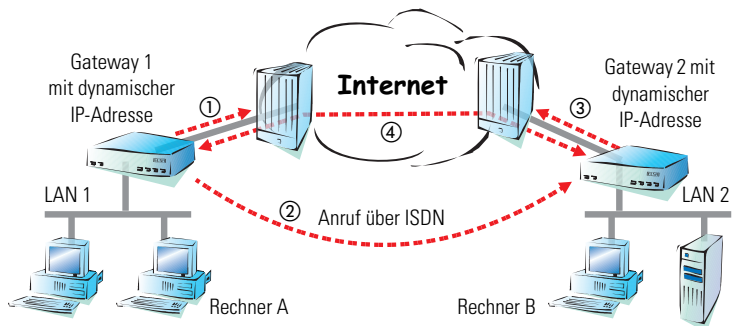
- ① Gateway 1 wählt Gateway 2 über ISDN an. Es nutzt dabei die ISDN-Möglichkeit, kostenlos seine eigene Rufnummer über den D-Kanal zu übermitteln. Gateway 2 ermittelt anhand der empfangenen Rufnummer aus den konfigurierten VPN-Gegenstellen die IP-Adresse von Gateway 1.

Für den Fall, dass Gateway 2 keine Rufnummer über den D-Kanal erhält (etwa weil das erforderliche ISDN-Leistungsmerkmal nicht zur Verfügung steht) oder eine unbekannte Rufnummer übertragen wird, nimmt Gateway 2 den Anruf entgegen, und die Geräte authentifizieren sich über den B-Kanal. Nach erfolgreicher Aushandlung übermittelt Gateway 1 seine IP-Adresse und baut den B-Kanal sofort wieder ab.

- ② Nun ist Gateway 2 an der Reihe: Zunächst baut es eine Verbindung zu seinem ISP auf, von dem es eine dynamische IP-Adresse zugewiesen bekommt.
- ③ Gateway 2 kann den VPN-Tunnel zu Gateway 1 jetzt aufbauen. Ihm ist die statische IP-Adresse von Gateway 1 ja von Anfang an bekannt.

Dynamisch – dynamisch

Der Aufbau von VPN-Tunneln gelingt mit *ELSA LANCOM Dynamic VPN* auch zwischen zwei Gateways, die beide nur über dynamische IP-Adressen verfügen. Passen wir das besprochene Beispiel an, so dass diesmal auch Gateway 1 nur über eine dynamische IP-Adresse verfügt. Wieder möchte Rechner A eine Verbindung zu Rechner B aufbauen:



- ① Gateway 1 baut eine Verbindung zu seinem ISP auf, um eine öffentliche dynamische Adresse zu erhalten.

- ② Es folgt der Anruf über ISDN bei Gateway 2 zur Übermittlung dieser dynamischen Adresse. Zur Übermittlung werden drei Verfahren verwendet:

- **Als Information im LLC-Element des D-Kanals.** Über das D-Kanal-Protokoll von Euro-ISDN (DSS-1) können im sogenannten LLC-Element (**L**ower **L**ayer **C**ompatibility) beim Anruf zusätzliche Informationen an die Gegenstelle übermittelt werden. Diese Übermittlung findet vor dem Aufbau des B-Kanals statt. Die Gegenstelle lehnt nach erfolgreicher Übertragung der Adresse den Anruf ab. Eine gebührenpflichtige Verbindung über den B-Kanal kommt auf diese Weise nicht zustande. Die IP-Adresse wird aber trotzdem übertragen, nach diesem Verfahren sogar kostenlos.



Das LLC-Element steht normalerweise im Euro-ISDN ohne besondere Anmeldung oder Freischaltung zur Verfügung. Es kann allerdings von Telefongesellschaften oder einzelnen Vermittlungsstellen auch gesperrt werden. Im nationalen ISDN nach 1TR6 gibt es kein LLC-Element. Das beschriebene Übermittlungsverfahren funktioniert daher nicht.

- **Als Subadresse über den D-Kanal.** Funktioniert die Adressübermittlung über das LLC-Element nicht, dann versucht Gateway 1 die Adresse als sogenannte Subadresse zu übermitteln. Die Subadresse ist wie das LLC-Element ein Informationselement des D-Kanal-Protokolls und ermöglicht wie dieses die kostenlose Übermittlung kurzer Informationen. Allerdings muss hier die Telefongesellschaft das ISDN-Merkmal 'Subadressierung' (normalerweise gegen Berechnung) freigeschaltet haben. Wie beim LLC-Element wird der Anruf nach erfolgreicher Übertragung der IP-Adresse von der Gegenstelle abgelehnt und die Verbindung bleibt gebührenfrei.
 - **Über den B-Kanal.** Scheitern beide Versuche, die IP-Adresse über den D-Kanal zu übertragen, dann muss für die Übertragung der IP-Adresse eine konventionelle Verbindung über den B-Kanal aufgebaut werden. Nach der Übertragung der IP-Adresse wird die Verbindung sofort abgebaut. Es fallen die üblichen Gebühren an.
- ③ Gateway 2 baut eine Verbindung zum ISP auf, der ihm eine dynamische IP-Adresse zuweist.
- ④ Gateway 2 baut den VPN-Tunnel zu Gateway 1 auf.



ELSA LANCOM Dynamic VPN funktioniert nur zwischen ELSA LANCOM, die jeweils über zumindest eine ISDN-Schnittstelle verfügen und zwischen denen eine ISDN-Verbindung aufgebaut werden kann.

1.5

ELSA LANCOM VPN im Überblick

In diesem Abschnitt sind alle Funktionen und Eigenschaften von *ELSA LANCOM VPN* aufgelistet. VPN-Experten wird dieser Überblick viel sagen. Er ist sehr kompakt, verwendet allerdings eine Vielzahl komplexer Fachbegriffe. Für das Verständnis ist die Kenntnis der technischen Grundlagen von VPN notwendig. Seien Sie beruhigt: Sie können diesen Abschnitt auch bedenkenlos überspringen. Für die Inbetriebnahme und den Betrieb von *ELSA LANCOM VPN* sind die Informationen nicht notwendig.

- VPN nach dem IPSec-Standard
- VPN-Tunnel über Festverbindung, Wählverbindung und IP-Netzwerk
- *ELSA LANCOM Dynamic VPN*: Öffentliche IP-Adresse können statisch oder dynamisch sein (ISDN-Verbindung erforderlich)
- Unterstützte Anschluss Technologien:

Gerät	Anschluss-technologie	Bemerkungen
<i>ELSA LANCOM Business 4000</i>	ISDN	
<i>ELSA LANCOM Business 4100</i>	ISDN (4 x)	
<i>ELSA LANCOM Business 6001</i>	X.21, ISDN	Backup über ISDN
<i>ELSA LANCOM Business 6011</i>	G.703, X.21, ISDN	Backup über ISDN
<i>ELSA LANCOM Business 6021</i>	G.703 (2 x), X.21, ISDN	Backup über ISDN
<i>ELSA LANCOM DSL/-1610 Office</i>	10Base-T (DSL, Kabelmodem etc.)	<i>ELSA LANCOM Dynamic VPN</i> nicht möglich
<i>ELSA LANCOM DSL/I-1611 Office</i>	10Base-T (DSL, Kabelmodem etc.), ISDN	Backup über ISDN

- IPSec-Protokolle AH und ESP jeweils im Transport- und Tunnelmodus
- Hash-Algorithmen:
 - HMAC-MD5-96, Hashlänge 128 bit
 - HMAC-SHA-1-96, Hashlänge 160 bit
- Symmetrische Verschlüsselungsverfahren
 - DES-CBC, Schlüssellänge 56 bit

- Triple-DES-CBC, Schlüssellänge 112 bit
- CAST-CBC, Schlüssellänge 128 bit
- Blowfish-CBC, Schlüssellänge 128 bit
- Gegenseitige Authentifizierung durch Preshared Keys
- Schlüsselaustausch über Oakley, Verschlüsselung nach Diffie-Hellman, Unterstützung der Well-known-groups 1 bis 5 (Schlüssellängen 768 bit, 1024 bit, 1536 bit, elliptische Kurven mit $GF(2^{155})$ und $GF(2^{185})$)
- Schlüsselmanagement nach ISAKMP

1.6

So geht es weiter

Im folgenden Kapitel wird die Installation der *ELSA LANCOM VPN Option* auf einem *ELSA LANCOM* beschrieben.

Sobald die *ELSA LANCOM VPN Option* auf dem gewünschten *ELSA LANCOM* installiert ist, lesen Sie im Kapitel 'Einrichtung der VPN-Verbindung' auf Seite 27, welche Schritte für den Aufbau von VPN-Verbindungen notwendig sind.

2 Die Installation der VPN-Option

In diesem kurzen Kapitel erfahren Sie, wie *ELSA LANCOM VPN Option* in Ihren *ELSA LANCOM* installiert wird. Die Installation erfolgt in sechs Schritten:

- ① Überprüfen der Installations-Voraussetzungen
- ② Online-Registrierung
- ③ Update der *ELSA LANtools* (*ELSA LANconfig*, *ELSA LANmonitor*)
- ④ Aufspielen der aktuellen Firmware
- ⑤ Freischalten der VPN-Option
- ⑥ Überprüfen der Freischaltung

2.1 Installations-Voraussetzungen

Nehmen Sie sich einige Minuten Zeit, und überprüfen Sie, ob bei Ihnen alle Voraussetzungen für eine erfolgreiche Installation vorliegen.

2.1.1 Unterstützte **ELSA LANCOM**

Die *ELSA LANCOM VPN Option* wird von folgenden *ELSA LANCOM* unterstützt:

- *ELSA LANCOM Business 4000*
- *ELSA LANCOM Business 4100*
- *ELSA LANCOM Business 6001*
- *ELSA LANCOM Business 6011*
- *ELSA LANCOM Business 6021*
- *ELSA LANCOM DSL/1610 Office (ohne ELSA LANCOM Dynamic VPN)*
- *ELSA LANCOM DSL/I-1611 Office*

2.1.2 Lieferumfang

Vergewissern Sie sich, dass das Optionspaket folgende Komponenten enthält:

- *ELSA LANCOM VPN*-CD mit *ELSA LANtools*, aktueller Firmware und elektronischer Dokumentation
- Gelber Aufkleber mit aufgedruckter Lizenznummer
- Handbuch

2.1.3

Zugriff auf das Gerät und *ELSA LANconfig*

Sie benötigen für die Installation der *ELSA LANCOM VPN Option* einen Rechner mit einem Windows-Betriebssystem (Windows 95, Windows 98, Windows NT 4.0, Windows 2000 oder Windows Millennium Edition). Dieser Rechner muss Zugriff auf den zu konfigurierenden *ELSA LANCOM* haben. Als Zugriffsart kommen entweder die eingebaute serielle Konfigurationsschnittstelle des Gerätes (Outband), das LAN (Inband) oder die Fernkonfiguration in Frage.

Auf dem Rechner muss das Konfigurationsprogramm *ELSA LANconfig* in Version 1.65 oder neuer installiert sein. Wenn Sie *ELSA LANconfig* auf diesem Rechner bereits installiert haben, dann überprüfen Sie die Version. Nähere Informationen zur Versionsüberprüfung finden Sie im folgenden Abschnitt.

Der Aufruf und die Bedienung von *ELSA LANconfig* ist in der Dokumentation Ihres *ELSA LANCOM* ausführlich beschrieben.

2.1.4

Version von *ELSA LANconfig* überprüfen

Vergewissern Sie sich, dass Sie *ELSA LANconfig* in Version 1.65 oder neuer benutzen. Unter dem Menübefehl ? ► **Info** erhalten Sie die Versionsnummer.

Die Version 1.65 der *ELSA LANtools* befindet sich auf der *ELSA LANCOM VPN*-CD und kann bei Bedarf über das SETUP-Programm auf Ihren Rechner installiert werden.

Brandaktuelle Versionen von ELSA LANconfig und ELSA LANmonitor finden Sie auf der ELSA-Homepage www.elsa.de im Dateibereich ('Download').



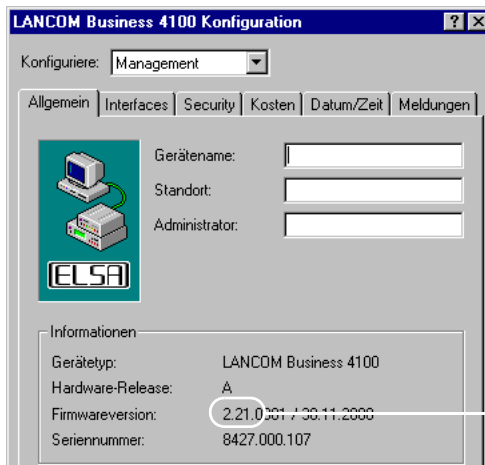
2.1.5

Version der Firmware überprüfen

Die Firmware Ihres *ELSA LANCOM* muss *ELSA LANCOM VPN* unterstützen. In Abhängigkeit von Ihrem Gerät muss mindestens folgende Firmware-Version aufgespielt sein:

Gerät	Firmware
<i>ELSA LANCOM Business 4000/4100</i>	Version 2.21
<i>ELSA LANCOM Business 6001/6011/6021</i>	Version 2.21
<i>ELSA LANCOM DSL/-1610 Office</i>	Version 2.41
<i>ELSA LANCOM DSL/I-1611 Office</i>	Version 2.41

Die Version der Firmware eines *ELSA LANCOM* können Sie auf einfache Art herauszufinden. Doppelklicken Sie in der *ELSA LANconfig*-Auswahlliste auf den gewünschten *ELSA LANCOM*. Es öffnet sich das Konfigurationsfenster, auf dem Sie die Firmware-Version leicht ablesen können:



Die ersten Ziffern zeigen die aktuelle Firmware-Version

2.1.6

Firmware aktualisieren

Dieser Abschnitt ist für Sie nur dann interessant, wenn die Überprüfung der Firmware-Version Ihres Gerätes ergeben hat, dass Sie eine neue Version aufspielen müssen.

Eine aktuelle Firmware für alle unterstützten Geräte ist auf der *ELSA LANCOM VPN Option*-CD im Verzeichnis 'Firmware' abgelegt. In diesem Verzeichnis existieren für die verschiedenen Geräte der *ELSA LANCOM*-Serie passende Unterverzeichnisse, beispielsweise 'Firmware\4x00\' für die Geräte der Serie 4000/4100. Dort finden Sie beispielsweise eine Datei mit der Endung '.221', die die gewünschte Firmware enthält.



Brandneue Firmware-Updates finden Sie auf der ELSA-Homepage www.elsa.de im Dateibereich ('Download'). Suchen Sie Ihr Gerät in der Geräteliste aus, und laden Sie die Datei mit der aktuellen Firmware-Version auf Ihren Rechner herunter.

Informationen zum Aufspielen einer neuen Firmware auf Ihr *ELSA LANCOM* finden Sie im Gerätehandbuch.

2.2

Online-Registrierung

Mit der korrekten Firmware-Version enthält Ihr *ELSA LANCOM* bereits die gesamte VPN-Software. Sie muss nur noch freigeschaltet werden.

Zur Freischaltung der VPN-Option im *ELSA LANCOM* benötigen Sie einen Freischaltcode.



Beachten Sie bitte: Der Freischaltcode liegt dem Paket nicht bei, sondern wird Ihnen bei der Online-Registrierung mitgeteilt.

Der *ELSA LANCOM VPN Option* liegt ein Lizenznachweis (gelber Aufkleber) bei. Auf diesem Aufkleber ist eine Lizenznummer abgedruckt. Mit dieser Lizenznummer können Sie sich einmalig bei ELSA registrieren und erhalten dann einen Freischaltcode.



Eine erfolgreiche Online-Registrierung entwertet die verwendete Lizenznummer Ihrer ELSA LANCOM VPN Option. Der hieraus gewonnene Freischaltcode ist ausschließlich auf dem per Seriennummer angegebenen ELSA LANCOM verwendbar! Vergewissern Sie sich, dass Sie die VPN-Option tatsächlich nur auf dem angegebenen Gerät installieren wollen. Ein späterer Wechsel auf ein anderes Gerät ist ausgeschlossen!

Zur Online-Registrierung halten Sie bitte folgende Daten bereit:

- Genaue Bezeichnung der Software-Option
- Die Lizenznummer (vom gelben Lizenznachweis)
- Seriennummer Ihres freizuschaltenden *ELSA LANCOM* (befindet sich auf der Gehäuseunterseite)
- Ihre Kundendaten (Firma, Name, Anschrift, E-Mail-Adresse).



Die Registrierung ist auch anonym, also ohne Angabe der persönlichen Daten möglich. Zusätzliche Informationen erleichtern uns eine Unterstützung im Support- und Servicefall. Alle Daten werden selbstverständlich streng vertraulich behandelt.

Starten Sie einen Webbrowser, und gehen Sie auf folgende Web-Seite:

<http://www.elsa.de/register/routeroption>

Im angezeigten Formular geben Sie die oben genannten Daten ein und folgen den weiteren Anweisungen der Seite. Nach Eingabe aller Daten bekommen Sie den Freischaltcode zur VPN-Option für Ihr *ELSA LANCOM* sowie Ihre Kundendaten angezeigt. Diese Seite sollten Sie mit der Druckfunktion Ihres Webrowsers ausdrucken. Wenn Sie Ihre E-Mail-Adresse angegeben haben, werden Ihnen die Daten einschließlich des Freischaltcodes zusätzlich per E-Mail zugesandt. Die Online-Registrierung ist damit beendet.

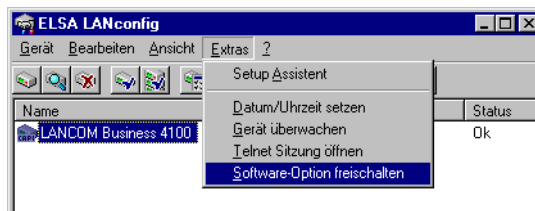


Heben Sie den Freischaltcode gut auf! Möglicherweise benötigen Sie ihn später zum erneuten Freischalten der VPN-Option, etwa nach einer Reparatur.

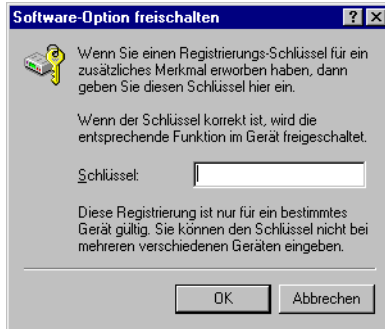
2.3

Freischalten der VPN-Option

Die Freischaltung der VPN-Option ist sehr einfach. In *ELSA LANconfig* markieren Sie den gewünschten *ELSA LANCOM* (durch einfachen Mausklick auf den Eintrag) und wählen den Menübefehl **Extras ► Software-Option freischalten**:



Das Eingabefenster 'Software-Option freischalten' bzw. 'Zusätzliches Merkmal freischalten' erscheint:



Geben Sie den Freischaltcode ein, den Sie über oben genannte Online-Registrierung erworben haben. Der *ELSA LANCOM* startet anschließend automatisch neu.

2.4

Überprüfen der Freischaltung

Die erfolgreiche Freischaltung der *ELSA LANCOM VPN Option* können Sie überprüfen, indem Sie bei ausgewähltem Gerät in *ELSA LANconfig* den Menübefehl **Gerät ► Eigenschaften** auswählen. Im Eigenschaften-Fenster sehen Sie im Register 'Info' eine Liste der aktiven Software-Optionen.

3 Einrichtung der VPN-Verbindung

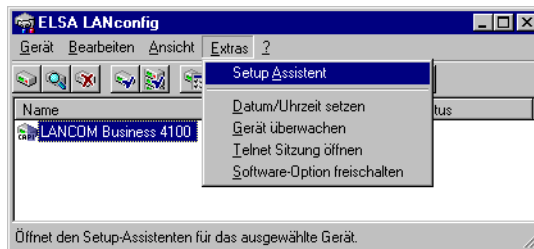
Nachdem Sie die *ELSA LANCOM VPN Option* auf dem gewünschten *ELSA LANCOM* installiert haben, erfahren Sie in diesem Kapitel alles Notwendige zum Aufbau einer VPN-Verbindung.

Dieses Kapitel gliedert sich in sechs Abschnitte:

- Die Benutzung des *ELSA LANconfig*-Assistenten für VPN
- Welche Eingaben sind für die VPN-Verbindung notwendig?
- Beispiele für VPN-Konfigurationen
- Einrichten der Basisverbindung
- Vor Eingabe der VPN-Verbindungsdaten
- Eingabe der Daten und Test der VPN-Verbindung

3.1 Der *ELSA LANconfig*-Assistent für VPN

Die Einrichtung von VPN-Strecken wird mit einem Setup-Assistenten von *ELSA LANconfig* vorgenommen. Zum Aufruf des Assistenten wird das gewünschte *ELSA LANCOM* markiert und der Menübefehl **Extras ► Setup Assistent** ausgewählt:



Daraufhin erscheint ein Fenster mit den für das jeweilige Gerät verfügbaren Assistenten.

Die Bedienung der Assistenten ist intuitiv. Schrittweise werden alle erforderlichen Parameter für die gewünschte Verbindung abgefragt. Mit **Weiter** und **Zurück** kann jederzeit vor- und zurückgesprungen werden.

Der Assistent für VPN-Strecken: Zwei lokale Netze verbinden

Für VPN gibt es keinen separaten Assistenten, sondern es wird der bestehende Assistent für die LAN-LAN-Kopplung ('Zwei lokale Netze verbinden') verwendet. Mit der Freischaltung von *ELSA LANCOM VPN* wird der LAN-LAN-Wizard um die VPN-Abfragen erweitert.

Bestehende Verbindungen in VPN-Verbindungen umwandeln

Für die Umwandlung bereits bestehender Netzwerkkopplungen in VPN-Verbindungen empfehlen wir Ihnen, den LAN-LAN-Assistenten ein zweites Mal komplett auszuführen.

Wenn Sie nach Ihrem eigenen Gerätenamen bzw. nach dem Namen der Gegenstelle gefragt werden, verwenden Sie dieselben Namen, mit denen die alte Netzwerkkopplung arbeitet. Achten Sie dabei auf die exakte Schreibweise.

Dadurch wird die bisherige Netzwerkverbindung durch eine VPN-basierte Netzwerkverbindung ersetzt.

3.2

Welche Fragen stellt der Assistent?

Es ist sehr hilfreich, alle notwendigen Informationen über die beteiligten Geräte zu sammeln, bevor man den Assistenten startet. Deshalb zunächst eine Übersicht über all jene Informationen, die der Installations-Assistent abfragt.

3.2.1

Die Konfigurationseinträge in der Übersicht

In dieser Übersicht finden Sie alle Fragen, die Ihnen der Assistent während der Installation stellt. Einige Fragen sind in bestimmten Konfigurationen nicht erforderlich. Wir erklären dennoch alle Abfragen, erwähnen aber, in welchen Fällen Sie unnötig sind.

Eine VPN-Verbindung besteht immer zwischen dem zu konfigurierenden Gerät und einer bekannten Gegenstelle. Die Konfiguration wird auf beiden Seiten vorgenommen. Dabei ist darauf zu achten, dass die Konfigurationsangaben zueinander passen.

Die Übersicht zeigt Ihnen auch die Abhängigkeiten der Informationen zwischen beiden Gegenstellen. Bei Beachtung dieser Abhängigkeiten lassen sich viele unnötige Fehlangaben vermeiden.

Angabe	Gateway 1		Gateway 2
VPN über direkte Verbindung oder über Internet?	<i>direkt/Internet</i>	↔	<i>direkt/Internet</i>
Typ der eigenen IP-Adresse	<i>statisch/dynamisch</i>	X↔	<i>statisch/dynamisch</i>
Typ IP-Adresse der Gegenstelle	<i>statisch/dynamisch</i>		<i>statisch/dynamisch</i>
Name des eigenen Gerätes	<i>Name1</i>	X↔	<i>Name2</i>
Name der Gegenstelle	<i>Name2</i>		<i>Name1</i>
Interface für Direktverbindung	<i>Interface1</i>		<i>Interface2</i>
ISDN-Rufnummer Gegenstelle	<i>Rufnummer1</i>		<i>Rufnummer2</i>
ISDN-Anruferkennung Gegenstelle	<i>ISDN-Kennung1</i>		<i>ISDN-Kennung2</i>
Kennwort der ISDN-Verbindung	<i>Kennwort1</i>	↔	<i>Kennwort1</i>
Shared Secret für Verschlüsselung	<i>geheim</i>	↔	<i>geheim</i>
Datenkomprimierung	<i>ein/aus</i>	↔	<i>ein/aus</i>
Kanalbündelung	<i>ein/aus</i>	↔	<i>ein/aus</i>
IP-Adresse der Gegenseite	<i>IP-Adresse1</i>		<i>IP-Adresse2</i>
IP-Netzadresse des entfernten Netzes	<i>IP-Adresse3</i>		<i>IP-Adresse4</i>
Netzmaske des entfernten Netzes	<i>IP-Netzmaske zu IP-Adresse3</i>		<i>IP-Netzmaske zu IP-Adresse4</i>
Zugriff auf Stationen im eigenen Netz erlaubt?	<i>Ja = Intranet Nein = Extranet</i>		<i>Ja = Intranet Nein = Extranet</i>
NetBIOS-Routing für Zugriff auf entferntes Netz?	<i>Ja/Nein</i>		<i>Ja/Nein</i>
Name der entfernten Arbeitsgruppe (nur bei NetBIOS)	<i>Arbeitsgruppe1</i>		<i>Arbeitsgruppe2</i>



In den Spalten 'Gateway 1' und 'Gateway 2' finden Sie Auswahlmöglichkeiten und Variable stellvertretend für konkrete Konfigurationsangaben. Diese Stellvertreter sind im Unterschied zu konkreten Eingaben in Kursivschrift gesetzt.

Die Spalte zwischen den Variablen kennzeichnet notwendige Abhängigkeiten, die bei der Eingabe an beiden Gateways zu beachten sind. Beispielsweise müssen die Angaben, ob die VPN-Verbindung über eine direkte Verbindung oder über das Internet aufgebaut werden soll, auf beiden Gateways übereinstimmen. Solche notwendige Übereinstimmungen werden durch Pfeile (↔) symbolisiert.

Die Tabelle gibt Ihnen nur einen ersten Überblick über die möglichen Konfigurationsangaben. Im anschließenden Abschnitt finden Sie detaillierte Beschreibungen der einzelnen Konfigurationsangaben.

Darauf folgt ein Abschnitt mit beispielhaften Konfigurationsbeschreibungen für die wichtigsten Verbindungsvarianten. Zu jeder Variante ist eine Tabelle mit konkreten Eingabewerten angegeben. In diesem Abschnitt suchen Sie sich aus den angebotenen Varianten einfach die passende heraus. Die zugehörige Tabelle zeigt Ihnen auf einen Blick, welche Angaben für Ihre Konfiguration erforderlich sind.

3.2.2 Bedeutung der Konfigurationseinträge



In diesem Abschnitt sind alle Abfragen ausführlich erklärt. Zur besseren Übersicht sind die Fragen nach Thema zusammengefasst.

Direkte Verbindung oder Verbindung über das Internet?

	Gateway 1		Gateway 2
VPN über direkte Verbindung oder über das Internet?	<i>direkt/Internet</i>	↔	<i>direkt/Internet</i>

VPN-Tunnel können sowohl über direkte Verbindungen (d.h. dedizierte Wahl- und Festverbindungen) zwischen den Netzen als auch über das Internet hergestellt werden. Je nach *ELSA LANCOM* werden folgende Anschlusstechniken unterstützt: ADSL, SDSL, Kabelmodem, ISDN, X.21, G.703.

Allgemeine Daten zum eigenen Gerät und zur Gegenstelle

Typ der eigenen IP-Adresse	<i>statisch/dynamisch</i>		<i>statisch/dynamisch</i>
Typ IP-Adresse der Gegenstelle	<i>statisch/dynamisch</i>		<i>statisch/dynamisch</i>
Name des eigenen Gerätes	<i>Name1</i>		<i>Name2</i>
Name der Gegenstelle	<i>Name2</i>		<i>Name1</i>

Für VPN-Verbindungen über das Internet (nicht bei direkten Verbindungen) muss der Typ der IP-Adressen auf beiden Seiten angegeben werden. Es gibt zwei **Typen von IP-Adressen**: statische und dynamische. Eine Erklärung zum Unterschied der beiden IP-Adresstypen finden Sie im Abschnitt 'Schieken Sie Ihre Daten in den Tunnel – zur Sicherheit' auf Seite 15.

Notwendig ist die Eingabe des eigenen IP-Adresstyps und des Typs der Gegenstelle. Beide Angaben müssen sich entsprechen.

Mit der Angabe des **eigenen Gerätenamen** benennen Sie Ihr *ELSA LANCOM* neu. Das Gerät steht mit dem gewählten Namen in der Geräteliste von *ELSA LANconfig* und *ELSA LANmonitor*. Wenn Sie den Namen Ihres Gerätes beibehalten möchten, dann geben Sie den bisherigen Namen ein.

Angaben zur Verbindung

Interface für Direktverbindung	<i>Interface1</i>		<i>Interface2</i>
ISDN-Rufnummer Gegenstelle	<i>Rufnummer1</i>		<i>Rufnummer2</i>
ISDN-Anruferkennung Gegenstelle	<i>ISDN-Kennung1</i>		<i>ISDN-Kennung2</i>
Kennwort der ISDN-Verbindung	<i>Kennwort1</i>	↔	<i>Kennwort1</i>

Bei den Angaben zur Verbindung sind je nach VPN-Verbindungstyp drei Fälle zu unterscheiden:

- Die VPN-Verbindung basiert auf einer direkten Verbindung zwischen den Gegenstellen, also nicht auf einer Verbindung über das Internet.
- Es wird eine Internetverbindung verwendet, und eine Seite verfügt nur über eine dynamische IP-Adresse. In diesem Fall benötigt *ELSA LANCOM Dynamic VPN* einige zusätzliche Angaben für den Aufbau der ISDN-Verbindung zur IP-Adressübermittlung.
- VPN-Tunnel über rein statische Internetverbindungen benötigen diese vier Angaben zur Verbindung nicht. Bei rein statischen Internetverbindungen wird die Gegenstelle über ihre öffentliche IP-Adresse angesprochen (siehe 'Die IP-Adresse der Gegenseite' auf Seite 34).

Das angegebene **Interface** wird für ISDN-Verbindungen zur Gegenstelle verwendet. Die Angabe des Interfaces ist sowohl bei direkten Verbindungen notwendig, als auch bei VPN-Verbindungen über das Internet, wenn die Gegenstelle nur über eine dynamische IP-Adresse verfügt.

Im Feld **ISDN-Rufnummer** wird die Rufnummer der ISDN-Gegenstelle angegeben. Erforderlich ist die Angabe der kompletten Rufnummer der Gegenstelle einschließlich aller notwendigen Vorwahlen. Wenn Ihr Gerät über eine Telefonanlage an das ISDN angeschlossen ist, muss in der Regel ein Präfix für die Amtsholung vorgesetzt werden (üblicherweise eine '0').

Falls der VPN-Tunnel über eine ISDN-Standleitung aufgebaut werden soll, dann geben Sie statt der Rufnummer ein 'F' für „Festverbindung“ ein.



Die Einrichtung einer ISDN-Festverbindung erfordert normalerweise zusätzliche Einstellungen in der erweiterten Konfiguration. Nähere Information dazu finden Sie in Ihrem Gerätehandbuch.

Mit der angegebenen **ISDN-Anruferkennung** wird der Anrufer identifiziert und authentifiziert. Eine Identifikation wird bei allen ISDN-Anrufen durchgeführt: bei direkten Verbindungen über ISDN ebenso wie bei Internetverbindungen, in denen Ihr eigenes Gerät nur eine dynamische IP-Adresse hat.

Wird ein **ELSA LANCOM** angerufen, vergleicht er die für die Gegenstelle eingetragene ISDN-Anruferkennung mit der Kennung, die der Anrufer tatsächlich über den D-Kanal übermittelt. Eine ISDN-Kennung setzt sich üblicherweise aus der nationalen Vorwahl und einer MSN zusammen.

Das **Kennwort für die ISDN-Verbindung** ist eine Alternative zur ISDN-Anruferkennung. Es wird immer dann zur Authentifikation des Anrufers herangezogen, wenn keine ISDN-Anruferkennung übermittelt wird. Das Kennwort muss auf beiden Seiten identisch eingegeben werden. Es wird für Anrufe in beide Richtungen verwendet.

Das Shared Secret

Shared Secret für Verschlüsselung	Shared Secret	↔	Shared Secret
-----------------------------------	---------------	---	---------------

Das Shared Secret ist das zentrale Kennwort für die Sicherheit innerhalb des VPN-Tunnels. Streng genommen wird es zwar nicht zu Verschlüsselung, sondern nur zur gegenseitigen Authentifizierung verwendet. Die Sicherheit der VPN-Verbindung hängt dennoch entscheidend vom Shared Secret ab.



Das Shared Secret ist nicht mit dem Verbindungskennwort zu verwechseln. Das Shared Secret wird zur gegenseitigen Authentifizierung beim Aufbau des logischen VPN-Tunnels verwendet. Mit dem Verbindungskennwort meldet sich ein Anrufer hingegen schon während des physikalischen Verbindungsaufbaus bei der Gegenstelle an. Nähere Informationen zum Verbindungskennwort finden Sie im Abschnitt 'Angaben zur Verbindung' auf Seite 32.

Für den Umgang mit Kennwörtern gelten einige grundsätzliche Regeln, deren Einhaltung wir Ihnen auch für das Shared Secret ans Herz legen wollen:

- **Halten Sie das Kennwort so geheim wie möglich.**

Notieren Sie niemals ein Kennwort. Beliebte aber völlig ungeeignet sind beispielsweise: Notizbücher, Brieftaschen und Textdateien im Computer. Es klingt trivial, kann aber nicht häufig genug wiederholt werden: verrate

ten Sie Ihr Kennwort nicht weiter. Die sichersten Systeme kapitulieren vor der Geschwätzigkeit.

- **Kennwörter nur sicher übertragen.**

Ein gewähltes Kennwort muss der Gegenseite mitgeteilt werden. Wählen Sie dazu ein möglichst sicheres Verfahren. Meiden Sie: Ungeschützte E-Mail, Brief, Fax. Besser ist die persönliche Übermittlung unter vier Augen. Die höchste Sicherheit erreichen Sie, wenn Sie das Kennwort auf beiden Seiten persönlich eingeben.

- **Wählen Sie ein sicheres Kennwort.**

Verwenden Sie zufällige Buchstaben- und Ziffernfolgen. Kennwörter aus dem allgemeinen Sprachgebrauch sind unsicher. Auch Sonderzeichen wie '&"?#-*+_:;,!°' erschweren es Angreifern, Ihr Kennwort zu erraten und so erhöhen die Sicherheit des Kennworts.

- **Verwenden Sie ein Kennwort niemals doppelt.**

Wenn Sie dasselbe Kennwort für mehrere Zwecke verwenden, mindern Sie seine Sicherheit. Wenn eine Gegenseite unsicher ist, werden mit einem Schlag auch alle anderen Verbindungen gefährdet, bei denen dieses Kennwort verwendet wird.

- **Wechseln Sie das Kennwort regelmäßig.**

Kennwörter sollen möglichst häufig gewechselt werden. Das ist mit Mühe verbunden, erhöht aber die Sicherheit des Kennwortes beträchtlich.

- **Wechseln Sie das Kennwort sofort bei Verdacht.**

Wenn ein Mitarbeiter mit Zugriff auf ein Kennwort Ihr Unternehmen verlässt, wird es höchste Zeit, dieses Kennwort zu wechseln. Ein Kennwort sollte auch immer dann gewechselt werden, wenn der geringste Verdacht einer undichten Stelle auftritt.

Wenn Sie diese einfachen Regeln einhalten, erreichen Sie mit dem Shared Secret ein hohes Maß an Sicherheit.

Datenkomprimierung und Kanalbündelung

Datenkomprimierung	<i>ein/aus</i>	↔	<i>ein/aus</i>
Kanalbündelung	<i>ein/aus</i>	↔	<i>ein/aus</i>

Bei der Einrichtung einer direkten VPN-Verbindung bietet der LAN-LAN-Assistent zwei erweiterte Verbindungsoptionen: Zum einen die Datenkomprimierung, zum anderen die Bündelung zweier Verbindungskanäle über MLPPP (**M**ulti**L**ink-**PPP**). Mit beiden Optionen kann die Übertragungsgeschwindigkeit der Verbindung gesteigert werden.



Datenkomprimierung und Kanalbündelung sind auch bei VPN-Verbindungen über das Internet möglich. Die entsprechenden Einstellungen werden allerdings nicht im LAN-LAN-Assistenten, sondern im Internet-Assistenten bei der Einrichtung des Internet-Zugangs vorgenommen.

Die IP-Adresse der Gegenseite

IP-Adresse der Gegenseite	IP-Adresse1	IP-Adresse2
---------------------------	-------------	-------------

Die **IP-Adresse der Gegenseite** wird in folgenden Situationen zum Aufbau der VPN-Verbindung benötigt:

- Bei direkter Verbindung über Stand- oder Wählleitung wird die private IP-Adresse des entfernten *ELSA LANCOM* eingegeben.
- Für eine VPN-Verbindung über das Internet zu einer Gegenstelle mit statischer Adresse wird deren öffentliche IP-Adresse angegeben.
- Verfügt die Gegenstelle hingegen nur über eine dynamische IP-Adresse, so ist deren öffentliche IP-Adresse erst beim Verbindungsaufbau bekannt. Deshalb wird die IP-Adresse im Assistenten nicht abgefragt.

Routing-Einstellungen

IP-Netzadresse des entfernten Netzes	IP-Adresse3	IP-Adresse4
Netzmaske des entfernten Netzes	IP-Netzmaske zu IP-Adresse3	IP-Netzmaske zu IP-Adresse4
Zugriff auf Stationen im eigenen Netz erlaubt?	Ja = Intranet Nein = Extranet	Ja = Intranet Nein = Extranet

Die Routing-Einstellungen betreffen nicht speziell VPN-Verbindungen, sondern werden bei allen LAN-LAN-Kopplungen abgefragt.

Die **IP-Adresse des entfernten Netzwerkes** wird immer mitsamt der zugehörigen **Netzmaske** eingegeben.

Schließlich können Sie den **Zugriff auf Ihr eigenes Netzwerk** beschränken. Im Intranet-Modus hat das entfernte Netzwerk auf IP-Ebene vollständigen Zugriff auf Ihr lokales Netzwerk. Im Extranet-Modus haben die Stationen des entfernten Netzwerkes keinen Zugriff auf Ihr lokales Netzwerk.

Routing für NetBIOS

NetBIOS-Routing für Zugriff auf entferntes Netz?	Ja/Nein	Ja/Nein
Name der entfernten Arbeitsgruppe (nur bei NetBIOS)	Arbeitsgruppe1	Arbeitsgruppe2

Auch die Angaben für das NetBIOS-Routing sind nicht VPN-spezifisch, sondern werden für alle LAN-LAN-Kopplungen auf IP-Basis abgefragt.

Das Protokoll NetBIOS wird von einigen Netzwerk-Systemen für den Zugriff auf gemeinsame Ressourcen (zumeist Server und Drucker) verwendet. Prominentes Beispiel für die Verwendung von NetBIOS: Windows-Netze.

3.3

Beispiele für VPN-Konfigurationen

In diesem Abschnitt finden Sie die wichtigsten Typen von VPN-Verbindungen. Zu jedem VPN-Verbindungstyp sind die notwendigen Konfigurationsangaben in der Form der bekannten Tabelle angegeben.



Die Tabellen enthalten nur die erforderlichen Angaben. So fehlen beispielsweise bei statischen Internetverbindungen die Parameter zur ISDN-Verbindung. Auch die Angaben für NetBIOS werden nicht aufgeführt. In allen Beispielen werden die Tunnel zwischen zwei ELSA LANCOMs aufgebaut. Direkte Verbindungen und die Internet-Einwahl erfolgen über ISDN (über die erste S₀-Schnittstelle). Bei Geräten der Serie ELSA LANCOM Business 6000 kann stattdessen auch eine 2-Mbit-Schnittstelle gewählt werden. Alle abgebildeten LANs verwenden die Netzmaske 255.255.0.0.

3.3.1

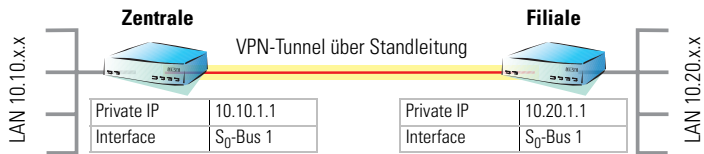
VPN über direkte Verbindung

Die ersten beiden Verbindungstypen fassen wir unter dem Begriff der „direkten Verbindung“ zusammen:

- Standleitung (Festverbindung) über ISDN oder G.703
- Wählverbindung über ISDN

Diese Verbindungen zeichnen sich dadurch aus, dass sie unmittelbar zwischen den beiden verbundenen Geräten aufgebaut werden.

VPN-Verbindung über Standleitung



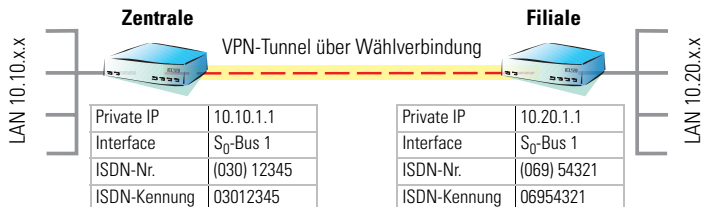
Die beiden **ELSA LANCOM Zentrale** und **Filiale** sind über eine Standleitung miteinander verbunden.

	Zentrale	Filiale
VPN über direkte Verbindung oder über Internet?	direkt	↔ direkt
Name des eigenen Gerätes	Zentrale	↗ Filiale
Name der Gegenstelle	Filiale	↘ Zentrale
Interface	S ₀ -Bus 1	S ₀ -Bus 1
ISDN-Rufnummer Gegenstelle	F	F
Shared Secret für Verschlüsselung	<i>geheim</i>	↔ <i>geheim</i>
IP-Adresse der Gegenseite	10.20.1.1	10.10.1.1
IP-Netzadresse des entfernten Netzes	10.20.0.0	10.10.0.0
Netzmaske des entfernten Netzes	255.255.0.0	255.255.0.0



Die Einrichtung einer ISDN-Festverbindung erfordert in aller Regel zusätzliche Maßnahmen in der erweiterten Konfiguration von ELSA LANconfig. Nähere Information dazu finden Sie im Gerätehandbuch.

VPN über Wählverbindung



Im Beispiel sind die beiden **ELSA LANCOM Zentrale** und **Filiale** über eine direkte ISDN-Wählverbindung gekoppelt.

	Zentrale		Filiale
VPN über direkte Verbindung oder über Internet?	direkt	↔	direkt
Name des eigenen Gerätes	Zentrale	✕	Filiale
Name der Gegenstelle	Filiale		Zentrale
Interface	S ₀ -Bus 1		S ₀ -Bus 1
ISDN-Rufnummer Gegenstelle	06954321		03012345
ISDN-Anruferkennung Gegenstelle	03012345		06954321
Kennwort der ISDN-Verbindung	<i>vertraulich</i>	↔	<i>vertraulich</i>
Shared Secret für Verschlüsselung	<i>geheim</i>	↔	<i>geheim</i>
IP-Adresse der Gegenseite	10.20.1.1		10.10.1.1
IP-Netzadresse des entfernten Netzes	10.20.0.0		10.10.0.0
Netzmaske des entfernten Netzes	255.255.0.0		255.255.0.0

3.3.2

VPN über das Internet

Bei VPN-Verbindungen über das Internet spielt der Typ der IP-Adresse auf den beiden Seiten der Verbindung eine bedeutende Rolle für die Konfiguration. Wir unterscheiden zwischen drei verschiedenen Fällen:

- statisch/statisch
- statisch/dynamisch
- dynamisch/dynamisch



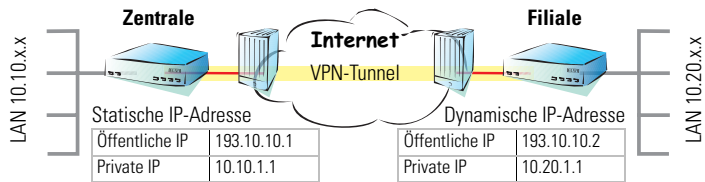
Bei der Einrichtung einer VPN-Verbindung über das Internet ist zu beachten, dass der LAN-LAN-Assistent keinen neuen Zugang ins Internet einrichtet. Ein Internet-Zugang muss bereits vor Ausführung des LAN-LAN-Assistenten eingerichtet sein. Die einwandfreie Funktion dieses Internet-Zugangs sollte vor Einrichtung der VPN-Verbindung auf jeden Fall getestet werden.



Bei mehreren bestehenden Internet-Zugängen wird derjenige verwendet, der mit der Default-Route (255.255.255.255) in der Routing-Tabelle verknüpft ist.

In den folgenden Beispielen wird die Verbindung zum Internet Service Provider bei Geräten mit statischer IP-Adresse über eine Standleitung aufgebaut, bei Geräten mit dynamischer IP-Adresse über eine ISDN-Wählverbindung. Der Verbindungstyp zum ISP ist an dieser Stelle für die Konfiguration unerheblich und kann leicht angepasst werden.

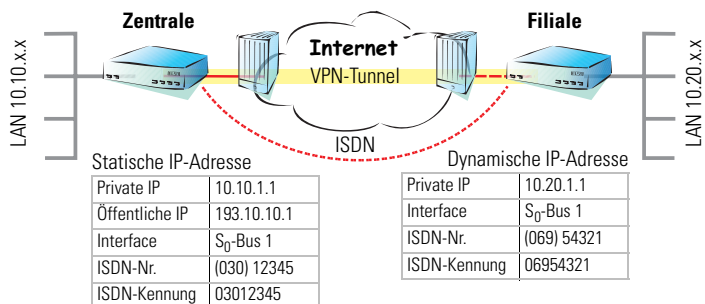
Statisch/statisch



Zwischen den beiden **ELSA LANCOM Zentrale** und **Filiale** besteht ein VPN-Tunnel, der über das Internet aufgebaut wurde. Beide Gateways verfügen über statische IP-Adressen.

Angabe	Zentrale	Filiale
VPN über direkte Verbindung oder über Internet?	Internet	Internet
Typ der eigenen IP-Adresse	statisch	statisch
Typ IP-Adresse der Gegenstelle	statisch	statisch
Name des eigenen Gerätes	Zentrale	Filiale
Name der Gegenstelle	Filiale	Zentrale
Shared Secret für Verschlüsselung	<i>geheim</i>	<i>geheim</i>
IP-Adresse der Gegenseite	193.10.10.2	193.10.10.1
IP-Netzadresse des entfernten Netzes	10.20.0.0	10.10.0.0
Netzmaske des entfernten Netzes	255.255.0.0	255.255.0.0

Statisch/dynamisch



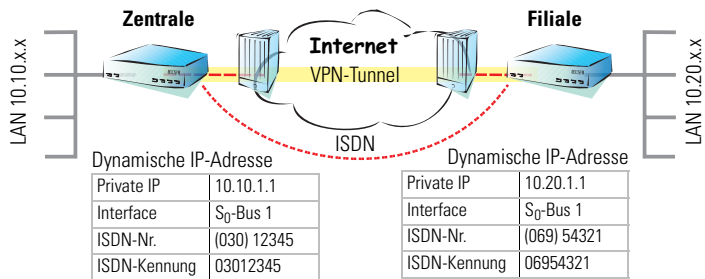
Zwischen den beiden **ELSA LANCOM Zentrale** und **Filiale** besteht ein VPN-Tunnel, der über das Internet aufgebaut wurde. **Zentrale** verfügt über eine statische IP-Adresse, **Filiale** nur über eine dynamische.



Die Angaben zur ISDN-Verbindung werden für die Übertragung der IP-Adresse verwendet und nicht für den eigentlichen Verbindungsaufbau ins Internet. Die Internetverbindung wird mit dem Internet-Zugangs-Assistenten konfiguriert.

Angabe	Zentrale	Filiale
VPN über direkte Verbindung oder über Internet?	Internet	Internet
Typ der eigenen IP-Adresse	statisch	dynamisch
Typ IP-Adresse der Gegenstelle	dynamisch	statisch
Name des eigenen Gerätes	Zentrale	Filiale
Name der Gegenstelle	Filiale	Zentrale
Interface	S ₀ -Bus 1	S ₀ -Bus 1
ISDN-Rufnummer Gegenstelle	06954321	03012345
ISDN-Anruferkennung Gegenstelle	03012345	06954321
Kennwort der ISDN-Verbindung	vertraulich	vertraulich
Shared Secret für Verschlüsselung	geheim	geheim
IP-Adresse der Gegenseite		193.10.10.1
IP-Netzadresse des entfernten Netzes	10.20.0.0	10.10.0.0
Netzmaske des entfernten Netzes	255.255.0.0	255.255.0.0

Dynamisch/dynamisch



Zwischen den beiden **ELSA LANCOM Zentrale** und **Filiale** besteht ein VPN-Tunnel, der über das Internet aufgebaut wurde. Beide Seiten haben dynamische IP-Adressen.



Die Angaben zur ISDN-Verbindung werden für die Übertragung der IP-Adresse verwendet und nicht für den eigentlichen Verbindungsaufbau ins

Internet. Die Internetverbindung wird mit dem Internet-Zugangs-Assistenten konfiguriert.

Angabe	Zentrale		Filiale
VPN über direkte Verbindung oder über Internet?	Internet	↔	Internet
Typ der eigenen IP-Adresse	dynamisch	↔	dynamisch
Typ IP-Adresse der Gegenstelle	dynamisch	↔	dynamisch
Name des eigenen Gerätes	Zentrale	↔	Filiale
Name der Gegenstelle	Filiale	↔	Zentrale
Interface	S ₀ -Bus 1		S ₀ -Bus 1
ISDN-Rufnummer Gegenstelle	06954321		03012345
ISDN-Anruferkennung Gegenstelle	03012345		06954321
Kennwort der ISDN-Verbindung	<i>vertraulich</i>	↔	<i>vertraulich</i>
Shared Secret für Verschlüsselung	<i>geheim</i>	↔	<i>geheim</i>
IP-Netzadresse des entfernten Netzes	10.20.0.0		10.10.0.0
Netzmaske des entfernten Netzes	255.255.0.0		255.255.0.0

3.4

Einrichten der Basisverbindung

Der LAN-LAN-Assistent nimmt nicht in allen Fällen die Einrichtung und Konfiguration der Basisverbindung (Stand-, Wählleitung oder Internetverbindung) selbstständig vor. In einigen Fällen sind ergänzende Konfigurationsschritte erforderlich.

3.4.1

Direkte Verbindungen

Direkte Wählverbindungen richtet der LAN-LAN-Assistent vollständig ein. In aller Regel sind keine Modifikationen in der erweiterten Konfiguration notwendig.

Auch für direkte Festverbindungen über 2-Mbit-Leitungen (G.703, X.21) sind keine weiteren Konfigurationsschritte erforderlich. Anders bei ISDN-Festverbindungen: Sie erfordern in der Regel weitergehende Anpassungen in der erweiterten Konfiguration. Alle notwendigen Informationen finden Sie in der Dokumentation zu Ihrem Gerät.

3.4.2

Verbindungen über Internet

Der LAN-LAN-Assistent richtet keinen Internet-Zugang ein. Er setzt vielmehr eine funktionierende Zugangskonfiguration für das Internet voraus und verwendet diese. Die Einrichtung des Zugangs erfolgt über den Internet-Zugangs-Assistenten. Der Internet-Zugang sollte eingerichtet sein, bevor die VPN-Verbindung mit dem LAN-LAN-Assistenten begonnen wird.

Wählverbindungen ins Internet werden vollständig über den Internet-Zugangs-Assistenten eingerichtet. Auch Festverbindungen über 2-Mbit-Schnittstellen (G.703, X.21) erfordern keine weiteren Schritte.

Bei der Verwendung von ISDN-Festverbindungen wird im Assistenten statt der ISDN-Rufnummer ein 'F' für „Festverbindung“ eingegeben. Üblicherweise sind anschließend zusätzliche Konfigurationsschritte notwendig. Einzelheiten finden Sie in der Gerätedokumentation.

Die VPN-Verbindung verwendet immer den 'DEFAULT'-Internet-Zugang. In der Routing-Tabelle muss dem gewünschten Zugang daher die IP-Adresse 255.255.255.255 zugewiesen sein.

Im *ELSA LANCOM* können auch mehrere Internet-Zugänge eingerichtet werden, über die wechselweise in Abhängigkeit von der Tageszeit der Zugang zum Internet erfolgt.

3.5

Vor Eingabe der VPN-Verbindungsdaten

Bevor Sie den LAN-LAN-Assistenten zum Aufbau einer VPN-Netzkopplung ausführen, prüfen Sie bitte, ob folgende Voraussetzungen vorliegen:

- Die *ELSA LANCOM VPN Option* ist auf beiden *ELSA LANCOM* freigeschaltet.
- Sie kennen alle notwendigen Konfigurationsangaben.
- Wenn die VPN-Verbindung über das Internet erfolgen soll, ist ein Internet-Zugang in beiden *ELSA LANCOM* konfiguriert und funktioniert einwandfrei.

3.6

Eingabe der Daten und Test der VPN-Verbindung

Starten Sie den LAN-LAN-Assistenten und geben Sie die erforderlichen Konfigurationsdaten ein.

Nach Abschluss des Assistenten auf beiden Seiten können Sie die VPN-Verbindung testen. Schicken Sie aus Ihrem Netz eine PING-Anforderung an einen beliebigen Rechner im entfernten Netzwerk.

4 Die Technik hinter VPN

Dieses Kapitel erklärt die technischen Grundlagen von VPN im allgemeinen und *ELSA LANCOM VPN* im besonderen. Sie erhalten einen Überblick über die verwendeten Konzepte und Standards, auf denen die Technik basiert.

Dieses Wissen ist für die Nutzung von VPN mit *ELSA LANCOM* nicht zwingend erforderlich, kann aber hilfreich sein. *ELSA LANCOM VPN* ist so konzipiert, dass auch Anwender ohne tiefere Kenntnisse die Vorteile der VPN-Technik nutzen können. Insbesondere der Aufbau von VPN-Verbindungen ist ohne detaillierte Basiskenntnisse möglich.

4.1 Wie funktioniert VPN?

Ein VPN muss in der Praxis einer Reihe von Ansprüchen gerecht werden:

- Unbefugte Dritte dürfen die Daten nicht lesen können (Verschlüsselung)
- Ausschluss von Datenmanipulationen (Datenintegrität)
- Zweifelsfreie Feststellung des Absenders der Daten (Authentizität)
- Einfache Handhabung der Schlüssel
- Kompatibilität mit VPN-Geräten verschiedener Hersteller

Diese fünf wichtigen Ziele erreicht *ELSA LANCOM VPN* durch die Verwendung des weitverbreiteten IPSec-Standards.

4.1.1 IPSec – Die Basis für *ELSA LANCOM VPN*

Das ursprüngliche IP-Protokoll enthält keinerlei Sicherheitsvorkehrungen. Erschwerend kommt hinzu, dass Pakete unter IP nicht gezielt an den Empfänger gesendet werden, sondern über das gesamte Netzwerksegment an alle angeschlossenen Rechner gestreut werden. Wer auch immer möchte, bedient sich und liest die Pakete mit. Datenmissbrauch ist so möglich.

Deshalb wurde IP weiterentwickelt und es gibt IP inzwischen auch in einer sicheren Variante: IPSec. *ELSA LANCOM VPN* basiert auf IPSec.

IPSec steht für „**IP Security Protocol**“ und ist ursprünglich der Name einer Arbeitsgruppe innerhalb des Interessenverbandes IETF, der **I**nternet **E**ngineering **T**ask **F**orce. Diese Arbeitsgruppe hat über die Jahre ein Rahmenwerk für ein gesichertes IP-Protokoll entwickelt, das heute allgemein als IPSec bezeichnet wird.

Wichtig ist, dass IPSec selber kein Protokoll ist, sondern nur der Standard für ein Protokoll-Rahmenwerk. IPSec besteht in der Tat aus verschiedensten Protokollen und Algorithmen für die Verschlüsselung, die Authentifizierung und das Schlüssel-Management. Diese Standards werden in den folgenden Abschnitten vorgestellt.

Sicherheit im IP-Gewand

IPSec ist (nahezu) vollständig innerhalb in Ebene 3 des OSI-Modells implementiert, also in der Vermittlungsebene (dem Network Layer). Auf Ebene 3 wird in IP-Netzwerken der Verkehr der Datenpakete auf Basis des IP-Protokolls abgewickelt.

Damit ersetzt IPSec das IP-Protokoll. Die Pakete werden unter IPSec intern anders aufgebaut als IP-Pakete. Ihr äußerer Aufbau bleibt dabei aber vollständig kompatibel zu IP. IPSec-Pakete werden deshalb weitgehend problemlos innerhalb bestehender IP-Netze transportiert. Die für den Transport der Pakete zuständigen Geräte im Netzwerk können IPSec-Pakete bei Blick auf Äußere nicht von IP-Paketen unterscheiden.

Ausnahmen sind bestimmte Firewalls und Proxy-Server, die auch auf den Inhalt der Pakete zugreifen. Die Probleme resultieren dabei aus (teilweise funktionsbedingten) Inkompatibilitäten dieser Geräte mit dem geltenden IP-Standard. Diese Geräte müssen entsprechend an IPSec angepasst werden.

In der nächsten Generation des IP-Standards (IPv6) wird IPSec fest implementiert werden. Man kann deshalb davon ausgehen, dass IPSec auch in Zukunft der wichtigste Standard für virtuelle private Netzwerke sein wird.

4.1.2

Alternativen zu IPSec

IPSec ist ein offener Standard. Er ist unabhängig von einzelnen Herstellern und wird innerhalb der IETF unter Einbezug der interessierten Öffentlichkeit entwickelt. Die IETF steht jedermann offen und verfolgt keine wirtschaftliche Interessen. Aus dieser offenen Gestaltung zur Zusammenführung verschiedener technischer Ansätze resultiert die breite Anerkennung von IPSec.

Dennoch gab und gibt es andere Ansätze zur Verwirklichung von VPNs. Nur die beiden wichtigsten seien hier erwähnt. Sie setzen nicht auf der Netzwerkebene wie IPSec an, sondern auf Verbindungs- und auf Anwendungsebene.

Sicherheit auf Verbindungsebene – PPTP, L2F, L2TP

Bereits auf der Verbindungsebene (Level 2 des OSI-Modells) können Tunnel gebildet werden. Microsoft und Ascend entwickelten frühzeitig das **P**oint-to-**P**oint **T**unneling **P**rotocol (PPTP). Cisco stellte ein ähnliches Protokoll mit **L**ayer **2** **F**orwarding (L2F) vor. Beide Hersteller einigten sich auf ein gemeinsames Vorgehen und in der IETF wurde daraus das **L**ayer **2** **T**unnel **P**rotocol (L2TP).

Die Protokolle haben das Ziel, Sicherheit bei der Einwahl in Netzwerke zu bieten und die Standards PPP und SLIP zu ersetzen. Ihr Vorteil gegenüber IPSec liegt vor allem darin, dass beliebige Netzwerk-Protokolle auf eine solche sichere Netzwerkverbindung aufgesetzt werden können, insbesondere NetBEUI und IPX.

Ein wesentlicher Nachteil der beschriebenen Protokolle ist die fehlende Sicherheit auf Paketebene. Außerdem wurden die Protokolle speziell für Einwahlverbindungen entwickelt. L2TP kann auch mit IPSec kombiniert werden und ergibt in dieser Kombination bei Einwahlverbindungen ein gesteigertes Maß an Sicherheit.

Sicherheit auf höherer Ebene – SSL, S/MIME, PGP

Auch auf höheren Ebenen des OSI-Modells lässt sich die Kommunikation durch Verschlüsselung absichern. Bekannte Beispiele für Protokolle dieser Art sind SSL (**S**ecure **S**ocket **L**ayer) vornehmlich für Webbrowser-Verbindungen, S/MIME (**S**ecure **M**ultipurpose **I**nternet **M**ail **E**xtensions) für E-Mails und PGP (**P**retty **G**ood **P**rivacy) für E-Mails und Dateien.

Bei allen obengenannten Protokollen übernimmt eine Anwendung die Verschlüsselung der übertragenen Daten, beispielsweise der Webbrowser auf der einen Seite und der HTTP-Server auf der anderen Seite.

Ein Nachteil dieser Protokolle ist die Beschränkung auf bestimmte Anwendungen. Für verschiedene Anwendungen werden zudem in aller Regel verschiedene Schlüssel benötigt. Die Verwaltung der Konfiguration wird auf jedem einzelnen Rechner vorgenommen und kann nicht komfortabel nur auf den Gateways erfolgen, wie das bei IPSec möglich ist. Zwar sind Sicherheitsprotokolle auf Anwendungsebene intelligenter, schließlich kennen sie die Bedeutung der übertragenen Daten. Zumeist sind sie aber auch deutlich komplexer.

Alle diese Layer-4-Protokolle erlauben nur Ende-Ende-Verbindungen, sind also ungeeignet für die Kopplung ganzer Netzwerke.

Andererseits benötigen diese Mechanismen nicht die geringsten Änderungen der Netzwerkgeräte oder der Zugangssoftware. Zudem können sie im Unterschied zu Protokollen in unteren Netzwerkebenen auch dann noch wirken, wenn die Dateninhalte schon in den Rechner gelangt sind.

Die Kombination ist möglich

Alle genannten Alternativen sind verträglich zu IPSec und daher auch parallel anzuwenden. Auf diese Weise kann das Sicherheitsniveau erhöht werden. Es ist beispielsweise möglich, sich mit einer L2TP-Verbindung ins Internet einzuwählen, einen IPSec-Tunnel zu einem Web-Server aufzubauen und dabei die HTTP-Daten zwischen Webserver und Browser im gesicherten SSL-Modus auszutauschen.

Allerdings beeinträchtigt jede zusätzlich eingesetzte Verschlüsselung den Datendurchsatz. Der Anwender wird im Einzelfall entscheiden, ob ihm die Sicherheit alleine über IPSec ausreicht oder nicht. Nur in seltenen Fällen wird eine höhere Sicherheit tatsächlich notwendig sein. Zumal sich der verwendete Grad an Sicherheit auch innerhalb von IPSec noch einstellen lässt.

4.2

Die Standards hinter IPSec

IPSec basiert auf verschiedenen Protokollen für die verschiedenen Teilfunktionen. Die Protokolle bauen aufeinander auf und ergänzen sich. Die durch dieses Konzept erreichte Modularität ist ein wichtiger Vorteil von IPSec gegenüber anderen Standards. IPSec ist nicht auf bestimmte Protokolle beschränkt, sondern kann jederzeit um zukünftige Entwicklungen ergänzt werden. Die bisher integrierten Protokolle bieten außerdem schon jetzt ein so hohes Maß an Flexibilität, dass IPSec perfekt an nahezu jedes Bedürfnis angepasst werden kann.

4.2.1

Module von IPSec und ihre Aufgaben

IPSec hat eine Reihe von Aufgaben zu erfüllen. Für jede dieser Aufgaben wurde eines oder mehrere Protokolle definiert.

- Sicherung der Authentizität der Pakete
- Verschlüsselung der Pakete
- Übermittlung und Management der Schlüssel

4.2.2

Security Associations – nummerierte Tunnel

Eine logische Verbindung (Tunnel) zwischen zwei IPSec-Geräten wird als SA (**S**ecurity **A**ssociation) bezeichnet. SAs werden selbstständig vom IPSec-Gerät verwaltet. Eine SA besteht aus drei Werten:

- **Security Parameter Index (SPI)**
Kennziffer zur Unterscheidung mehrerer logischer Verbindungen zum selben Zielgerät mit denselben Protokollen
- **IP-Ziel-Adresse**
- **Verwendetes Sicherheitsprotokoll**
Kennzeichnet das bei der Verbindung eingesetzte Sicherheitsprotokoll: AH oder ESP (zu diesen Protokollen in den folgenden Abschnitten mehr).

Eine SA gilt dabei nur für eine Kommunikationsrichtung der Verbindung (simplex). Für eine vollwertige Send- und Empfangsverbindung werden zwei SAs benötigt. Außerdem gilt eine SA nur für ein eingesetztes Protokoll. Werden AH und ESP verwendet, so sind ebenfalls zwei separate SAs notwendig, also jeweils zwei für jede Kommunikationsrichtung.

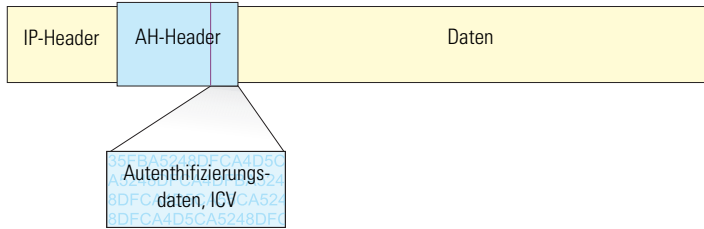
Die SAs werden im IPSec-Gerät in einer internen Datenbank verwaltet, in der auch die erweiterten Verbindungsparameter abgelegt werden. Zu diesen Parametern gehören beispielsweise die verwendeten Algorithmen und Schlüssel.

4.2.3

Die Authentifizierung – das AH-Protokoll

Das AH-Protokoll (**A**uthentication **H**earer) gewährleistet die Integrität und Authentizität der Daten. Häufig wird die Integrität als Bestandteil der Authentizität betrachtet. Wir betrachten im Folgenden die Integrität als separates Problem, das von AH gelöst wird. Neben Integrität und Authentizität bietet AH auch einen wirksamen Schutz gegen Wiedereinspielen empfangener Pakete (Replay Protection).

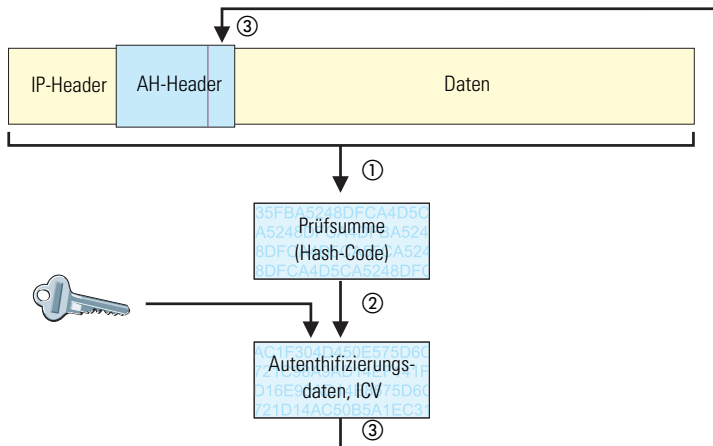
IP-Paketen fügt AH einen eigenen Header direkt hinter dem ursprünglichen IP-Header hinzu. Wichtigster Bestandteil dieses AH-Headers ist ein Feld mit Authentifizierungsdaten (Authentication Data), häufig auch als **I**ntegrity **C**heck **V**alue (ICV) bezeichnet.



Der Ablauf von AH im Sender

Im Sender der Pakete läuft die Erstellung der Authentication Data in 3 Schritten ab.

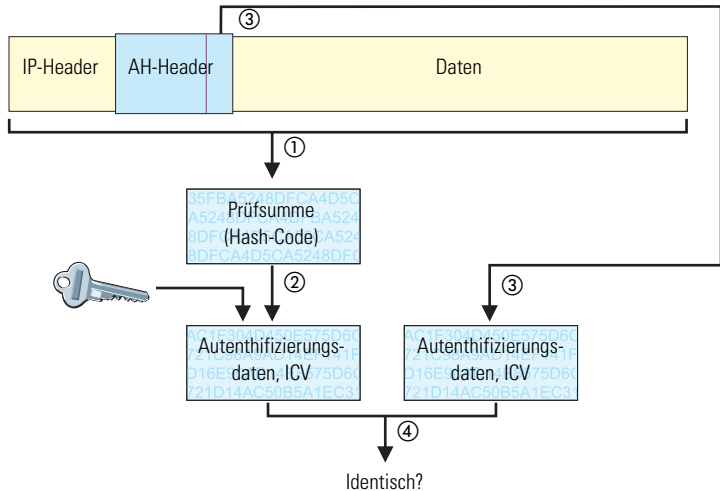
- ① Aus dem Gesamtpaket wird eine Prüfsumme mittels Hash-Algorithmen errechnet.
- ② Diese Prüfsumme wird zusammen mit einem dem Sender und Empfänger bekannten Schlüssel erneut durch einen Hash-Algorithmus geschickt.
- ③ Es ergeben sich die gesuchten Authentifizierungsdaten, die im AH-Header abgelegt werden.



Prüfung von Integrität und Authentizität im Empfänger

Beim Empfänger läuft das AH-Protokoll sehr ähnlich ab. Auch der Empfänger berechnet zunächst mit seinem Schlüssel die Authentifizierungsdaten für das

empfangene Paket. Beim Vergleich mit dem übermittelten ICV des Paketes stellt sich heraus, ob Integrität und Authentizität des Paketes gegeben sind oder nicht.



Bildung der Prüfsumme für den Integritäts-Check

Um die Integrität, also die Korrektheit der transferierten Pakete zu gewährleisten, versieht AH beim Versand jedes Paket mit einer Prüfsumme. Beim Empfänger prüft AH, ob Prüfsumme und Inhalt des Paketes übereinstimmen. Ist das nicht der Fall, dann wurde es entweder falsch übertragen oder bewusst verändert. Solche Pakete werden sofort verworfen und gelangen nicht mehr auf höhere Protokollebenen.

Zur Errechnung der Prüfsumme stehen verschiedene sogenannte Hash-Algorithmen zur Verfügung. Hash-Algorithmen zeichnen sich dadurch aus, dass das Ergebnis (der Hash-Code) eindeutig für die Ausgangsdaten („Fingerabdruck“) ist. Umgekehrt können vom Hash-Code die Ausgangsdaten nicht errechnet werden.

ELSA LANCOM VPN unterstützt die beiden gängigsten Hash-Algorithmen: MD5 und SHA-1. Beide Methoden arbeiten übrigens ohne Schlüssel, d.h. alleine auf der Basis fester Algorithmen. Schlüssel kommen erst in einem späteren Schritt von AH ins Spiel: bei der endgültigen Berechnung der Authentication Data. Die Integritäts-Prüfsumme ist nur ein notwendiges Zwischenergebnis auf dem Weg dorthin.

Berechnung der Authentifizierungsdaten

Im zweiten Schritt bildet AH einen neuen Hash-Code aus der Prüfsumme und einem Schlüssel, die endgültigen Authentifizierungsdaten. Auch für diesen Prozess gibt es unter IPSec verschiedene Standards zur Auswahl. *ELSA LANCOM VPN* unterstützt HMAC (**H**ash-based **M**essage **A**uthentication **C**ode). Als Hash-Algorithmen stehen die Hash-Funktionen MD5 und SHA-1 zur Verfügung. Die HMAC-Versionen heißen entsprechend HMAC-MD5-96 und HMAC-SHA-1-96.

Jetzt wird deutlich, dass AH das Paket selber unverschlüsselt lässt. Lediglich die Prüfsumme des Paketes und der eigene Schlüssel werden gemeinsam zum ICV, den Authentifizierungsdaten, chiffriert und dem Paket als Prüfkriterium beigelegt.

Replay Protection – Schutz vor wiederholten Paketen

AH kennzeichnet zusätzlich zur Beschriftung mit dem ICV jedes Paket auch mit einer eindeutigen, fortlaufenden Nummer (Sequence Number). Dadurch kann der Empfänger solche Pakete erkennen, die von einem Dritten aufgenommen wurden und nun wiederholt gesendet werden. Diese Art von Angriffen wird als „Packet Replay“ bezeichnet.

Standardmäßig gibt der Sender jedem Paket eine solche fortlaufende Nummer mit auf die Reise. Entscheidet der Empfänger, dass er keine Replay Protection benötigt, beendet der Sender die Numerierung.

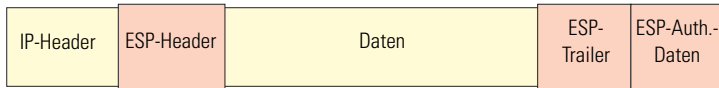
4.2.4

Verschlüsselung der Pakete – das ESP-Protokoll

Das ESP-Protokoll (**E**ncapsulating **S**ecurity **P**ayload) verschlüsselt die Pakete zum Schutz vor unbefugtem Zugriff. Diese ehemals einzige Funktion von ESP wurde in der weiteren Entwicklung des Protokolls um Möglichkeiten zum Schutz der Integrität und zur Feststellung der Authentizität erweitert. Zudem verfügt auch ESP inzwischen über einen wirksamen Schutz gegen Wiedereinspielung von Paketen. ESP bietet damit alle Funktionen von AH an – dennoch empfiehlt sich in einigen Fällen der Einsatz von AH neben ESP.

Arbeitsweise von ESP

Der Aufbau von ESP ist komplizierter als der von AH. Auch ESP fügt einen Header hinter den IP-Header ein, zusätzlich allerdings auch noch einen eigenen Trailer und einen Block mit ESP-Authentifizierungsdaten.



Transport- und Tunnel-Modus

ESP kann (wie AH auch) in zwei Modi verwendet werden: Im Transport-Modus und im Tunnel-Modus.

Im Transport-Modus wird der IP-Header des ursprünglichen Paketes unverändert gelassen und es werden ESP-Header, die verschlüsselten Daten und die beiden Trailer eingefügt.

Der IP-Header enthält die unveränderte IP-Adresse. Der Transport-Modus kann daher nur zwischen zwei Endpunkten verwendet werden, beispielsweise zur Fernkonfiguration eines Routers. Zur Kopplung von Netzen über das Internet kann der Transport-Modus nicht eingesetzt werden – hier wird ein neuer IP-Header mit der öffentlichen IP-Adresse des Gegenübers benötigt. In diesen Fällen kommt ESP im Tunnel-Modus zum Einsatz.

Im Tunnel-Modus wird das gesamte Paket inkl. dem ursprünglichen IP-Header am Tunnel-Eingang verschlüsselt und authentifiziert und mit ESP-Header und -Trailern versehen. Diesem neuen Paket wird ein neuer IP-Header vorangesetzt, diesmal mit der öffentlichen IP-Adresse des Empfängers am Tunnel-Ende.

Verschlüsselungs-Algorithmen

IPSec setzt als übergeordnetes Protokoll keine bestimmte Verschlüsselungs-Algorithmen voraus. In der Wahl der angewandten Verfahren sind die Hersteller von IPSec-Produkten daher frei. *ELSA LANCOM VPN* unterstützt derzeit die folgenden gängigen Standards:

- **DES – Data Encryption Standard**

DES wurde Anfang der 70er Jahre von IBM für die NSA (National Security Agency) entwickelt und war jahrelang weltweiter Verschlüsselungsstandard. Die Schlüssellänge dieses symmetrischen Verfahrens beträgt 56

bit. Es gilt heute aufgrund der geringen Schlüssellänge als unsicher und sollte nach Möglichkeit nicht mehr verwendet werden.

- **Triple-DES** (auch 3DES, dreifacher DES)

Ist eine Weiterentwicklung des DES. Der herkömmliche DES-Algorithmus wird dreimal hintereinander angewendet. Dabei werden zwei oder drei verschiedene Schlüssel mit jeweils 56 bit Länge eingesetzt. Die von *ELSA LANCOM VPN* angewandte Form des Triple-DES-Algorithmus benutzt zwei verschiedene Schlüssel für die drei DES-Durchläufe. Beim dritten DES-Durchlauf wird erneut der Schlüssel des ersten Durchlaufs eingesetzt. Es ergibt sich eine effektive Schlüssellänge von 112 bit.

Triple-DES kombiniert die ausgeklügelte Technik des DES mit einem ausreichend langen Schlüssel und gilt daher als sehr sicher. Triple-DES arbeitet allerdings langsamer als andere Verfahren.

- **CAST** (nach den Autoren **C**arlisle **A**dams und **S**tafford **T**avares)

Ist ein symmetrisches Verfahren mit einer Schlüssellänge von 128 bit. CAST ermöglicht eine variable Änderung von Teilen des Algorithmus' zur Laufzeit.

- **Blowfish**

Die Entwicklung des prominenten Kryptografen Bruce Schneier verschlüsselt symmetrisch. Blowfish erreicht auf Multifunktionsprozessoren einen hervorragenden Datendurchsatz. Das Verfahren gilt als außerordentlich effizient und sicher. Blowfish wird bei *ELSA LANCOM VPN* vom LAN-LAN-Assistenten mit einer Schlüssellänge von 128 bit als Standard voreingestellt.



Die Verschlüsselung kann unter ELSA LANconfig in der Expertenkonfiguration angepasst werden. Eingriffe dieser Art sind in der Regel nur dann erforderlich, wenn VPN-Verbindungen zwischen Geräten unterschiedlicher Hersteller aufgebaut werden sollen.

4.2.5

Management der Schlüssel – IKE

Das **I**nternet **K**ey **E**xchange Protocol (IKE) ist ein Protokoll, in dem Unterprotokolle zum Aufbau der SAs und für das Schlüsselmanagement eingebunden werden können.

Innerhalb von IKE werden in *ELSA LANCOM VPN* zwei Unterprotokolle verwendet: Oakley für die Authentifizierung der Partner und den Schlüsselaustausch sowie ISAKMP für die Verwaltung der SAs.

Aufbau der SA mit ISAKMP/Oakley

Jeder Aufbau einer SA erfolgt in mehreren Schritten (bei dynamischen Internetverbindungen erfolgen diese Schritte, nachdem die öffentliche IP-Adresse übertragen wurde):

- ① Per ISAKMP sendet der Initiator an die Gegenstelle eine Meldung im Klartext mit der Aufforderung zum Aufbau einer SA und Vorschlägen (Proposals) für die Sicherheitsparameter dieser SA.
- ② Die Gegenstelle antwortet mit der Annahme eines Vorschlags.
- ③ Beide Geräte erzeugen nun Schlüsselpaare (bestehend aus öffentlichem und privatem Schlüssel) für eine Diffie-Hellman-Verschlüsselung.
- ④ In zwei weiteren Mitteilungen tauschen beide Geräte ihre öffentlichen Schlüssel für Diffie-Hellman aus.
- ⑤ Die weitere Kommunikation wird mit Diffie-Hellman verschlüsselt. Der Initiator sendet einen Hash-Wert seines Shared Secret. Die Gegenstelle verifiziert den Hash-Wert und sendet einen Hash-Wert des eigenen Shared Secret zurück. Ab diesem Zeitpunkt besteht eine verschlüsselte Verbindung, in der sich beide Partner gegenseitig authentifiziert haben. Die sogenannte Phase 1 des SA-Aufbaus ist beendet.
- ⑥ In Phase 2 werden die Sitzungsschlüssel für die Authentifizierung und die symmetrische Verschlüsselung des eigentlichen Datentransfers per Zufall erzeugt und übertragen.



Für die Verschlüsselung des eigentlichen Datentransfers werden symmetrische Verfahren eingesetzt. Asymmetrische Verfahren (auch bekannt als Public-Key-Verschlüsselung) sind zwar sicherer, da keine geheimen Schlüssel übertragen werden müssen. Zugleich erfordern sie aber aufwändige Berechnungen und sind daher deutlich langsamer als symmetrische Verfahren. In der Praxis wird Public-Key-Verschlüsselung meist nur für den Austausch von Schlüsselmateriale eingesetzt. Die eigentliche Datenverschlüsselung erfolgt anschließend mit schnellen symmetrischen Verfahren.

Der regelmäßige Austausch neuer Schlüssel

ISAKMP sorgt während des Bestehens der SA dafür, dass regelmäßig neues Schlüsselmateriale zwischen den beiden Geräten ausgetauscht wird. Dieser Vorgang geschieht automatisch und kann über die Einstellung der 'Lifetime' in der erweiterten Konfiguration von *ELSA LANconfig* kontrolliert werden.

